rshu

NPCC, Inc.

NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

NPCC REGIONAL STANDARDS COMMITTEE

AGENDA FOR MEETING #14-3
June 18, 2014, 10:00 a.m. - 5:00 p.m. EST
June 19, 2014, 8:00 a.m. - 3:00 p.m. EST
Hampton Inn & Suites Saratoga Springs Downtown Hotel
25 Lake Avenue
Saratoga Springs, New York
Attire: Business Casual

Dial-In: 415-655-0003 (USA) / 416-915-6530 (Canada) **Guest Code: 28796919**

For Reference: Glossary of Terms Used in NERC Reliability Standards, dated April 3, 2014
NPCC Glossary of Terms, dated January 18, 2012

Introductions and Chair's Remarks

NPCC Antitrust Compliance Guidelines

Agenda Items:

1.0 Review of Agenda

2.0 RSC Meeting Minutes

2.1 Approval of Minutes: April 10-11, 2014 RSC Meeting #14-2*

3.0 Drafting Team Members and Executive Tracking Summary

3.1 NPCC Members on NERC Drafting Teams*
3.2 Executive Tracking Summary*
3.3 NERC Project Tracking Spreadsheet (*link*)

4.0 Open Action Items*

4.1 Open Action Items List

5.0 Items Requiring RSC Discussion / Approval

5.1 NERC Weekly Standards Bulletin

5.2 Project 2014-01 – Standards Applicability for Dispersed Generation Resources

-Michael Jones from Nation Grid requested a discussion regarding a cut-off time for submission of comments.

5.3 Project 2010-02 - Connecting Facilities to the Grid - FAC-001-2 and FAC-002-2

* Item in Meeting Material

5.4 Project 2007-17.3 - Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays) - PRC-005-X

-https://cc.readytalk.com/cc/playback/Playback.do?id=19ak93

5.5 NERC Bulk Electric System Update

5.6 Project 2012-13 - NUC - Nuclear Plant Interface Coordination

5.7 Project 2013-03 - Geomagnetic Disturbance Mitigation

5.8 NERC State of Reliability Report Finds Bulk Power System Performance Level Remains High

5.9 Project 2010-05.2 - Special Protection Systems - Phase 2 of Protection Systems

5.10 NERC RAPA Meeting

5.11 NPCC RCC Meeting Minutes

6.0 NERC Reliability Standards

http://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx

6.1 Currently Posted Projects

Project	Comment Period	Ballot Period	Standards Developer	6/18/14 Call-In
Project 2007-11 Disturbance Monitoring - PRC-002-2	6/23/14		Steve Crutchfield	1:00 PM
Project 2008-02 Undervoltage Load Shedding & Underfrequency Load Shedding - PRC-010, PRC-020, PRC-021 and PRC-022	4/16/14 6/23/14 (I)		Erika Chanzes Lacey Ourso	1:15 PM
Project 2010-05.1 - Protection System: Phase 1 (Misoperations) - PRC-004	6/30/14 (F)	6/30/14 (A)	Scott Barfield	1:30 PM
Project 2014-02 - Critical Infrastructure Protection Standards Version 5 Revisions	7/16/14 (F)	7/16/14 (I)	Marisa Hecht Ryan Stewart	1:45 PM
Project 2014-03 - Revisions to TOP/IRO Reliability Standards	7/2/14 (F)	6/17/14 (I)	Ed Dobrowolski	2:00 PM
Project 2013-03 - Geomagnetic Disturbance Mitigation			Luis Marti	2:30 PM
Comments: (I) – Informal; (F) – Formal **Ballots:** (I) – Initial; (A) – Additional; (F) – Final				

6.2 Ballot History (Since last RSC Meeting)*

6.3 Comment Form History (Since last RSC Meeting)*

7.0 NERC Drafting Team Nominations

http://www.nerc.com/pa/Stand/Pages/Drafting-Team-Vacancies.aspx

7.1 Currently Posted Drafting Team Vacancies

7.1.1 None at this time

7.2 Closed Drafting Team Nominations (Since last RSC Meeting)

7.2.1 None at this time

7.3 Solicitation For Informal Development Teams

7.3.1 None at this time

* Item in Meeting Material

8.0 NPCC Regional Reliability Standards*
https://www.npcc.org/Standards/default.aspx

8.1 Current Activities: Regional Standards (PRC-002-NPCC-01 Update)
8.2 Current Activities: Regional Standard Interpretations

9.0 NPCC Non-Standards*
https://www.npcc.org/Standards/SitePages/NonStandardsList.aspx

9.1 Directories Posted to the Open Process
9.1.1 Directory #1 Design and Operation of the Bulk Power System
9.1.2 Directory#3 Maintenance Criteria BPS
9.2 Directory Interpretations
9.2.1 None at this time
9.3 Criteria (A) / Guides (B) / Procedures (C) Documents
9.4 Directory Manual Revisions
9.4.1 Cost Revisions
9.4.2 Other (Comment Form)

10.0 RSC Member Items of Interest
10.1 RSC Roster*

11.0 Standards Activity Post NERC BOT Approval*
(Since last RSC Meeting)

11.1 NERC Filings to FERC
http://www.nerc.com/FilingsOrders/Pages/default.aspx
11.2 FERC Orders / Rules
http://www.nerc.com/FilingsOrders/Pages/default.aspx
11.3 Federal Register
https://www.federalregister.gov/
11.4 FERC Sunshine Act Meeting Notice

12.0 NERC Meetings

12.1 Standards Committee (SC)
http://www.nerc.com/comm/SC/Pages/default.aspx

January 15th - Meeting	January 29th - Call	February 12th - Call
March 12th & 13th - Meeting	April 9th - Call	May 14th - Call
June 10th & 11th - Meeting	July 16th - Call	August 20th - Call
September 23rd & 24th Meeting	October 22nd - Call	November 19th - Call
December 9th & 10th - Meeting		

* Item in Meeting Material

12.2 Standards Committee Process Subcommittee (SCPS)
http://www.nerc.com/comm/SC/Pages/Standards%20Committee%20Process%20Subcommittee%20SCPS/Standards-Committee-Process-Subcommittee-SCPS.aspx

February 6th & 7th	March 12th & 13th	April 23rd Call
June 10th & 11th	September 23rd & 24th	

12.3 Standards Committee Project Management and Oversight Subcommittee (PMOS)
http://www.nerc.com/comm/SC/Pages/ProjectManagementandOversightSubcommittee(PMOS).aspx

February 21st - Call	February 28th - Meeting	April 17th - Meeting

12.4 Member Representatives Committee (MRC) Meeting
http://www.nerc.com/gov/bot/MRC/Pages/AgendaHighlightsandMinutes2013.aspx

February 5th	May 6th & 7th	August 13th & 14th
November 12th & 13th		

12.5 Board of Trustees (BOT) Meeting
http://www.nerc.com/gov/bot/Pages/Agenda-Highlights-and-Minutes-.aspx

February 6th	May 6th & 7th	August 13th & 14th
November 12& 13		

12.6 Reliability Issues Steering Committee (RISC)
http://www.nerc.com/comm/RISC/Pages/AgendasHighlightsandMinutes.aspx

February 13th - Call	March 19th - Meeting	April 9th - Call
May 7th - Meeting	June 17th - Meeting	June 10th - Call
August 14 - Meeting	September 12th - Meeting	October 7th – Call
November 13th - Meeting	December 2nd - Meeting	

13.0 NERC Compliance Tools (Since last RSC Meeting)

13.1 Compliance Analysis Reports (CARs)
http://www.nerc.com/pa/comp/Pages/Compliance-Analysis-Reports.aspx

13.1.1 There have not been any CARs posted since the last RSC meeting

13.2 Reliability Standard Audit Worksheets (RSAWs)
http://www.nerc.com/pa/comp/Pages/Reliability-Standard-Audit-Worksheets-(RSAWs).aspx

13.2.1 Four RSAWs have been issued since the last RSC meeting:

- FAC-003-3, Transmission Vegetation Management, issued 4/24/2014
- NUC-001-2.1, Nuclear Plant Interface Coordination, issued 4/24/2014
- PRC-001-1.1, System Protection Coordination, issued 4/24/2014
- PRC-005-1.1b, Transmission and Generation Protection System Maintenance and Testing, issued 5/15/2014

13.2.2 One RSAW has been posted for comment since the last RSC meeting:

- PRC-002-2, Disturbance Monitoring and Reporting Requirements, issued 6/6/2014

* Item in Meeting Material

13.3 Compliance Application Notices (CANs)
http://www.nerc.com/pa/comp/Resources/Pages/Compliance-Application-Notices.aspx

14.0 NERC Items of Interest (Since last RSC Meeting)

14.1 Lessons Learned
http://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx

14.1.1 Three Lessons Learned have been issued since the last RSC meeting:

- LL20140503 - Facilities Design, Commission, and Maintenance - Improved Contractor Oversight Needed

  Issued 5/20/2014

  Primary Interest Groups: Transmission Owners (TOs), Generator Owners (GOs), Generator Operators (GOPs), Distribution Providers (DPs)
- LL20140502 - Facilities Design, Commission, and Maintenance - Circuit Breaker Modification Leads to Inadvertent Trips

  Issued 5/20/2014

  Primary Interest Groups: Transmission Owners (TOs), Transmission Operators (TOPs), Generator Owners (GOs), Generator Operators (GOPs),
- LL20140501 - Relaying and Protection Systems - High AC Voltage can Lead to Remote Terminal Unit Failures

  Issued 5/20/2014

  Primary Interest Groups: Generator Owners (GOs), Generator Operators (GOPs), Transmission Owners (TOs), Transmission Operators (TOPs)

14.2 Alerts
http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx

14.2.1 One NERC Alert has been released since the last RSC meeting:

- Industry Advisory: Elevated Risk due to large Scale Encryption Vulnerability
  Issued 4/11/14
  Responsible Entities: Balancing Authorities, Distribution Providers, Generator Operator, Generator Owner, Interchange Authority, Load Serving Entity, Planning Authority, Purchasing-Selling Entity, Reliability Coordinator, Resource Planner, Reserve Sharing Group, Transmission Owner, Transmission Operator, Transmission Planner, Transmission Service Provider.

14.3 Five Year ERO Performance Accessmenet

15.0 Other Items of Interest

15.1 NERC Reliability Leadership Summit – September 11, 2014, Washington, DC

15.2 NERC Fall Standards and Compliance Workshop – September 23-25, 2014, Atlanta, GA

* Item in Meeting Material

15.3 2015 Regional Entity Business Plans and Budgets

16.0 Future RSC Meetings and Conference Calls

16.1 RSC 2014 Meeting Dates

Feb. 19th – 20th, NextEra Energy Offices
April 10th & 11th, NPCC Offices
June 18th & 19th, Saratoga, NY
September 17th & 18th, Montreal, Quebec
December 4th & 5th, Halifax, Nova Scotia

Have a joint CC Meeting at Halifax?

16.2 RSC 2014 Conference Call Schedule (calls can be scheduled as needed)
all Calls are planned to start at 10:00 a.m. (call: 415-655-0003 (USA) / 416-915-6530 (Canada), Guest Code 29173141)

July 3	July 18	August 1
August 15	August 29	September 12
September 26	October 10	October 24
November 7	November 21	December 19

Respectfully Submitted,

Guy V. Zito, Chair RSC
Assistant Vice President-Standards
Northeast Power Coordinating Council, Inc.

* Item in Meeting Material

Northeast Power Coordinating Council, Inc. (NPCC)
Antitrust Compliance Guidelines

It is NPCC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. The antitrust laws make it important that meeting participants avoid discussion of topics that could result in charges of anti-competitive behavior, including: restraint of trade and conspiracies to monopolize, unfair or deceptive business acts or practices, price discrimination, division of markets, allocation of production, imposition of boycotts, exclusive dealing arrangements, and any other activity that unreasonably restrains competition.

It is the responsibility of every NPCC participant and employee who may in any way affect NPCC's compliance with the antitrust laws to carry out this commitment.

Participants in NPCC activities (including those participating in its committees, task forces and subgroups) should refrain from discussing the following throughout any meeting or during any breaks (including NPCC meetings, conference calls and informal discussions):

- Industry-related topics considered sensitive or market intelligence in nature that are outside of their committee's scope or assignment, or the published agenda for the meeting;
- Their company's prices for products or services, or prices charged by their competitors;
- Costs, discounts, terms of sale, profit margins or anything else that might affect prices;
- The resale prices their customers should charge for products they sell them;
- Allocating markets, customers, territories or products with their competitors;
- Limiting production;
- Whether or not to deal with any company; and
- Any competitively sensitive information concerning their company or a competitor.

Any decisions or actions by NPCC as a result of such meetings will only be taken in the interest of promoting and maintaining the reliability and adequacy of the bulk power system.
Any NPCC meeting participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NPCC's antitrust compliance policy is implicated in any situation should call NPCC's Secretary, Andrianne S. Payson at 212-335-4765.

* Item in Meeting Material

NPCC, Inc.
NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

NPCC REGIONAL STANDARDS COMMITTEE

AGENDA FOR MEETING #14-1
February 19, 2014, 10:00 a.m. - 5:00 p.m. EST
February 20, 2014, 8:00 a.m. - 3:00 p.m. EST
NextEra Energy, 700 Universe Boulevard, Juno Beach, FL
Attire: Business Casual
Dial-In: 415-655-0003 (USA) / 416-915-6530 (Canada) **Guest Code 29173141**

Note: For reference – Links to the Glossary of Terms Used in NERC Reliability Standards, updated February 13, 2014 and the NPCC Glossary of Terms, updated January 18, 2012, are provided here.

MEETING MINUTES

Attendees:

	Name	***Organization***	***Sector***	***Day(s)***	***Comment***
1.	*Kal Ayoub*	*FERC*	*Guest*	*1 & 2*	
2.	*Guy Zito*	*Northeast Power Coordinating Council*		*1 & 2*	
3.	*Lee Pedowicz*	*Northeast Power Coordinating Council*		*1 & 2*	
4.	*Gerry Dunbar*	*Northeast Power Coordinating Council*		*1 & 2*	
5.	*Damase Hebert*	*Northeast Power Coordinating Council*		*1*	*Part-time via phone*
6.	*Michael Lombardi*	*Northeast Power Coordinating Council*		*1 & 2*	
7.	*Peter Yost Sector 1 Proxy for Chris de Graffenried*	*Consolidated Edison Co. of NY, Inc.*	*1 / 3*	*1*	*via phone*
8.	*Ben Wu*	*Orange and Rockland Utilities*	*1*	*1 & 2*	
9.	*Si-Truc Phan Sector 1 Proxy for Sylvain Clermont*	*Hydro Québec TransÉnergie*	*1 / 2*	*1 & 2*	
10.	*Brian Shanahan*	*National Grid*	*1*	*1 & 2*	
11.	*Alan MacNaughton*	*New Brunswick Power Transmission*	*1*	*1 & 2*	*via phone*
12.	*Mark Kenny*	*Northeast Utilities*	*1*	*1 & 2*	*via phone*
13.	*Ayesha Sabouba*	*Hydro One Networks Inc.*	*1*	*1 & 2*	*via phone*
14.	*Helen Lainis*	*Independent Electricity System Operator*	*2*	*1*	*via phone*
15.	*Kathleen Goodman*	*ISO-NE*	*2*	*1 & 2*	*via phone*
16.	*Jim Grant Proxy for Greg Campoli*	*New York Independent System Operator*	*2*	*1 & 2*	*via phone*
17.	*Michael Jones*	*National Grid*	*3*	*1 & 2*	
18.	*Thomas Neglia Proxy for David Burke*	*Orange and Rockland Utilities, Inc.*	*3*	*1*	*via phone*

DRAFT

	Name	*Organization*	*Sector*	*Day(s)*	*Comment*
19.	*Mike Garton*	*Dominion Resources Services, Inc.*	*4*	*1 & 2*	
20.	*Silvia Parada Mitchell*	*NextEra Energy, LLC*	*4*	*1 & 2*	
21.	*Herb Schrayshuen*	*Power Advisors, LLC – Proxy for NextEra Energy, LLC*	*4*	*1 & 2*	*via phone*
22.	*Bruce Metruck Sector 4 Proxy for Wayne Sipperly*	*New York Power Authority*	*4 / 5*	*1 & 2*	
23.	*Brian Robinson*	*Utility Services*	*5*	*1 & 2*	
24.	*Vijay Puran*	*NYS Department of Public Services*	*6*	*1 & 2*	*via phone*
25.	*Don Nelson*	*Massachusetts DPU*	*Guest*	*2*	*via phone*
26.	*Don Weaver*	*New Brunswick Energy and Utilities Board*	*Guest*	*1 & 2*	
27.	*Ron Falsetti*	*AESI*	*Guest*	*1*	
28.	*Jack Ng*	*Consolidated Edison Co. of NY, Inc.*	*Guest*	*1 & 2*	*via phone*
29.	*Franck Leblanc*	*Florida Power & Light Company*	*Guest*	*1 & 2*	
30.	*Mike O'Neil*	*Florida Power & Light Company*	*Guest*	*1*	*Part-time*
31.	*Edina Bajrektarevic*	*NextEra Energy, LLC*	*Guest*	*1*	*Part-time*

Introductions and Chair's Remarks

- Guy Zito called the meeting to order at 10:00 AM on Wednesday February 19, 2014. [Subsequent technical delays with the phone line postponed the start of the meeting to 10:15AM]

NPCC Antitrust Compliance Guidelines**

- NPCC Antitrust Compliance Guidelines were read.

Agenda Items:

1.0 Review of Agenda

- The review of the agenda resulted in the addition of: 1) Project 2007-06 - System Protection Coordination PRC-027-1, under Agenda Item 10.0 RSC Member Items of Interest; 2) Project 2010-01 - Training under Agenda Item 11.0, Standards Activity Post NERC BOT Approval

2.0 RSC Meeting Minutes

2.1 Approval of Minutes: December 5 & 6, 2013 RSC Meeting #13-6**

- The December 2013 meeting minutes were reviewed. A motion was made and seconded (by Mike Garton and Silvia Parada Mitchell, respectively) to approve the minutes as written. The motion passed.

3.0 Drafting Team Members and Executive Tracking Summary

3.1 NPCC Members on NERC Drafting Teams**

- The spreadsheet of NPCC Members on NERC Drafting Teams was reviewed. It was noted that the spreadsheet was unchanged since the last RSC meeting; however, the NERC Standards Committee (SC) has recently approved the drafting team recommendations for the CIP V5 and Dispersed Generation teams. Both the CIP V5 and Dispersed Generation teams have NPCC representation. The spreadsheet of NPCC Members on NERC Drafting Teams will be updated accordingly.

3.2 Executive Tracking Summary**

- The NERC Executive Tracking Summary (ETS) spreadsheet was reviewed. Updates to the spreadsheet, since the last RSC meeting were related to:

- *NERC Reliability Standards*
- *NERC RSAWs*
- *NPCC Regional Reliability Standards*
- *NPCC Directory Tracking*

3.3 NERC Project Tracking Spreadsheet (*link*)

- A link to the PMOS Project Tracking Spreadsheet was included for information.

4.0 Open Action Items**

- The Open Action Items from previous RSC meetings were reviewed and status updates provided.

- *Item 4.1, "Coordination with the Compliance Committee to develop Joint Activity Action List"*
  - No joint items requiring a combined Compliance Committee and Regional Standards Committee meeting were identified.
- *Item 4.2, "New York Adoption of More Stringent/Specific NPCC Criteria - determine more stringent criteria and submit filing"*
  - NPCC Legal is currently working on the filing and anticipates the submittal no later than the April RSC Meeting.
- *Item 13-5.6,* "NPCC outreach program development – discussion item: members provide input and opportunities for development of an outreach program"
  - Ongoing: A meeting with NYPA is scheduled in March 2014
- *Item 13-6.1 "Research the use of Google Docs"*
  - Completed - The use of Google Doc as a collaboration tool for the development of comment forms for NERC Reliability Standards was discussed. The information provided was useful but it was determined that no action will be taken at this time to change the current process.
- *Item 13-6.2 "Revise Ballot History Spreadsheet to include record of how NPCC voted"*
  - Completed

5.0 Items Requiring RSC Discussion / Approval

5.1 NPCC Regional Standard Processes Manual (RSPM)

- It was reported that the ballot of the NPCC Regional Standard Processes Manual (RSPM) passed. The next step is to present the RSPM to the NPCC Board for approval in March 2014.

5.2 Standards Outreach

- This item was discussed under Agenda Item 4.0, "Open Action Items" - specifically, Open Action Item 13-5.6. As noted, a meeting at NYPA is scheduled in March 2014.

6.0 NERC Reliability Standards

http://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx

6.1 Currently Posted Projects

Project	Comment Period	Ballot Period	Call-In
2014 Work Plan for NERC Reliability Standards Development	2/6/14 – 2/21/14 (I)		11:00 AM
Project 2010-17 - Definition of Bulk Electric System (Phase 2) – Reference Document	1/29/14 – 2/27/14 (I)		11:15 AM

Project	Comment Period	Ballot Period	Call-In
Project 2010-05.1 - Protection System: Phase 1 (Misoperations) – PRC-004-3	1/16/14 - 3/3/14 (F)	2/21/14 – 3/3/14 (A)	10:30 AM
Project 2012-13 - NUC - Nuclear Plant Interface Coordination – NUC-001-2.1 SAR	2/12/14 – 3/13/14 (I)		10:45 AM
Project 2007-17.3 - Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays) - PRC-005-4	2/13/14 – 3/14/14 (I)		
Project 2010-04 Demand Data (MOD C) – MOD-031-1	2/14/14 – 3/20/14	3/11/14 – 3/20/14 (A)	11:30 AM
2010-14.2 - Phase 2 of Balancing Authority Reliability-based Control; Time Error, AGC, and Inadvertent: BAL-004, BAL-005-0.1b, BAL-006-2	Future		11:45 AM

- The currently posted continent-wide projects were addressed used a two pronged approach. On day one of the RSC meeting the NERC Standards Developers called into the meeting to provide an overview of the currently posted projects and to field questions from the RSC members. On day two of the RSC meeting, the currently posted continent-wide projects were discussed by the RSC along with a review of the comments forms and all comments received by NPCC to date. Based on RSC comments, Lee Pedowicz added responses to the appropriate Comment Forms. Comments will be finalized and submitted to NERC.

- *2014 Work Plan for NERC Reliability Standards Development*
  - 2014 Work Plan is a Project Management Tool. It currently captures "what we know" but is meant to be a dynamic living tool to which new projects can be added.
  - TPL Directives may not move forward – when more data becomes available in January 2017, NERC will evaluate the additional data
  - A Projected Posting Schedule is available on the NERC Standards web page
- *Project 2010-17 - Definition of Bulk Electric System (Phase 2) – Reference Document*
  - The Phase 2 Reference Document is meant to assist the industry with the application of the revised BES definition.
  - Follow up with Drafting Team to identify established set of criteria for when an entity can request an exclusion and what should be provided ***[Action]***
- *Project 2010-05.1 - Protection System: Phase 1 (Misoperations) – PRC-004-3*
  - NERC Standards Developer confirmed an RSC member's observation that composite protection could result in reduced reporting of misoperations. Specifically, the application of composite protection would mean a failure of the primary protection would not be reported as a misoperation if the backup protection functioned properly.
- *Project 2012-13 - NUC - Nuclear Plant Interface Coordination – NUC-001-2.1 SAR*
  - Periodic review of NUC-001 recommended revisions to provide greater clarity and to sharpen industry focus on tasks that have a more direct impact on reliability. The proposed changes are intended to reduce administrative burden, add clarity, remove redundancy, and bring compliance elements in accordance with NERC guidelines. An RSC member indicated that the associated implementation plan should take into account the time needed to revise the agreements between the Transmission Entities and the nuclear plants.
- *Project 2007-17.3 - Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays) - PRC-005-4*

- Comments were reviewed and discussed. Prior to submittal to NERC, the RSC will forward the comments to TFSP for its review

- *Project 2010-04 Demand Data (MOD C) – MOD-031-1*
  - The RSC Agenda incorrectly identified this project as currently posted. Although not currently posted, this project will be posted soon.
  - The NERC Standards Developer gave a brief overview of pending changes
- *2010-14.2 - Phase 2 of Balancing Authority Reliability-based Control; Time Error, AGC, and Inadvertent: BAL-004, BAL-005-0.1b, BAL-006-2*
  - This project is not currently posted.
  - The NERC Standards Developer gave a brief overview of pending changes

6.2 Ballot History (Since last RSC Meeting)**

- Ballot History spreadsheet was included in the meeting materials for information. As discussed under Agenda Item 4.0, "Open Action Items," a new column has been added to the spreadsheet to identify how NPCC voted.

- The RSC indicated that prior to a final ballot; a ballot position does not need to be disseminated if the prior ballot position is unchanged.

- It was indicated that NPCC will vote in support of NERC standards unless there is a deal breaker identified

6.3 Comment Form History (Since last RSC Meeting)**

- Comment Form History spreadsheet was included in the meeting materials for information.

6.4 Project 2007-11 Disturbance Monitoring – PRC-002-2

- Drafting Team is currently responding to comments received from the prior posting and should be done in the next couple of weeks. The guidelines and implementation plan will be changed. A 45 comment period is expected to begin in mid-April and will have an associated ballot period at the end.

- CEAP report is currently being developed with the intent of having it completed prior to the next posting. A second CEAP posting is not expected as significant changes to the standard have not been identified.

- The standard is about capturing data and getting results and not about the equipment. Some push back on DDRs for generator has been received. If the Transmission Owner is capturing data on a nearby bus then the Generator Owner does not have to. A suggestion was made by an RSC member that the RSAW address and clarify this issue for the generators.

- The necessity to revise or retire the NPCC Regional Standard will be made once the continent-wide standard is finished

7.0 NERC Drafting Team Nominations

http://www.nerc.com/pa/Stand/Pages/Drafting-Team-Vacancies.aspx

7.1 Currently Posted Drafting Team Vacancies

7.1.1 None at this time

7.2 Closed Drafting Team Nominations (Since last RSC Meeting)

7.2.1 Project 2010-02 - Connecting New Facilities to the Grid (Implement FAC Five-Year Review Recommendations)

7.2.2 Project 2010-05.2 - Protection Systems – Special Protection Systems (SPS)

- Proposed under this project is the expansion from 3 types to 4 types of Special Protection Systems. It was noted that the RSC should follow this closely.

7.2.3 Project 2010-13.3 - Relay Loadability – Stable Power Swings
7.2.4 Project 2014-01 - Standards Applicability for Dispersed Power Producing Resources
7.2.5 TOP/IRO Revisions
7.2.6 CIP Version 5 Revisions

- *As discussed under Agenda Item 4.0, "Open Action Items," the NERC Standards Committee (SC) has recently approved the drafting team recommendations for the Dispersed Generation (Item 7.2.4) and CIP V5 (Item 7.2.6) teams*

7.3 Solicitation For Informal Development Teams

7.3.1 None at this time

8.0 NPCC Regional Reliability Standards**

https://www.npcc.org/Standards/default.aspx

8.1 Current Activities: Regional Standards

- *There are not any Regional Standards currently in active development*

8.2 Current Activities: Regional Standard Interpretations

- *There are no outstanding Regional Standard Interpretations*
- *At the RSC meeting it was noted that the Compliance Clarification for PRC-002-NPCC-01 has been received and will be posted to the NPCC web site. Subsequent to the meeting the clarification was posted and can be found under Standards - PRC-002-NPCC-01 Regional Standard Clarifications & Interpretations*

9.0 NPCC Non-Standards**

https://www.npcc.org/Standards/SitePages/NonStandardsList.aspx

9.1 Directories In Development

- *Gerry Dunbar provided updates for Directories 1, 3, 9 and 10:*
  - *Directory#1 --- Posted to the Open Process for 45 days concluding on Jan. 25th, 2014. Combined working group of the CP11 and CO7 have reconvened on behalf of the TFCO and TFCP to consider comments and draft responses.*
  - *Directory#3 --- TFSP has completed its comparison of the FERC approved PRC-005-2 Protection System Maintenance standard with Directory #3 and has determined that the standard is sufficiently comprehensive to allow Directory #3 to be retired without creating a reliability gap. TFSP is finalizing its recommendation and will be posting Directory#3 to the Open Process to receive comments on its proposal in accordance with the NPCC Directory Manual.*
  - *Preliminary comparison of D#9/ D#10 and NERC BOT approved MOD-025-2 complete. Pending TFCO formal review.*
- *As indicated by the NPCC Board, the consideration of cost effectiveness should be extended to include Directories. Revise the Directory Development Manual to address cost effectiveness **[Action]***

9.2 Directory Interpretations

- *There are no outstanding Directory Interpretations*

9.3 Criteria (A) / Guides (B) / Procedures (C) Documents

- *The following (C) Documents were retired by TFCO in December 2013:*
  - *C-05 Monitoring Procedures for Emergency operations Criteria*
  - *C-07 Monitoring Procedures for the Guide for Rating Generating Capability*

- *C-21 Monitoring Procedures for Conformance with Normal and Emergency Transfer Limits*
- *C-44 Regional Methodology and Procedures for Forecasting TTC and ATC*

10.0 RSC Member Items of Interest

- Information on the following topics can be found in the meeting materials, the links provided and additional notes provided herein.

10.1 2014 NERC Standards Committee Overview**

10.2 NPCC and ERO 2015 Business Plan and Budget Preparation Schedule**

10.3 Cybersecurity Capability Maturity Model**

- The RSC was introduced to the Cybersecurity Capability Maturity Model (aka C2M2) which was developed in support of a White House initiative led by the DOE. The model is included in the meeting material.

- In addition, it was noted that the Department of Homeland Security announced the creation of the Critical Infrastructure Cyber Community "C³" [pronounced C-Cubed] Voluntary Program. This program is an innovative public-private partnership designed to help align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyber risks. The C³ Voluntary Program emphasizes three C's:

- *Converging critical infrastructure community resources to support cybersecurity risk management and resilience through use of the Framework;*
- *Connecting critical infrastructure stakeholders to the national resilience effort through cybersecurity resilience advocacy, engagement and awareness; and*
- *Coordinating critical infrastructure cross sector efforts to maximize national cybersecurity resilience.*

To learn more about the C³ Voluntary Program, visit: http://www.dhs.gov/ccubedvp

10.4 NPCC Board of Directors Policy Input**

10.5 NERC Standards Balloting System**

- NERC is rolling out a new Standards Balloting System (SBS). During the transition period from the current to the new system:

- *Ongoing projects will be balloted in the current system*
- *Once available, the new SBS will be used for new and future projects (This will result in the old and new ballot systems being used concurrently until the projects are currently ongoing are completed or retired.)*

10.6 Events Analysis "Lessons Learned" Template**

- NPCC has created a new Events Analysis "Lessons Learned" Template. The RSC reviewed the new template along with previous recommendations made by TFSP

- Recommend that comments note the process surrounding the form is not clear

10.7 NERC TOP/IRO Technical Conference – St. Louis, MO & Washington, DC

10.8 NERC created Word .doc version of the EOP-004-2 Attachment 2: Event Reporting Form

- Additional Items discussed:

10.9 Guy Zito is working with NERC on a potential revision to the NERC Interpretation process that could result in NERC adoption of a Clarification process.

10.10 NERC posted a Loss of Generator Guideline for comment. The RSC will not be submitting comments on the Guideline.

10.11 Concerns were raised regarding Project 2007-06 - System Protection Coordination PRC-027-1. For example, there were concerns regarding: coordination between entities; tracking and notification of 10% or greater change in fault current at an interconnecting bus; need for a common tool to facilitate data exchange. The specific concerns were emailed to the RSC during the meeting. These concerns will be shared with the Standard Drafting Team. ***[Action]***

11.0 <u>Standards Activity Post NERC BOT Approval</u>**

(Since last RSC Meeting)

- Damase Hebert reviewed the standards activities, post NERC BOT approval, which has transpired since the last RSC meeting. The review of NERC Filings to FERC included:

- *Petition of NERC for Approval of Proposed Reliability Standard PRC-005-3 (Protection System Maintenance), one new (Automatic Reclosing) and five revised definitions (Unsolved Maintenance Issue, Segment, Component Type, Component, and Countable Event), the implementation plan for PRC-005-3 and the Violation Factors (VSFs) and the revised Violation Severity Levels (VSLs).*
- *Petition of NERC for Approval of Reliability Standard MOD-001-2 and Retirement of Reliability Standards MOD-001-1a, MOD-004-1, MOD-008-1, MOD-028-2, MOD-029-1a, and MOD-030-2. NERC also requests approval of (1) the associated implementation plan (2) the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs), and (3) the proposed retirement of Reliability Standards MOD-001-1a, MOD-004-1, MOD-008-1, MOD-028-2, MOD-029-1a, and MOD-030-2.*
- *Reply Comments of NERC on BES Phase 2 Proceeding in which NERC responded to comments submitted by the Electricity Consumers Resource Council, American Forest & Paper Association, Council of Industrial Boiler Owners and American Fuel & Petrochemical Manufacturers (collectively, "ELCON"), First Wind Holdings, LLC Wind Holdings, LLC ("First Wind"), and the American Wind Energy Association ("AWEA").*

- The review of FERC Orders included:

- *Order on Motion to Defer Action on Notice of Proposed Rulemaking. FERC issues an order granting the motion to defer action on the Notice of Proposed Rulemaking (NOPR) in connection with the revisions to the Transmission Operations (TOP) and Interconnection Reliability Operations and Coordination (IRO) Reliability Standards until January 31, 2015.*
- *Notice of Proposed Rulemaking to Approve EOP-010-1 Geomagnetic Disturbance Operations. FERC issues a Notice of Proposed Rulemaking (NOPR) proposing to approve Reliability Standard EOP-010-1 (Geomagnetic Disturbance Operations).*
- *Order No. 794 Approving Reliability Standard BAL-003-1 (Frequency Response and Frequency Bias Setting). FERC issues a final rule approving the Reliability Standard BAL-003-1 (Frequency Response and Frequency Bias Setting).*
- *Order No. 793 Final Rule Approving Protection System Maintenance Reliability Standard. FERC issues a final rule approving NERC's revised Reliability Standard, PRC-005-2 (Protection System Maintenance), which will supersede four existing Reliability Standards, PRC-005-1.1b (Transmission and Generation Protection System Maintenance and Testing), PRC-008-0 (Underfrequency Load Shedding Equipment Maintenance), PRC-011-0 (Undervoltage Load Shedding*

Equipment Maintenance), and PRC-017-0 (Special Protection System Maintenance and Testing).

- *Rehearing Requests of Interest were reviewed regarding the CIP 5 requests filed in mid-December 2013, specifically*
  - *Utility Services requests that FERC clarify that the implementation periods (24 and 36 months) start after the effective date of the standard on April 1, 2016. In the alternative, Utility Services requests that FERC clarify that the implementation plan for entities without applicability under CIP V3 Reliability Standards and entities with potential for Low Impact assets starts after the CIP V5 Reliability Standards become effective.*
  - *EEI and EPSA request clarification with respect to FERC's directive to request NERC to conduct a survey and to submit an informational filing within one year regarding cyber assets included or excluded under the new BES Cyber Asset definition, including its "15 minute parameter."*
  - *EEI and EPSA seek clarification on the effective date. Both the NERC petition and the FERC Order use the terms "issued" and "effective date of order." This means that the effective date for implementation could be either January 1, 2016 or April 1, 2016. EEI and EPSA seek clarification.*
  - *EEI and EPSA state that the April 1, 2017 effective date for low assets was based on the 36 month implementation period but did not take into account the additional directives made by the Commission related to low impact assets. EEI and EPSA state that such an effective date may or may not be reasonable, but it is impossible to tell at this point because the record is still being developed. Therefore, they request a stay on any determination of the effective date for low assets pending NERC's filing in response to the FERC directives.*
  - *APPA and NRECA request FERC to clarify how entities can address day 1 compliance in view of the FERC's directive to address the identify, assess, and correct language. They argue that it is conceivable if not likely that CIP version 5 will become mandatory and enforceable before revised standards that address the Commission's directive have been completed and approved. The question whether entities should assume IAC isn't there or request FERC to provide more guidance on what IAC means, even temporarily*

11.1 NERC Filings to FERC
http://www.nerc.com/FilingsOrders/Pages/default.aspx

11.2 FERC Orders / Rules
http://www.nerc.com/FilingsOrders/Pages/default.aspx

11.3 Federal Register
https://www.federalregister.gov/

- *Project 2010-01, Support Personnel Training (PER-005-2) was NERC BOT approved on 2/6/14. An RSC member indicated that "independently" should be added when referring to operations. A request was made that the NOPR (when issued) be circulated to the RSC and this concern be followed up on.*

12.0 NERC Meetings

12.1 Standards Committee (SC)
http://www.nerc.com/comm/SC/Pages/default.aspx

January 15th - Meeting	January 29th - Call	February 12th - Call
March 12th & 13th - Meeting	April 9th - Call	May 14th - Call
June 10th & 11th - Meeting	July 16th - Call	August 20th - Call
September 23rd & 24th Meeting	October 22nd - Call	November 19th - Call
December 9th & 10th - Meeting		

12.2 Standards Committee Process Subcommittee (SCPS)
http://www.nerc.com/comm/SC/Pages/Standards%20Committee%20Process%20Subcommittee%20SCPS/Standards-Committee-Process-Subcommittee-SCPS.aspx

February 6th & 7th	March 12th & 13th	June 10th & 11th
September 23rd & 24th		

12.3 Standards Committee Project Management and Oversight Subcommittee (PMOS)
http://www.nerc.com/comm/SC/Pages/ProjectManagementandOversightSubcommittee(PMOS).aspx

February 21st - Call	February 28th - Meeting	April 17th - Meeting

12.4 Member Representatives Committee (MRC) Meeting
http://www.nerc.com/gov/bot/MRC/Pages/AgendaHighlightsandMinutes2013.aspx

February 5th	May 7th & May 8th	August 13th & 14th
November 12th & 13th		

12.5 Board of Trustees (BOT) Meeting
http://www.nerc.com/gov/bot/Pages/Agenda-Highlights-and-Minutes-.aspx

February 6th	May 6th & 7th	August 13th & 14th
November 12& 13		

12.6 Reliability Issues Steering Committee (RISC)
http://www.nerc.com/comm/RISC/Pages/AgendasHighlightsandMinutes.aspx

February 13th - Call	March 19th - Meeting	April 9th - Call
May 7th - Meeting	June 17th - Meeting	June 10th - Call
August 14 - Meeting	September 12th - Meeting	October 7th – Call
November 13th - Meeting	December 2nd - Meeting	

13.0 NERC Compliance Tools (Since last RSC Meeting)

13.1 Compliance Analysis Reports (CARs)
http://www.nerc.com/pa/comp/Pages/Compliance-Analysis-Reports.aspx

13.1.1 There have not been any CARs posted since the last RSC meeting

13.2 Reliability Standard Audit Worksheets (RSAWs)
http://www.nerc.com/pa/comp/Pages/Reliability-Standard-Audit-Worksheets-(RSAWs).aspx

13.2.1 There have not been any RSAWs issued since the last RSC meeting

- *Follow up with NERC on current RSAW development process* ***[Action]***

14.0 NERC Items of Interest (Since last RSC Meeting)

14.1 Lessons Learned
http://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx

14.1.1 There have not been any Lessons Learned published since the last RSC Meeting

14.2 Alerts
http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx

14.2.1 There have not been any NERC Alerts released since the last RSC meeting

15.0 Other Items of Interest

15.1 NERC-Led CIP Version 5 Technical Conferences were held January 21, 2014 and January 23, 2014

15.2 NERC State of Standards was held January 30, 2014

15.3 NERC Spring Standards and Compliance Workshop – April 1-3, 2014, San Diego, CA (Registration) (Details)

- *Subsequent to the RSC meeting, the NERC Announcement was issued to which provided the hotel registration, meeting agenda and additional meeting details for the Workshop. The Announcement was distributed to the RSC email list and is also available on the NERC web site at: http://www.nerc.com/pa/Stand/Pages/Workshops.aspx*

15.4 NERC Reliability Leadership Summit – September 11, 2014, Washington, DC

15.5 NERC Fall Standards and Compliance Workshop – September 23-25, 2014, Atlanta, GA

- *Added:*

15.6 Added: NPCC Spring Compliance and Standards Workshop – May 28-30, 2014, Cooperstown, NY

16.0 Future RSC Meetings and Conference Calls

16.1 RSC 2014 Meeting Dates

Feb. 19th – 20th, NextEra Energy Offices
April 10th & 11th, NPCC Offices
June 18th & 19th, Saratoga, NY
September 17th & 18th, Montreal, Quebec
December 4th & 5th, Halifax, Nova Scotia

16.2 RSC 2014 Conference Call Schedule
all Calls are planned to start at 10:00 a.m. (call: 415-655-0003 (USA) / 416-915-6530 (Canada), Guest Code 29173141)

February 28	March 14	March 28
April 11	April 25	May 9
May 23	June 6	June 20
July 3	July 18	August 1
August 15	August 29	September 12
September 26	October 10	October 24
November 7	November 21	December 5
December 19		

- *The meeting adjourned at 10:50 AM on Thursday February 20, 2014. RSC Members were invited to stay for the 11:00 AM Industry Webinar regarding Project 2010-05.1 Protection Systems: Misoperations*

Respectfully Submitted,

Guy V. Zito, Chair RSC
Assistant Vice President-Standards
Northeast Power Coordinating Council, Inc.

NPCC Representatives on NERC Standards Drafting Teams						
Project No.	**Project Title**	**DT Type**	**NPCC Representatives**	**Company**	**Telephone**	**E-mail Address**
2007-02	Operating Personnel Communications Protocols	Standard	Tom Irvine	Hydro One Networks	705-792-3004	tom.irvine@hydroone.com
2007-06	System Protection Coordination	Standard	David Cirka	National Grid	781-907-3240	david.cirka@us.ngrid.com
2007-11	Disturbance Monitoring	Standard	Lee Pedowicz	NPCC	212-840-1070	lpedowicz@npcc.org
			Vladimir Stanisic	AESI	905-875-2075 x253	vladimirs@aesi-inc.com
2007-17.3	Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays)	Standard				
2008-02	Undervoltage Load Shedding	Standard	Charles-Eric Langlois	Hydro-Quebec TransEnergie	514-879-4100	langlois.charles-eric@hydro.qc.ca
2009-03	Emergency Operations	Standard	Connie Lowe	Dominion Resource Services, Inc.	804-819-2917	connie.lowe@dom.com
2010-01	Training (PER)	Standard	Mark Grear	Constellation	410-470-4380	mark.grear@constellation.com
2010-02	FAC Five-Year Review Team	Standard	John Beck	Con Edison	212-460-4244	beckj@coned.com
2010-03	Modeling Data (MOD B)	Standard				
2010-04	Demand Data (MOD C)	Standard	Andrey Oks	NPCC	212-840-1070	aoks@npcc.org
2010-05.1	Protection Systems: Phase 1 (Misoperations)	Standard	Paul Difilippo	Hydro One Networks	647-328-7068	paul.difilippo@hydroone.com
2010-05.2	Special Protection Systems (Phase 2)	Standard	John Ciufo	Hydro One Networks	416-345-5258	john.ciufo@hydroone.com
			Charles-Eric Langlois	Hydro-Quebec TransEnergie	514-879-4100	langlois.charles-eric@hydro.qc.ca
2010-13.3	Phase 3 of Relay Loadability: Stable Power Swings	Standard				
2010-14.1	Balancing Authority Reliability-Based Control, Phase 1: Reserves	Standard	Michael Potishnak	Representing NPCC	413-323-8834	mpot@charter.net
2010-14.2	Balancing Authority Reliability-Based Control, Phase 2	Standard	Michael Potishnak	Representing NPCC	413-323-8834	mpot@charter.net
2010-17	Definition of Bulk Electric System	Standard	Brian Evans-Mongeon	Utility Services	802-552-4022	brian.evans-mongeon@utilitysvcs.com
			Phil Fedora	NPCC	212-840-4909	pfedora@npcc.org
			Ajay Garg	Hydro One Networks	416.345.5420	ajay.garg@HydroOne.com
			Jennifer T. Sterling	Exelon	630-437-2764	jennifer.sterling@exeloncorp.com
2012-09	IRO Five-Year Review	Standard	John Mulhern	Con Edison	212-580-6791	mulhernj@coned.com
2012-13	NUC - Nuclear Plant Interface Coordination	Standard	Kevin Donnelly	Con Edison	914-933-2962	donnellyk@coned.com
2013-03	Geomagnetic Disturbance Mitigation	Standard	Emanuel Bernabeu	Dominion	804-432-8780	emanuel.e.bernabeu@dom.com
			Kenneth Fleischer	NextEra Energy	561-691-2456	kenneth.fleischer@fpl.com
			Luis Marti	Hydro One Networks	416-345-5317	luis.marti@hydroone.com
2013-04	Voltage and Reactive Control (VAR)	Standard	Sharma Kolluri	Entergy	504-576-4045	vkollur@entergy.com
2014-01	Standards Applicability for Dispersed Generation Resources	Standard	Brian Evans-Mongeon	Utility Services	802-552-4022	brian.evans-mongeon@utilitysvcs.com
2014-02	Critical Infrastructure Protection Standards Version 5 Revisions	Standard	Greg Goodrich	NYISO	518-356-7591	ggoodrich@nyiso.com
2014-03	Revisions to TOP/IRO Reliability Standards	Standard	Kyle Russell	IESO	905-855-6475	kyle.russell@ieso.ca
2014-04	Physical Security	Standard	Kathy Judge	National Grid	508-860-6040	kathleen.judge@nationalgrid.com

Source = NERC Standard Drafting Team Rosters - March 2014

Change Control: Changes Since March 2014:

Projects Removed:

1. Project 2010-13.2, Phase 2 of Relay Loadability: Generation

Projects Added:

1. Project 2014-04, Physical Security

NPCC Representative Changes:

1. Project 2010-17, Removed Jennifer Dering as the NPCC Representative as she is no longer at NYPA
2. Project 2012-13, Added Kevin Donnelly, Con Edison, as the NPCC Representative
3. Project 2014-03, Added Kyle Russell, IESO, as the NPCC Representative
4. Project 2014-04, Added Kathy Judge, National Grid, as the NPCC Representative

Revised: 5/7/2014

Tab Name	Last Revised	Summary of Changes
NERC RS Exec Tracking Summary	5/7/2014	
NERC RSAWs	4/24/2014	
NPCC RRS Tracking Summary	3/24/2014	- Regional Standard Processes Manual; Following NPCC BOD approval, NERC posted the proposed NPCC Regional Standard Processes Manual for a 45-day industry review through 8 p.m. Eastern on Wednesday, May 7, 2014
NPCC Doc Tracking Summary	12/12/2013	- C-00 (Discontinued) - C-05 (Retired) - C-07 (Retired) - C-21 (Retired) - C-44 (Retired)
NPCC Directory Tracking Summary	12/11/2013	- Directory #1, Design and Operation of the Bulk Power System posted in Open Process - Directory Development and Revision Manual - Comment Response Document posted
NPCC Directory Interpretations	10/25/2013	- Directory #3 Interpretation on behalf of Hydro One Networks included
Quarterly Filing to NSUARB	8/13/2013	Annotated worksheet to indicate that "Revisions to D#7 and D#12 approved by the Full Members on 7/9/2013. "

Prior Revision

Tab Name	Last Revised	Summary of Changes

NERC Reliability Standards Executive Tracking Summary

Revised: 5/7/2014

Line No.	Project No. / Title	Associated Standard	SAR Posted?	Posted for Comment?	Posted For Ballot?	Industry Approved?	NERC BOT Approved?	Petitioned for FERC Approval?	FERC Approved	Comments	Project Status	
4	Project 2007-02 — Operating Personnel Communications Protocols	~~COM-002-1,~~ COM-002-4	Yes 2nd (Thru 5/2/07)	COM-002-4 Yes (Thru 2/3/14) RSAW Yes (Thru 1/31/14)	Yes (Final Thru 4/7/14)	Yes (4/7/14)	Yes (5/7/14)				Under Development	x
29	Project 2010-04 Demand Data (MOD C)	MOD-031-1 (MOD-016, MOD-017, MOD-018, MOD-019, MOD-020, MOD-021)	x	Yes (Thru 4/10/14)	Yes (Final Thru 5/5/14)		Yes (5/7/2014)			A draft RSAW has been posted to the project page.	Under Development	x
58	Project 2013-04: Voltage and Reactive Control	VAR-001-4, VAR-002-3	Yes (Thru 9/3/13)	VAR-002-3 Yes (Thru 4/14/14) VAR-001-4 / VAR-002-3 Yes (Thru 11/25/13)	VAR-002-3 Yes (Final Thru 5/5/14) VAR-001-4 Yes (Final Thru 12/23/13)	VAR-001-4 Yes (12/23/13)	VAR-002-3 Yes (5/7/14) VAR-001-4 Yes (2/6/14)				VAR-002-3 - Under Development VAR-001-4 - Pending Regulatory Approval	x

Acronyms;
SAR- Standards Authorization Request
RS- Reliability Standard
DT- Drafting Team
SC- NERC Standards Committee
TBD- To Be Determined
BOT- NERC Board of Trustee

NERC Reliability Standard Audit Worksheet (RSAW) Executive Tracking Summary

Revised: 4/24/2014

Further details regarding the individual documents may be found at:
http://www.nerc.com/pa/comp/Pages/Reliability-Standard-Audit-Worksheets-(RSAWs).aspx

RSAW#	Title	Posted for Comment?	Comments Posted?	RSAW Issued?	Comments	
BAL-001-1	Real Power Balancing Control Performance	x	x	3/28/2014	New RSAW Posted	
BAL-003-0.1b	Frequency Response and Bias	x	x	3/20/2014		
BAL-005-0.2b	Automatic Generation Control	x	x	5/20/2013	Revised RSAWs Posted	
CIP-001-2a	Sabotage Reporting	x	x	10/13/2012		
CIP-014-1		Yes (thru 4/24/14)				x
COM-002-2a	Communication and Coordination	x	Yes (4/27/12)	11/14/2012		
COM-002-4	Operating Personnel Communications Protocols	Yes (Thru 1/31/14)				
COM-003-1	Operating Personnel Communications Protocols	Yes (Thru 4/5/13)				
EOP-001-2.1b	Emergency Operations Planning	x	x	8/9/2013	Revised RSAWs Posted	
EOP-002-3.1	Capacity and Energy Emergencies	x	x	3/20/2014	Revised RSAWs Posted	
EOP-003-2	Load Shedding Plans	x	x	10/13/2012		
EOP-004-2	Event Reporting	N/A	N/A	10/15/2013	New RSAW	
EOP-005-2	System Restoration from Blackstart Resources	x	x	7/17/2013	Revised RSAWs Posted	
EOP-006-2	System Restoration Coordination	x	x	7/17/2013	Revised RSAWs Posted	
EOP-008-1	Loss of Control Center Functionality	x	x	6/28/2013	Revised RSAWs Posted	
FAC-003-3	Transmission Vegetation Management	N/A	N/A	4/24/2014	Revision serves to clarify guidance for Requirement R6 regarding initial inspections for calendar year 2014 by expanding the Note to Auditor section	x
FAC-008-3	Facility Ratings	x	x	3/20/2014	Revised RSAWs Posted	
FAC-013-2	Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon	x	x	10/13/2012		
IRO-002-2	Reliability Coordination - Facilities	x	x	3/20/2014		
IRO-003-2	Reliability Coordination - Wide-Area View	x	x	3/20/2014		
IRO-005-3.1a	Reliability Coordination - Current-Day Operations	x	x	5/20/2013	Revised RSAWs Posted	
IRO-014-1	Procedures, Processes, or Plans to Support Coordination Between Reliability Coordinators	x	x	10/13/2012		
MOD-028-2	Area Interchange Methodology	N/A	N/A	10/10/2013	New RSAW	
MOD-031-1	Demand and Energy Data	Yes (Thru 11/22/13)			Draft RSAW posted along with Draft Standard	
NUC-001-2		N/A	N/A	4/24/2014	Revised RSAW represent the initial release for the errata versions of the Reliability Standard	x
PER-001-0.2	Operating Personnel Responsibility and Authority	x	x	5/20/2013	Revised RSAWs Posted	
PER-003-1	Operating Personnel Credentials	x	x	1/23/2013		
PER-005-1	System Personnel Training	N/A	N/A	10/15/2013	Revised RSAWs Posted	
PRC-001-1	System Protection Coordination	N/A	N/A	4/24/2014	Revised RSAW represent the initial release for the errata versions of the Reliability Standard	x
PRC-002-NPCC-01	Disturbance Monitoring	x	x	3/19/2014		
PRC-004-2.1a	Analysis and Mitigation of Transmission and Generation Protection System Misoperations	x	x	3/28/2014	Revised RSAWs Posted	
PRC-004-3	Protection System Misoperation Identification and Correction	Yes (Thru 3/19/14)			Draft RSAW posted along with Draft Standard	
PRC-005-1.1b	Transmission and Generation Protection System Maintenance and Testing	x	x	3/28/2014	Revised RSAWs Posted	
PRC-006-1	Automatic Underfrequency Load Shedding	x	x	6/28/2013	Revised RSAWs Posted	
PRC-023-2	Transmission Relay Loadability	N/A	N/A	10/10/2013	Revised RSAWs Posted	
PRC-025-1	Generator Relay Loadability	Yes (Thru 3/11/13)				
TOP-001-1a	Reliability Responsibilities and Authorities	x	x	5/20/2013	Revised RSAWs Posted	
TOP-002-2.1b	Normal Operations Planning	x	x	3/20/2014	Revised RSAWs Posted	

NPCC Regional Reliability Standards Executive Tracking Summary

Revised: 3/24/2014

Further details regarding the individual documents may be found at: http://www.npcc.org/regStandards/UnderDev.aspx

Line No.	Regional Standard ID	Regional Reliability Standard Title	RSAR Posted?	Posted for Comment?	Posted For Ballot?	Industry Approved?	NPCC BOD Approved?	NERC BOT Approved?	Petitioned for FERC Approval?	FERC Approved	Comments	Project Status
1	BPS-501-NPCC-01	Classification of Bulk Power System Elements (Withdrawn by RSC 8/07/09)	Yes (Thru 2/4/08)	NA	NA	NA	NA	NA	NA	NA	Withdrawn by RSC 8/07/09	Withdrawn
2	PRC-002-NPCC-01	Disturbance Monitoring	Yes (Thru 9/10/08)	Yes (Thru 10/24/09)	Yes (Thru 1/6/10)	Yes (1/6/10)	Yes (1/9/10)	Yes (11/4/10)	Yes (5/31/11)	Yes (10/20/11)	10/24/11 - Approved Standard posted publicly	Completed
3	PRC-006-NPCC-01	Automatic Underfrequency Load Shedding Program	Yes (Thru 8/25/08)	Yes (Thru 11/2/11)	Yes (Pre-ballot Thru 11/2/11)	Yes (11/18/11)	Yes (11/30/11)	Yes (2/9/12)	Yes (5/4/12)	Yes (2/21/13)		Completed
4	PRC-006-NPCC-02										- Regional Standard Authorization Request (RSAR) has been submitted and approved - Drafting Team Nomination period ended March 25, 2013 - Draft Team kick-off conference call was Monday April 8, 2013	Under Development
5	PRC-002-NPCC-01, Interpretation R1.1		x	x	x	Yes (TFSP 10/19/12)	N/A	N/A	N/A	N/A	Posted on the NPCC website under "Regional Standards General" on 6/24/13	Completed
6	PRC-002-NPCC-01, Interpretation R1.2.2		x	x	x	Yes (TFSP 4/8/13)	N/A	N/A	N/A	N/A	Posted on the NPCC website under "Regional Standards General" on 6/24/13	Completed
7	PRC-002-NPCC-01, Interpretation R4,. R5, and R6		x	x	x	Yes (TFSP 5/16/13)	N/A	N/A	N/A	N/A	Posted on the NPCC website under "Regional Standards General" on 6/24/13	Completed
8	BAL-002-NPCC-01	Regional Reserve Sharing	Yes (Thru 11/2/10)	Yes (Thru 12/16/11)	Yes (Thru 1/6/10)						Nomination Form posted - nominations due by 11/10/11	Under Development
9	PRC-012-NPCC-01	Special Protection Systems	Yes (thru 8/18/08)									On Hold
10	Regional Standard Processes Manual	Regional Standard Processes Manual (RSPM)	N/A	Yes (Thru 10/20/13)	Yes (Thru 1/27/14)	Yes (1/27/14)	Yes (3/11/14)				NERC posted the proposed NPCC Regional Standard Processes Manual for a 45-day industry review through 8 p.m. Eastern on Wednesday, May 7, 2014	

Acronyms;
RSAR- Regional Standards Authorization Request
RRS- Regional Reliability Standard
DT- Drafting Team
SC - NERC Standards Committee
TBD- To Be Determined
BOD- NPCC Board of Directors
BOT- NERC Board of Trustee

NPCC Document Open Process Executive Tracking Summary

Revised: **12/12/2013**

Further details regarding the individual documents may be found at: https://www.npcc.org/Standards/SitePages/NonStandardsList.aspx

Line No.	Type	Document	Description	Effective Date	Comments	Status	
1	Criteria	A-01	Criteria for Review and Approval of Documents				
2	Criteria	A-10	Classification of BPS Elements				
3	Criteria	A-15	Disturbance Monitoring Equipment Criteria				
4	Guideline	B-01	NPCC Guide for the Application of Autoreclosing to the Bulk Power System				
5	Guideline	B-12	Guidelines for On-Line Computer System Performance During Disturbances				
6	Guideline	B-25	Guide to Time Suynchronization				
7	Guideline	B-26	Guide for Application of Disturbance Recording Equipement				
8	Guideline	B-27	Regional Critical Asset Identification Methodology				
9	Guideline	B-28	Guide for Generator Sequence of Events Monitoring				
10	Procedure	C-01	NPCC Emergency Preparedness Conference Call Procedures - NPCC Security Conference Call Procedures				
11	Procedure	C-15	Procedures for Solar Magnetic Disturbances Which Affect Electric Power Systems				
12	Procedure	C-17	Procedures for Monitoring and Reporting Critical Operating Tool Failures				
13	Procedure	C-25	Procedure to Collect Power System Event Data				
14	Procedure	C-29	Procedures for System Modeling:Data Requirements and Facility Ratings				
15	Procedure	C-30	Procedure for Task Force on System Protection Review of Disturbances and Protection Misoperations				
16	Procedure	C-33	Procedure for Analysis and Classification of Dynamic Control Systems				
17	Procedure	C-36	Procedures for Communications During Emergencies				
18	Procedure	C-39	Procedure to Collect Major Disturbance Event Data				
19	Procedure	C-42	Procedure for Reporting and Reviewing System Disturbances				
20	Procedure	C-43	NPCC Operational Review for the Integration of New facilities				
21	Procedure	C-45	Procedure for Analysis and Reporting of Protection System Misoperations				
22	Procedure	C-00 (Discontinued)	Listing of NPCC Documents by Type		Discontinued November 2013		x
23	Procedure	C-05 (Retired)	Monitoring Procedures for Emergency Operation Criteria		TFCO Retired 12/6/13		x
24	Procedure	C-07 (Retired)	Monitoring Procedures for the Guide for Rating Generating Capability		TFCO Retired 12/6/13		x
25	Procedure	C-21 (Retired)	Monitoring Procedures for Conformance with Normal and Emergency Transfer Limits		TFCO Retired 12/6/13		x
26	Procedure	C-44 (Retired)	NPCC Regional Methodology and Procedures for Forecasting TTC and ATC		TFCO Retired 12/6/13		x

NPCC Directory Executive Tracking Summary

Revised: 12/11/2013 Further details regarding the individual documents may be found at: https://www.npcc.org/Standards/SitePages/NonStandardsList.aspx

Line No.	Document	Developed From	Title of Directory	Phase	Task Force Review	Posted Open Process?	RCC Approval?	Full Membership Ballot?	Comments	Status
1	Directory #1	Criteria A-2	Design and Operation of the Bulk Power System		TFCP(CP11) and TFCO (CO7)	Yes (Posted thru 1/25/14)				Open Process x
2	Directory #2	Criteria A-3	Emergency Operations		TFCO					Phase 2 reformatting pending TFCO resources.
3	Directory #3	Criteria A-4	Maintenance Criteria for Bulk Power System Protection		TFSP					TFSP to identify differences/gaps between Directory #3 and draft revised PRC-005 and evaluate impact of retiring Directory #3 – pending FERC approval of PRC -005-2
4	Directory #4	Criteria A-5	Bulk Power System Protection Criteria		TFSP				Open Process posting expected in 2013.	TFSP currently reviewing D#4.
5	Directory #5	Criteria A-6	Reserve		TFCO				Revisions to Version 0 of Directory #5 approved by the NPCC Full Members in October 2012.	
6	Directory #6		Regional Reserve Sharing	1/2/1900				Passed 04/09/2012	Directory #6 approved by the NPCC Full Members in Phase 2 format in April 2012.	
7	Directory #7	Criteria A-11	Special Protection Systems		TFSP			Passed 7/9/2013	TFSP Revisions.	
8	Directory #8	Criteria A-12	System Restoration		TFCO					TFCO working group CO11 reviewing initial Phase 2 draft of Directory #8.
9	Directory #9	Criteria A-13	Verification of Generator Gross and Net Real Power Capability	1/2/1900	TFCO			Passed 12/28/11	Directory#9 Phase 2 reformatting complete December 2011.	
10	Directory #10	Criteria A-14	Verification of Generator Gross and Net Reactive Power Capability	1/2/1900	TFCO			Passed 12/28/11	Directory#10 Phase 2 reformatting complete December 2011.	
11	Directory #11									
12	Directory #12		Under frequency Load Shedding Program Requirements		TFSS			Passed 7/9/2013	TFSS Revisions	Directory#12 will be retired once PRC-006-NPCC-1 is fully implemented.
13	Manual		Directory Development and Revision Manual			Yes (Posted thru 9/29/13)			Comment Response Document posted publicly on 11/12/13.	Open Process x

NPCC Directory Interpretations

Revised: 10/25/2013 Further details regarding the individual documents may be found at: https://www.npcc.org/Standards/Directory%20Interpretations/Forms/Public%20List.aspx

Line No.	Document	Title of Directory	Date Final	Task Force Review	Posted Open Process?	RCC Approval?	Full Membership Ballot?	Comments	Status
1	Directory #8 Interpretation	System Restoration	6/18/2012	TFCO	N/A		N/A	Interpretation on behalf of the NYSRC	Complete
2	Directory#3 Interpretation	Maintenance Criteria for Bulk Power System Protection	8/28/2012	TFSP	N/A		N/A	Interpretation on behalf of Bangor Hydro	Complete
3	Directory #3 Interpretation	Maintenance Criteria for Bulk Power System Protection	12/14/2012	TFSP	N/A		N/A	Interpretation on behalf of Con Ed	Complete
4	Directory #3 Interpretation	Maintenance Criteria for Bulk Power System Protection	2/15/2013	TFSP	N/A		N/A	Response Clarified - Interpretation on behalf of Acumen Engineered Solutions	Complete
5	Directory#3 Interpretation	Maintenance Criteria for Bulk Power System Protection	10/25/2013	TFSP	N/A		N/A	Interpretation on behalf of Hydro One Networks	
6	Directory#3 Interpretation	Maintenance Criteria for Bulk Power System Protection		TFSP	N/A		N/A	Interpretation on behalf of IESO	Pending TFSP Review

Quarterly Application to the Nova Scotia Utility and Review Board (NSUARB) for Approval of NPCC Regional Reliability Criteria

Revised: **8/13/2013**

Line No.	Filing Period	Filing Due	Filing Submitted	Comments
1	October 1 to December 31, 2012	3/1/2013	3/1/2013	This filing is NPCC's initial quarterly filing covering the October 1 to December 31, 2012 period and covers the changes to the NPCC Criteria as a result of voting by the Full Members of NPCC.
2	January 1 to March 31, 2013	6/1/2013	N/A	No changes were made during the refeenced period which required filing.
3	April 1 to June 30, 2013	9/1/2013	N/A	No changes were made during the referenced period which required filing.
4	July 1 to September 30, 2013	12/1/2013	N/A	Revisions to D#7 and D#12 approved by the Full Members on 7/9/2013.
5	October 1 to December 31, 2013	3/1/2014	N/A	

Milestone Keys:

IC- Initial Comment
IB- Initial Ballot
AB - Additional Ballot
PB- Presented to BOT
F-Projected filing with
FERC
EVRP- Five-year Review Posting
FYRR - Five-year Review Recommendation to SC

Project Status

On Schedule with Project
Project Off Schedule by One Quarter
Project Off Schedule by Two or more Quarters
No Development Work in Progress

Project Tracking Spreadsheet: 2014 Project Work Plan (Status Updated: 3/11/2014)

This worksheet displays estimates of anticipated standards development milestones for projects in 2014, and it is intended to be a project management tool for use in tracking the status of projects under development compared to their anticipated milestones. Detailed information for each project is available from their respective project pages on the NERC website. Projects that remained from 2013's Project Tracking Spreadsheet that were not prioritized in the RSDP, but that are continuing beyond the first quarter of 2014, are also represented here. Projects not anticipated to continue beyond the first quarter of 2014 are not included (information for those projects remains available under the "Standards Under Development" page on the NERC website). Note that projects listed here represent known projects for 2014. As facts and circumstances warrant, it may be necessary to update this tool, and additional projects may be added in response to regulatory directives, input from RISC, or to meet goals of the NERC strategic plan.

Projected Posting Schedule

The above is a link to the schedule of upcoming postings, which is updated weekly. It includes near term posting projections.

Project Number	Activity/Project (Project Names Hyperlinked to Project Page)	Deliverable	Deadline, if any	Priority in 2014-2016 RSDP, if applicable (see Note 1, below)	2013 PRI Resp	Number of Directives	# of Guidances (see Note 2)	Comments	PMOS Liaison	NERC Contact	Status: Green, Yellow, Red	Milestones: Planned vs. Actual/Projected (See Notes 3 and 4)
2007-06	System Protection Coordination	PRC-003, PRC-027		N/A		1			Jennifer Sterling	Al McMeekin	Project extended to address an additional issue by FERC	Plan
												Actual/Projected
2007-11	Disturbance Monitoring	PRC-002, PRC-018		Medium	2		1		Guy Zito	Steve Crutchfield		Plan
												Actual/Projected
2007-17.3	Protection System Maintenance: Sudden Pressure Relays	PRC-005-4		Pending Prioritization in 1Q 2014	1	1			Charles Yeung	Jordan Mallory		Plan
												Actual/Projected
2008-02	Undervoltage Load Shedding	PRC-010, PRC-022		High	2	1	1		Jennifer Sterling	Erika Chances	Delayed to coordinate with the development of the SPS definition	Plan
												Actual/Projected
2009-02	Real-time Reliability Monitoring and Analysis Capabilities	New Standards	January 31, 2015 deadline to address concerns in NOPR proposing to remand TOP/IRO standards	High		3			Jennifer Sterling	Ed Dobrowolski		Plan
												Actual/Projected
2009-03	Emergency Operations	EOP-001, EOP-002, EOP-003		High	14	3	2		Gary Kruempel	Laura Anderson	Delayed to coordinate with PER-5 batching	Plan
												Actual/Projected
2010-02	Connecting new facilities to the grid/Five-year Review of FAC standards	FAC-001, FAC-002		Low		1	1	Standards that were affirmed during FYR were presented to the Board in Q1 2014. Standards recommended for revision are continuing development in 2014.	Ken Goldsmith	Mallory Huggins		Plan
												Actual/Projected
2010-03	Demand Data (MOD-C)	MOD-016, MOD-017, MOD-018, MOD-019, MOD-020, MOD-021		N/A	10	10	4	The project received a 57.59% approval on its second ballot. The SDT is reviewing industry comments.	Scott Miller	Darrel Richardson		Plan
												Actual/Projected
2010-05.1	Phase 1 of Protection Systems - Misoperations	PRC-003, PRC-004		N/A			2		Jennifer Sterling	Scott Barfield		Plan
												Actual/Projected
2010-05.2	Special Protection Systems: Phase 2 of Protection Systems	PRC	Self-imposed deadline for definition of SPS is February 2015 for coordination with other PRC projects.	Medium				Additional BOT milestone added. First is for definition of SPS; the second is for the standards.	Matt Morais	Al McMeekin		Plan
												Actual/Projected
2010-13.3	Relay Loadability Stable Power Swings	PRC	December 31, 2014 deadline to address phase 3 directives covered by this project	Pending Prioritization in 1Q 2014				The technical committee provided a report, but the project has not yet been evaluated for prioritization.	Charles Lyne	Scott Barfield		Plan
												Actual/Projected
2010-14.1	NAMC Directives and Issues-Project 2010-14.1 Balancing Authority Reliability-based Controls	BAL-001, BAL-002, BAL-013		N/A	4				Ron Parsons	Darrel Richardson	Project extended to address an additional issue raised by FERC	Plan
												Actual/Projected
2010-14.2	Phase 2 of Balancing Authority Reliability-based Control: Time Error, AGC, and Inadvertent	BAL-004, BAL-005-0.1b, BAL-006-2		Medium	11	7	6	Periodic review project delayed for completion of Project 2014-01.1 due to limited subject matter experts in BAL standards	Ken Goldsmith	Sean Cavote		Plan
												Actual/Projected
2012-09	Implementation of IRO Review Recommendations	IRO-003, IRO-004, IRO-008, IRO-009, IRO-010		Medium	2	2			Brian Murphy	Soo Jin Kim		Plan
												Actual/Projected
2012-13	Implementation of NUC Review Recommendations	NUC-001		Low					PMOS Oversight	Stephen Eldridge		Plan
												Actual/Projected
2013-03	Geomagnetic Disturbance Mitigation Stage II	New Standards	FERC filing deadline of January 21, 2015	High		14			Brian Murphy	Mark Olson		Plan
												Actual/Projected
2013-04	VAR Directives	VAR-002		N/A	3	6	5	VAR-001, which addresses the FERC directives, passed final ballot 12/23/2013 with 75.35% approval. VAR-002 received a 66.16% approval rating in November 2013, and the SDT is reviewing industry comments.	Ron Parsons	Soo Jin Kim		Plan
												Actual/Projected
2014-01	Standards Applicability for Dispersed Generation Resources	Various	Goal is to complete (including regulatory approval) prior to BES Phase 2 implementation 7/1/2016	Medium (prioritized by SC January 2014)					Gary Kruempel	Sean Cavote		Plan
												Actual/Projected
2014-02	CIP Version 5 Revisions	CIP	FERC filing deadline for certain directives of February 3, 2015.	Pending Prioritization in 1Q 2014		8			Brian Murphy	Marisa Hecht and Ryan Stewart		Plan
												Actual/Projected
2014-03	TOP/IRO Revisions	TOP/IRO	Deadline of January 31, 2015	Pending Prioritization in 1Q 2014					Brian Murphy	Ed Dobrowolski		Plan
												Actual/Projected
TBD	TPL Directive	TPL-001-4	Goal is to complete directives and file in time for FERC action prior to implementing TPL-001-4	Pending Prioritization in 1Q 2014		1		May not move forward.	Matt Morais	Ed Dobrowolski		Plan
												Actual/Projected

Note 1: The prioritizations here reflect those prioritizations assigned as part of the 2014-2016 Reliability Standards Development Plan (RSDP). In its approach to prioritizing Reliability Standards projects, the RSDP considered how Reliability Standard family priorities are applied to individual projects and outstanding work. Specific elements included: (1) RISC Category Rankings; (2) regulatory directives; (3) regulatory deadlines; (4) Reliability Standard requirement candidates for retirement; (5) the IDRP content and quality assessments; and (6) additional considerations (fill-in-the-blank status and five-year assessment commitments). Some projects were not prioritized in the RSDP, as they were originally anticipated to be complete before the end of the first quarter of 2014, and those projects have an "N/A" designation in this column. Other projects have been added to the Project Tracking Spreadsheet that were not prioritized in the RSDP. These were added in response to regulatory directives that were issued following completion of the RSDP, and they will be prioritized according to the same process during the first quarter of 2014 according to the same process described in the RSDP. Those projects are designated as "Pending Prioritization in 1Q 2014." As discussed in the 2014-2016 RSDP, the prioritization will occur in collaboration between NERC Staff and the Standards Committee.

Note 2: Refers to guidances from regulatory orders for standards activity to consider, but that do not carry the same effect as a directive.

Note 3: In the columns at right, in some cases, an "additional ballot" is not indicated for planning purposes, but if consensus is not supported on an initial ballot, or if substantive changes occur, one will be scheduled.

Note 4: In the columns at right, there are no "plan" milestones in some cases because the project was originally planned to be complete in 2013, and the project's "actual" milestones have extended into 2014).

RSC Meeting #14-3, Agenda Item 4.0 Open Action Items

Item	Description	Owner	Due	Status
4.1	Coordination with the Compliance Committee to develop Joint Activity Action List	Greg Campoli	RSC Meeting	Ongoing
4.2	New York Adoption of More Stringent/Specific NPCC Criteria - determine more stringent criteria and submit filing	Gerry Dunbar	April 2014	Update: An initial draft has been completed and is being reviewed by NPCC senior staff. NPCC estimates filing with the NYSPSC in late April or early May.
13-5.6	NPCC outreach program development – discussion item: members provide input and opportunities for development of an outreach program	RSC	RSC Meeting	Ongoing
14-1.1	Project 2010-17, BES - Follow up with Drafting Team to identify established set of criteria for when an entity can request an exclusion and what should be provided	Guy Zito		Update: On March 31, 2014, the Standards Committee endorsed posting the final Reference Document as a supporting document. This action item will remain open to facilitate future discussions regarding the BES exception process
14-1.2	Revise the Directory Development Manual to address cost effectiveness	G. Dunbar		Update: Preliminary revisions incorporating cost concepts into the Manual have been completed. Posting to the Open Process pending.

DRAFT

RSC Meeting #14-3, Agenda Item 4.0 Open Action Items

Item	Description	Owner	Due	Status
14-1.3	Project 2007-06 - System Protection Coordination – share concerns raised at the RSC meeting with the Standard Drafting Team *[At the February RSC meeting there were concerns regarding: coordination between entities; tracking and notification of 10% or greater change in fault current at an interconnecting bus; need for a common tool to facilitate data exchange.]*	Guy Zito		
14-1.4	Follow up with NERC on current RSAW development process	Guy Zito		Update: - An RSAW that is being developed during the standards development process will be posted concurrently with the standard - A working group developed a process to vet proposed changes to an RSAW that is already in place for an existing standard. The working group was formed with representation from the MRC, NERC staff, and the NERC Board. The proposed process is slated to be on the MRC agenda for the May 2014 meeting. (See meeting handout Item 4a for additional information)
14-2.1	Update NPCC Members on NERC Drafting Teams based on feedback received at the April 2014 RSC meeting			

DRAFT

RSC Meeting #14-3, Agenda Item 4.0 Open Action Items

Item	Description	Owner	Due	Status
14-2.2	Update Executive Tracking Summary spreadsheet for: • Project 2007-02 Operating Personnel Communications Protocols: COM-002-4 Final Ballot • Project 2010-05.1 was updated under the Reliability Standards tab but was missing from summary of changes. The summary of changes should be corrected.			
14-2.3	Update the rscmembers email list to include both Primary and Alternate RSC members			
14-2.4	Project 2010-02, the use of the term "Facilities" rather than entities defined by the function model was not supported by the RSC. Provide alternate language for consideration	Helen Lainis		

DRAFT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Weekly Standards Bulletin

May 5-11, 2014

ACTIVE STANDARDS POSTINGS

Current and Upcoming Ballots (ballot periods close at 8 p.m. Eastern)			
Project	**Action**	**Start Date**	**End Date**
Project 2013-04 - Voltage and Reactive Control - VAR-002-3	Final Ballot	04/24/14	05/05/14
Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Final Ballot	04/25/14	05/05/14
NEW Project 2014-04 - Physical Security - CIP-014-1	Final Ballot	05/01/14	05/05/14
Project 2010-02 - Connecting Facilities to the Grid - FAC-001-2 and FAC-002-2	Ballot and Non-Binding Polls	05/06/14	05/15/14
Project 2012-13 - NUC - Nuclear Plant Interface Coordination - NUC-001-3	Initial Ballot and Non-Binding Poll	05/13/14	05/22/14
Project 2007-17.3 - Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays) - PRC-005-X	Initial Ballot and Non-Binding Poll	05/23/14	06/02/14
Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings - PRC-026-1	Initial Ballot and Non-Binding Poll	05/30/14	06/09/14

Join Ballot Pools (ballot pool windows close at 8 a.m. Eastern)			
Project	**Action**	**Start Date**	**End Date**
Project 2012-13 - NUC - Nuclear Plant Interface Coordination - NUC-001-3	Join Ballot Pool	04/08/14	05/07/14
Project 2007-17.3 - Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays) - PRC-005-X	Join Ballot Pool	04/17/14	05/16/14

Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings - PRC-026-1	Join Ballot Pool	04/25/14	05/27/14

Posted for Comment (comment periods close at 8 p.m. Eastern)			
Project	**Action**	**Start Date**	**End Date**
Project 2014-01 - Standards Applicability for Dispersed Generation Resources	Comment Form	04/17/14	05/05/14
Project 2010-02 - Connecting Facilities to the Grid - FAC-001-2 and FAC-002-2	Comment Form	04/01/14	05/15/14
Project 2013-03 - Geomagnetic Disturbance Mitigation – TPL-007-1	Comment Form	04/22/14	05/21/14
Project 2012-13 - NUC - Nuclear Plant Interface Coordination - NUC-001-3	Comment Form	04/08/14	05/22/14
Project 2007-17.3 - Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays) - PRC-005-X	Comment Form	04/17/14	06/02/14
Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings – PRC-026-1	Comment Form	04/25/14	06/09/14

UPCOMING EVENTS

Webinars/Technical Conferences

- NEW Project 2010-13.3 Phase 3 of Relay Loadability: Stable Power Swings Webinar – Noon-2 p.m. Eastern, May 12, 2014 (Register)
- NEW Project 2007-17.3 - Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays) Webinar – 1-3 p.m. Eastern, May 15, 2014 (Register)
- NEW Project 2013-03 - Geomagnetic Disturbance Mitigation Technical Conference – 8:30-4 p.m. Eastern, May 20, 2014, Atlanta, GA (In-Person Registration) (Webinar Registration) (Details)

Drafting Team Meetings

The Standards calendar provides dial-in information for the in-person meetings below. The calendar also provides information about conference calls that drafting teams may hold in addition to in-person meetings.

- Project 2008-02 - Undervoltage Load Shedding – May 5-7, 2014, Atlanta, GA (Register) (Details) (Agenda)
- Project 2014-02 - Critical Infrastructure Protection Standards Version 5 Revisions – May 12-14, 2014, Columbus, OH (Register) (Details)
  - A meeting and conference call schedule has been posted to the Related Files portion of the project page.
- Project 2009-03 - Emergency Operations – May 13-15, 2014, Dallas, TX (Register) (Details) (Agenda)
- **NEW** Project 2010-05.2 - Special Protection Systems - Phase 2 of Protection Systems – May 20-22, 2014, Denver, CO (Registration and Details)
- Project 2010-02 - Connecting New Facilities to the Grid – May 21-22, 2014, San Francisco, CA (Register) (Details)
- **NEW** Project 2014-01 - Standards Applicability for Dispersed Generation Resources – May 28-29, 2014, Salt Lake City, UT (Register) (Details)
- **NEW** Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves – May 28-30, 2014, Atlanta, GA (Register)
- **NEW** Project 2013-03 - Geomagnetic Disturbance Mitigation – June 2-4, 2014, Atlanta, GA (Register) (Details)
- **NEW** Project 2010-13.3 - Relay Loadability: Stable Power Swings – June 16-20, 2014, Westminster, CO (Register) (Details) (Agenda)

Standards Committee Meetings and Conference Calls

The Standards calendar provides dial-in information for the meetings and calls below. The calendar also provides information about Project Management and Oversight Subcommittee and Process Subcommittee meetings and calls.

- Standards Committee Conference Call – 1-5 p.m. Eastern, May 14, 2014
- Standards Committee In-Person Meeting – June 10-11, 2014, Denver, CO
- Standards Committee Conference Call – 1-5 p.m. Eastern, July 16, 2014

RESOURCES POSTED LAST WEEK

Webinar Slides and Recordings

- Project 2014-01 - Standards Applicability for Dispersed Generation Resources – April 28, 2014 (Presentation) (Recording)
- Project 2010-02 - Connecting New Facilities to the Grid – April 29, 2014 (Presentation) (Recording)

Drafting Team Meeting Notes

- Project 2014-04 - Physical Security – April 2-3, 2014 (Meeting Notes)

OTHER

NEW NERC News Posted

The April issue of NERC News has been posted to the Newsroom web page.

NEW ERO Enterprise Compliance Auditor Manual Posted

NERC posted version 1 of the ERO Enterprise Compliance Auditor Manual (Manual), which was developed by NERC and the Regional Entities to help improve consistency and quality of compliance monitoring across the ERO. The Manual contains common tools, techniques, and approaches for Compliance Auditors. It is a living document, and revisions will occur as NERC and the Regional Entities improve, develop, and implement compliance monitoring processes. NERC and the Regional Entities will begin using the Manual and address update needs and other content in future versions. The Manual will be a public document posted on the NERC website under Compliance & Enforcement/Compliance Tools and Auditor Resources.

In addition to the release of the Manual, NERC posted a Manual Navigation Guide to provide information on the functionality of the Manual and to help users navigate through the document.

New Balloting and Commenting Software System: Practice Balloting and Commenting Events

NERC recently launched a new balloting and commenting software system (the Standards Balloting System or SBS). Please take this opportunity to register in the SBS if you have not already done so, and once registered, access the sample practice ballots on the Balloting and Commenting web page. The first projects will be balloted in the SBS next month; taking a few minutes during this time period to practice the steps needed to submit a vote and comment will make your balloting experience for the first live ballots an easier transition.

The sample practice ballots are open at staggered time periods, allowing ample opportunity to vote and comment. Practice is just a few clicks away:

- Access the **SBS system**
- Click on '**View Ballot Events'** to practice submitting a vote

- Click on '**View Surveys'** to practice submitting comments and accessing Social Survey

Gaining familiarity with the new features and functionality will be very helpful before new projects are open for balloting and commenting in the SBS. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

Helpful Tools:
Standards Balloting and Commenting System (SBS) Login, Registration, Validation and Permissions
Standards Balloting and Commenting System (SBS) Webinar
Frequently Asked Questions
Register for the NEW Registered Ballot Body

***Note**: If you are currently registered in the original NERC Registered Ballot Body, you will need to register for the SBS to vote and comment.*

Northeast Power Coordinating Council (NPCC) Regional Standards Processes Manual Posted for Comment

NERC posted the proposed NPCC's Regional Standards Processes Manual for a 45-day industry review through **8 p.m. Eastern on Wednesday, May 7, 2014**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the Regional Reliability Standards-Under Development Page.

NEW Western Electricity Coordinating Council (WECC) Reliability Development Procedures and Common Attributes Posted for Comment

NERC posted WECC's Reliability Standards Development Procedures & Exhibit C – Common Attributes for a 45-day industry review through **8 p.m. Eastern on Thursday, June 12, 2014.** Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the Regional Reliability Standards-Under Development Page.

ABOUT THE BULLETIN

This weekly bulletin compiles a list of Standards work with actionable deadlines, upcoming Standards events, recently posted standards resources, and other news and information relevant to NERC Standards development. Please email Wendy Muller with questions about commenting and balloting and Mallory Huggins with feedback on this bulletin. The current bulletin and old bulletins are available under "Program News" on the Standards home page.

QUICK LINKS

Ballot Results
Projected Standards Posting Schedule
Project Tracking Spreadsheet
2014-2016 Reliability Standards Development Plan

If you would like to receive this bulletin or be added to the distribution list for a particular project, please email Wendy Muller.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment November 20 – December 19, 2013.

Description of Current Draft

This version of PRC-005 contains revisions to the ~~-~~a ~~A~~pplicability ~~section~~ of the Standard intended to clarify application of ~~the~~ its Requirements to Bulk Electric System dispersed power producing resources. PRC-005-3, a~~A~~ subsequent version of PRC-005, ~~PRC-005-3,~~ has been adopted by the NERC Board of Trustees and is pending regulatory approval. Depending on the timing of regulatory approval, this interim version, which has been labeled PRC-005-2(X) for balloting purposes, may be filed for regulatory approval. The Protection System Maintenance and Testing Standard Drafting Team (PSMT SDT) is concurrently making technical revisions to PRC-005 in Project 2007-17.3 to address FERC directives. Project 2014-01 does not have in its scope any technical content changes beyond revising the applicability to ensure consistent application of the Requirements of PRC-005 to dispersed power-producing resources.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Initial Ballot	June – July 2014
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	August – September 2014
Final ballot	October 2014
BOT adoption	November 2014

When this standard has received ballot approval, the text boxes within the Applicability section of the Standard will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: **Protection System Maintenance**

2. Number: PRC-005-~~2~~ X

3. Purpose: To document and implement programs for the maintenance of all Protection Systems affecting the reliability of the Bulk Electric System (BES) so that these Protection Systems are kept in working order.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner

4.1.2 Generator Owner

4.1.3 Distribution Provider

4.2. Facilities:

4.2.1 Protection Systems that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)

4.2.2 Protection Systems used for underfrequency load-shedding systems installed per ERO underfrequency load-shedding requirements.

4.2.3 Protection Systems used for undervoltage load-shedding systems installed to prevent system voltage collapse or voltage instability for BES reliability.

4.2.4 Protection Systems installed as a Special Protection System (SPS) for BES reliability.

The only revisions made to this version of PRC-005 are revisions to section 4.2, to clarify applicability of the Requirements of the standard at generator Facilities. These applicability revisions are intended to clarify and provide for consistent application of the Requirements to BES generator Facilities included in the BES through Inclusion I4 – Dispersed Power Producing Resources.

This version is labeled PRC-005-2(X) for balloting purposes. The 'X' indicates that a version number will be applied at a later time, because multiple versions of PRC-005 are in development to reflect the fact that applicability changes need apply for versions of the standard that are approved (PRC-005-2), pending regulatory approval (PRC-005-3), and in development in Project 2007-17.3. Depending on the timing of approvals of other versions, NERC may file this interim version to provide regulatory certainty for entities as the revised BES definition is implemented.

4.2.5 Protection Systems for the following BES generator Facilities ~~that are part of the BES, including~~ for generators not identified through Inclusion I4 of the BES definition:

4.2.5.1 Protection Systems that act to trip the generator either directly or via lockout or auxiliary tripping relays.

4.2.5.2 Protection Systems for generator step-up transformers for generators that are part of the BES.

~~**4.2.5.3** Protection Systems for transformers connecting aggregated generation, where the aggregated generation is part of the BES (e.g., transformers connecting facilities such as wind-farms to the BES).~~

~~**4.2.5.4**~~**4.2.5.3** Protection Systems for station service or excitation transformers connected to the generator bus of generators which are part of the BES, that act to trip the generator either directly or via lockout or tripping auxiliary relays.

Rationale for 4.2.5: In order to differentiate between typical BES generator Facilities and BES generators at dispersed power producing facilities, section 4.2.5 was separated into two sections (4.2.5 and 4.2.6). The applicability to non-dispersed power producing Facilities has been maintained and can be found in 4.2.5. The applicability to dispersed power producing Facilities has been modified and relocated from 4.2.5 to 4.2.6.

4.2.6 Protection Systems for the following BES generator Facilities for dispersed power producing resources identified through Inclusion I4 of the BES definition:

4.2.6.1 Protection Systems for ~~electrical equipment~~Facilities used in aggregating dispersed BES generation from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above.

Rationale for 4.2.6: Applicability of the Requirements of PRC-005-2 to dispersed power producing resources is separated out in section 4.2.6. The intent is that for such resources, the Requirements would apply only to Protection Systems on equipment used in aggregating the BES dispersed power producing resources from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or higher including the Protection Systems for those transformers used in aggregating generation.

5. Effective Date: See Implementation Plan.

B. Requirements

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a Protection System Maintenance Program (PSMP) for its Protection Systems identified in Section 4.2. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

The PSMP shall:

1.1. Identify which maintenance method (time-based, performance-based per PRC-005 Attachment A, or a combination) is used to address each Protection System Component Type. All batteries associated with the station dc supply Component Type of a Protection System shall be included in a time-based program as described in Table 1-4 and Table 3.

Component Type *- Any one of the five specific ~~elements~~elements of the Protection System*

1.2. Include the applicable monitored Component attributes applied to each Protection System Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, and Table 3 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System Components.

Component – *A component is any individual discrete piece of equipment included in a Protection System, including but not limited to a protective relay or current sensing device. The designation of what constitutes a control circuit component is very dependent upon how an entity performs and tracks the testing of the control circuitry. Some entities test their control circuits on a breaker basis whereas others test their circuitry on a local zone of protection basis. Thus, entities are allowed the latitude to designate their own definitions of control circuit components. Another example of where the entity has some discretion on determining what constitutes a single component is the voltage and current sensing devices, where the entity may choose either to designate a full three-phase set of such devices or a single device as a single component.*

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals in its PSMP shall follow the procedure established in PRC-005 Attachment A to establish and maintain its performance-based intervals. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall maintain its Protection System Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall implement and follow its PSMP for its Protection System Components that are included within the performance-based program(s). *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

Unresolved Maintenance Issue *- A deficiency identified during a maintenance activity that causes the component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up corrective action.*

R5. Each Transmission Owner, Generator Owner, and Distribution Provider shall demonstrate efforts to correct identified Unresolved Maintenance Issues. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

C. Measures

M1. Each Transmission Owner, Generator Owner and Distribution Provider shall have a documented Protection System Maintenance Program in accordance with Requirement R1.

For each Protection System Component Type, the documentation shall include the type of maintenance method applied (time-based, performance-based, or a combination of these maintenance methods), and shall include all batteries associated with the station dc supply Component Types in a time-based program as described in Table 1-4 and Table 3. (Part 1.1)

For Component Types that use monitoring to extend the maintenance intervals, the responsible entity(s) shall have evidence for each protection Component Type (such as manufacturer's specifications or engineering drawings) of the appropriate monitored Component attributes as specified in Tables 1-1 through 1-5, Table 2, and Table 3. (Part 1.2)

M2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals shall have evidence that its current performance-based maintenance program(s) is in accordance with Requirement R2, which may include but is not limited to Component lists, dated maintenance records, and dated analysis records and results.

M3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System Components included within its time-based program in accordance with Requirement R3. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance intervals in accordance with Requirement R2 shall have evidence that it has implemented the Protection System Maintenance Program for the Protection System Components included in its performance-based program in accordance with Requirement R4. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence that it has undertaken efforts to correct identified Unresolved Maintenance Issues in accordance with Requirement R5. The evidence may include but is not limited to work orders, replacement Component orders, invoices, project schedules with completed milestones, return material authorizations (RMAs) or purchase orders.

D. Compliance

1. Compliance Monitoring Process

~~**1.1. Compliance Enforcement Authority**~~

1.1.

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards

~~Regional Entity~~

1.2. Compliance Monitoring and Enforcement Processes:

Compliance Audit

Self-Certification

Spot Checking
Compliance Investigation
Self-Reporting
Complaint

1.3. Evidence Retention

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

The Transmission Owner, Generator Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

For Requirement R1, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep its current dated Protection System Maintenance Program, as well as any superseded versions since the preceding compliance audit, including the documentation that specifies the type of maintenance program applied for each Protection System Component Type.

For Requirement R2, Requirement R3, Requirement R4, and Requirement R5, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the two most recent performances of each distinct maintenance activity for the Protection System Component, or all performances of each distinct maintenance activity for the Protection System Component since the previous scheduled audit date, whichever is longer.

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

1.4. Additional Compliance Information

None.

2. Violation Severity Levels

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The responsible entity's PSMP failed to specify whether one Component Type is being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1) OR The responsible entity's PSMP failed to include applicable station batteries in a time-based program. (Part 1.1)	The responsible entity's PSMP failed to specify whether two Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1)	The responsible entity's PSMP failed to include the applicable monitoring attributes applied to each Protection System Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, and Table 3 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System Components. (Part 1.2).	The responsible entity failed to establish a PSMP. OR The responsible entity failed to specify whether three or more Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1).
R2	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within three years.	NA	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within four years.	The responsible entity uses performance-based maintenance intervals in its PSMP but: 1) Failed to establish the technical justification described within Requirement R2 for the initial use of the performance-based PSMP OR 2) Failed to reduce Countable Events to no more than 4% within five years OR 3) Maintained a Segment with less than 60 Components OR 4) Failed to: • Annually update the list of Components, OR

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Annually perform maintenance on the greater of 5% of the segment population or 3 Components, OR • Annually analyze the program activities and results for each Segment.
R3	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain 5% or less of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain more than 15% of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.
R4	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain 5% or less of the annual scheduled maintenance for a specific Protection System Component Type in accordance with their performance-based PSMP.	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the annual scheduled maintenance for a specific Protection System Component Type in accordance with their performance-based PSMP.	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the annual scheduled maintenance for a specific Protection System Component Type in accordance with their performance-based PSMP.	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 15% of the annual scheduled maintenance for a specific Protection System Component Type in accordance with their performance-based PSMP.
R5	The responsible entity failed to undertake efforts to correct 5 or	The responsible entity failed to undertake efforts to correct greater than 5, but less than or equal to 10	The responsible entity failed to undertake efforts to correct greater than 10, but less than or equal to 15	The responsible entity failed to undertake efforts to correct greater

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
	fewer identified Unresolved Maintenance Issues.	identified Unresolved Maintenance Issues.	identified Unresolved Maintenance Issues.	than 15 identified Unresolved Maintenance Issues.

E. Regional Variances

None

F. Supplemental Reference Document

The following documents present a detailed discussion about determination of maintenance intervals and other useful information regarding establishment of a maintenance program.

1. PRC-005-2 Protection System Maintenance Supplementary Reference and FAQ — July 2012.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. 3. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/05
1a	February 17, 2011	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers	Project 2009-17 interpretation
1a	February 17, 2011	Adopted by Board of Trustees	
1a	September 26, 2011	FERC Order issued approving interpretation of R1 and R2 (FERC's Order is effective as of September 26, 2011)	
1.1a	February 1, 2012	Errata change: Clarified inclusion of generator interconnection Facility in Generator Owner's responsibility	Revision under Project 2010-07
1b	February 3, 2012	FERC Order issued approving interpretation of R1, R1.1, and R1.2 (FERC's Order dated March 14, 2012). Updated version from 1a to 1b.	Project 2009-10 Interpretation
1.1b	April 23, 2012	Updated standard version to 1.1b to reflect FERC approval of PRC-005-1b.	Revision under Project 2010-07

Version	Date	Action	Change Tracking
1.1b	May 9, 2012	PRC-005-1.1b was adopted by the Board of Trustees as part of Project 2010-07 (GOTO).	
2	November 7, 2012	Adopted by Board of Trustees	Complete revision, absorbing maintenance requirements from PRC-005-1b, PRC-008-0, PRC-011-0, PRC-017-0
2	October 17, 2013	Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase "or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;" to the second sentence under the "Retirement of Existing Standards" section.	
2	December 19, 2013	FERC Order issued approving PRC-005-2. (The enforcement date for PRC-005-2 will be April 1, 2015, which is the first date entities must be compliant with part of the standard. The implementation plan for PRC-005-2 includes specific compliance dates and timeframes for each of the Requirements. The regulatory approval date in the U.S. is February 24, 2014.	
TBD (balloted as 2(X)	TBD	~~.~~Standard revised in Project 2014-01~~.~~	Applicability section revised to clarify application of Requirements to BES dispersed power producing resources

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**[1]	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 calendar years	For all unmonitored relays: • Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (see Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. • Alarming for power supply failure (see Table 2).	12 calendar years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.

[1] For the tables in this standard, a calendar year starts on the first day of a new year (January 1) after a maintenance activity has been completed. For the tables in this standard, a calendar month starts on the first day of the first month after a maintenance activity has been completed.

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**[1]	**Maintenance Activities**
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2).	12 calendar years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 1-2 Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.	4 calendar months	Verify that the communications system is functional.
	6 calendar years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2).	12 calendar years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with all of the following: • Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation). (See Table 2) • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).	12 calendar years	Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the Protection System

Table 1-3 Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage and current sensing devices not having monitoring attributes of the category below.	12 calendar years	Verify that current and voltage signal values are provided to the protective relays.
Voltage and Current Sensing devices connected to microprocessor relays with AC measurements are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2).	No periodic maintenance specified	None.

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply using **Vented Lead-Acid (VLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack
	18 Calendar Months -or- 6 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **with Valve Regulated Lead-Acid (VRLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	6 Calendar Months	Inspect: • Condition of all individual units by measuring battery cell/unit internal ohmic values.
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Physical condition of battery rack
	6 Calendar Months -or- 3 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **Nickel-Cadmium (NiCad) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells. • Physical condition of battery rack
	6 Calendar Years	Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(d) Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System station dc supply not using a battery and not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	18 Calendar Months	Inspect: Condition of non-battery based dc supply
	6 Calendar Years	Verify that the dc supply can perform as manufactured when ac power is not present.

Table 1-4(e) Component Type – Protection System Station dc Supply for non-BES Interrupting Devices for SPS, non-distributed UFLS, and non-distributed UVLS systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a SPS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).	When control circuits are verified (See Table 1-5)	Verify Station dc supply voltage.

Table 1-4(f) Exclusions for Protection System Station dc Supply Monitoring Devices and Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2).	No periodic maintenance specified	No periodic verification of station dc supply voltage is required.
Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2).		No periodic inspection of the electrolyte level for each cell is required.
Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2).		No periodic inspection of unintentional dc grounds is required.
Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2).		No periodic verification of float voltage of battery charger is required.
Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2).		No periodic verification of the battery continuity is required.
Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2).		No periodic verification of the intercell and terminal connection resistance is required.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2).		No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2).		No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required.

Table 1-5 Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3) **Note:** Table requirements apply to all Control Circuitry Components of Protection Systems, and SPSs except as noted.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry).	6 calendar years	Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device.
Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 calendar years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with SPS.	12 calendar years	Verify all paths of the control circuits essential for proper operation of the SPS.
Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays.	12 calendar years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with protective functions and/or SPS whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

Table 2 – Alarming Paths and Monitoring In Tables 1-1 through 1-5 and Table 3, alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any alarm path through which alarms in Tables 1-1 through 1-5 and Table 3 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the "Alarm Path with monitoring" category below. Alarms are reported within 24 hours of detection to a location where corrective action can be initiated.	12 Calendar Years	Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated.
Alarm Path with monitoring: The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated.	No periodic maintenance specified	None.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 calendar years	Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self diagnosis and alarming (See Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. Alarming for power supply failure (See Table 2).	12 calendar years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2).	12 calendar years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Voltage and/or current sensing devices associated with UFLS or UVLS systems.	12 calendar years	Verify that current and/or voltage signal values are provided to the protective relays.
Protection System dc supply for tripping non-BES interrupting devices used only for a UFLS or UVLS system.	12 calendar years	Verify Protection System dc supply voltage.
Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-BES interrupting device trip coils).	12 calendar years	Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic).
Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-BES interrupting device trip coils).	12 calendar years	Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices.
Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-BES interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-BES interrupting devices (excludes non-BES interrupting device trip coils).	No periodic maintenance specified	None.
Trip coils of non-BES interrupting devices in UFLS or UVLS systems.	No periodic maintenance specified	None.

PRC-005 — Attachment A

Criteria for a Performance-Based Protection System Maintenance Program

Purpose: To establish a technical basis for initial and continued use of a performance-based Protection System Maintenance Program (PSMP).

To establish the technical justification for the initial use of a performance-based PSMP:

1. Develop a list with a description of Components included in each designated Segment of the Protection System Component population, with a minimum **Segment** population of 60 Components.
2. Maintain the Components in each Segment according to the time-based maximum allowable intervals established in Tables 1-1 through 1-5 and Table 3 until results of maintenance activities for the Segment are available for a minimum of 30 individual Components of the Segment.
3. Document the maintenance program activities and results for each Segment, including maintenance dates and Countable Events for each included Component.
4. Analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment and develop maintenance intervals.
5. Determine the maximum allowable maintenance interval for each Segment such that the Segment experiences **Countable Events** on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

> **Segment** – *Protection Systems or components of a consistent design standard, or a particular model or type from a single manufacturer that typically share other common elements. Consistent performance is expected across the entire population of a Segment. A Segment must contain at least sixty (60) individual components.*

> **Countable Event** – *A failure of a component requiring repair or replacement, any condition discovered during the maintenance activities in Tables 1-1 through 1-5 and Table 3 which requires corrective action, or a Misoperation attributed to hardware failure or calibration failure. Misoperations due to product design errors, software errors, relay settings different from specified settings, Protection System component configuration errors, or Protection System application errors are not included in Countable Events.*

To maintain the technical justification for the ongoing use of a performance-based PSMP:

1. At least annually, update the list of Protection System Components and Segments and/or description if any changes occur within the Segment.
2. Perform maintenance on the greater of 5% of the Components (addressed in the performance based PSMP) in each Segment or 3 individual Components within the Segment in each year.
3. For the prior year, analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment.

4. Using the prior year's data, determine the maximum allowable maintenance interval for each Segment such that the Segment experiences Countable Events on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.
5. If the Components in a Protection System Segment maintained through a performance-based PSMP experience 4% or more Countable Events, develop, document, and implement an action plan to reduce the Countable Events to less than 4% of the Segment population within 3 years.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment November 20 – December 19, 2013.

Description of Current Draft

~~The Protection System Maintenance and Testing Standard Drafting Team (PSMT SDT) is posting draft 1 of PRC-005-X for a 45-day comment period and ballot in the last ten days of the comment period under the new Standards Process Manual (Effective: June 26, 2013).~~

~~This draft contains the technical content of the standard.~~ ~~A parallel effort in the~~ The Project 2014-01, Standards Applicability for Dispersed Generation Resources Standards Drafting Team (DGR SDT)~~,~~ ~~will~~ is posting proposed ~~an~~ applicability changes to ~~PRC-005-2 and~~ PRC-005-3 for comment and ballot. This draft contains the DGR SDT's recommended changes within ~~technical content of~~ the standard. Project 2014-01 does not have in its scope any technical content changes beyond revising the applicability to ensure consistent application of the Requirements of PRC-005 to dispersed power-producing resources.

In a parallel effort, the Protection System Maintenance and Testing Standard Drafting Team (PSMT SDT) has posted draft 1 of PRC-005-X for a 45-day comment period, and ballot in the last ten days of the comment period under the new Standards Process Manual (Effective: June 26, 2013).

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Initial Ballot	June – July 2014
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	August – September 2014
Final ballot	October 2014
BOT adoption	November 2014

When this standard has received ballot approval, the text boxes within the Applicability section of the Standard will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: **Protection System and Automatic Reclosing Maintenance**

2. Number: PRC-005-3(X)

3. Purpose: To document and implement programs for the maintenance of all Protection Systems and Automatic Reclosing affecting the reliability of the Bulk Electric System (BES) so that they are kept in working order.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner

4.1.2 Generator Owner

4.1.3 Distribution Provider

4.2. Facilities:

4.2.1 Protection Systems that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)

4.2.2 Protection Systems used for underfrequency load-shedding systems installed per ERO underfrequency load-shedding requirements.

4.2.3 Protection Systems used for undervoltage load-shedding systems installed to prevent system voltage collapse or voltage instability for BES reliability.

4.2.4 Protection Systems installed as a Special Protection System (SPS) for BES reliability.

The only revisions made to this version of PRC-005 are revisions to section 4.2, to clarify applicability of the Requirements of the standard at generator Facilities. These applicability revisions are intended to clarify and provide for consistent application of the Requirements to BES generator Facilities included in the BES through Inclusion I4 – Dispersed Power Producing Resources.

This version is labeled PRC-005-3(X) for balloting purposes. The 'X' indicates that a version number will be applied at a later time, because multiple versions of PRC-005 are in development to reflect the fact that applicability changes need apply for versions of the standard that are approved (PRC-005-2), pending regulatory approval (PRC-005-3), and in development in Project 2007-17.3.

4.2.5 Protection Systems for the following BES generator Facilities ~~that are part of the BES, including~~ for generators not identified through Inclusion I4 of the BES definition:

4.2.5.1 Protection Systems that act to trip the generator either directly or via lockout or auxiliary tripping relays.

4.2.5.2 Protection Systems for generator step-up transformers for generators that are part of the BES.

~~**4.2.5.3** Protection Systems for transformers connecting aggregated generation, where the aggregated generation is part of the BES (e.g., transformers connecting facilities such as wind-farms to the BES).~~

~~**4.2.5.4**~~**4.2.5.3** Protection Systems for station service or excitation transformers connected to the generator bus of generators which are part of the BES, that act to trip the generator either directly or via lockout or tripping auxiliary relays.

Rationale for 4.2.5: In order to differentiate between typical BES generator Facilities and BES generators at dispersed power producing facilities, section 4.2.5 was separated into two sections (4.2.5 and 4.2.6). The applicability to non-dispersed power producing Facilities has been maintained and can be found in 4.2.5. The applicability to dispersed power producing Facilities has been modified and relocated from 4.2.5 to 4.2.6.

4.2.6 Protection Systems for the following BES generator Facilities for dispersed power producing resources identified through Inclusion I4 of the BES definition:

4.2.6.1 Protection Systems for ~~electrical equipment~~Facilities used in aggregating dispersed BES generation from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above.

Rationale for 4.2.6: Applicability of the Requirements of PRC-005-2 to dispersed power producing resources is separated out in section 4.2.6. The intent is that for such resources, the Requirements would apply ~~-~~only to Protection Systems on equipment used in aggregating the BES dispersed power producing resources from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or higher including the Protection Systems for those transformers used in aggregating generation.

~~4.2.6~~4.2.7 Automatic Reclosing[1], including:

~~4.2.6.1~~4.2.7.1 Automatic Reclosing applied on the terminals of Elements connected to the BES bus located at generating plant substations where the total installed gross generating plant capacity is greater than the gross capacity of the largest BES generating unit within the Balancing Authority Area.

~~4.2.6.2~~4.2.7.2 Automatic Reclosing applied on the terminals of all BES Elements at substations one bus away from generating plants specified in Section 4.2.6.1 when the substation is less than 10 circuit-miles from the generating plant substation.

~~4.2.6.3~~4.2.7.3 Automatic Reclosing applied as an integral part of an SPS specified in Section 4.2.4.

5. Effective Date: See Implementation Plan.

6. Definitions Used in this Standard: The following terms are defined for use only within PRC-005-3, and should remain with the standard upon approval rather than being moved to the Glossary of Terms.

Automatic Reclosing – Includes the following Components:

- Reclosing relay
- Control circuitry associated with the reclosing relay.

Unresolved Maintenance Issue – A deficiency identified during a maintenance activity that causes the component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up corrective action.

Segment – Components of a consistent design standard, or a particular model or type from a single manufacturer that typically share other common elements. Consistent performance is expected across the entire population of a Segment. A Segment must contain at least sixty (60) individual Components.

Component Type – Either any one of the five specific elements of the Protection System definition or any one of the two specific elements of the Automatic Reclosing definition.

Component – A Component is any individual discrete piece of equipment included in a Protection System or in Automatic Reclosing, including but not limited to a protective relay, reclosing relay, or current sensing device. The designation of what constitutes a control circuit

[1] Automatic Reclosing addressed in Section 4.2.6.1 and 4.2.6.2 may be excluded if the equipment owner can demonstrate that a close-in three-phase fault present for twice the normal clearing time (capturing a minimum trip-close-trip time delay) does not result in a total loss of gross generation in the Interconnection exceeding the gross capacity of the largest BES generating unit within the Balancing Authority Area where the Automatic Reclosing is applied.

Component is dependent upon how an entity performs and tracks the testing of the control circuitry. Some entities test their control circuits on a breaker basis whereas others test their circuitry on a local zone of protection basis. Thus, entities are allowed the latitude to designate their own definitions of control circuit Components. Another example of where the entity has some discretion on determining what constitutes a single Component is the voltage and current sensing devices, where the entity may choose either to designate a full three-phase set of such devices or a single device as a single Component.

Countable Event – A failure of a Component requiring repair or replacement, any condition discovered during the maintenance activities in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 which requires corrective action or a Protection System Misoperation attributed to hardware failure or calibration failure. Misoperations due to product design errors, software errors, relay settings different from specified settings, Protection System Component or Automatic Reclosing configuration or application errors are not included in Countable Events.

B. Requirements

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a Protection System Maintenance Program (PSMP) for its Protection Systems and Automatic Reclosing identified in Facilities Section 4.2. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

The PSMP shall:

1.1. Identify which maintenance method (time-based, performance-based per PRC-005 Attachment A, or a combination) is used to address each Protection System and Automatic Reclosing Component Type. All batteries associated with the station dc supply Component Type of a Protection System shall be included in a time-based program as described in Table 1-4 and Table 3.

1.2. Include the applicable monitored Component attributes applied to each Protection System and Automatic Reclosing Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System and Automatic Reclosing Components.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals in its PSMP shall follow the procedure established in PRC-005 Attachment A to establish and maintain its performance-based intervals. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall maintain its Protection System and Automatic Reclosing Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall implement and follow its PSMP for its Protection System and Automatic Reclosing Components that are included within the performance-based program(s). *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R5. Each Transmission Owner, Generator Owner, and Distribution Provider shall demonstrate efforts to correct identified Unresolved Maintenance Issues. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

C. Measures

M1. Each Transmission Owner, Generator Owner and Distribution Provider shall have a documented Protection System Maintenance Program in accordance with Requirement R1.

For each Protection System and Automatic Reclosing Component Type, the documentation shall include the type of maintenance method applied (time-based, performance-based, or a combination of these maintenance methods), and shall include all batteries associated with the station dc supply Component Types in a time-based program as described in Table 1-4 and Table 3. (Part 1.1)

For Component Types that use monitoring to extend the maintenance intervals, the responsible entity(s) shall have evidence for each Protection System and Automatic Reclosing Component Type (such as manufacturer's specifications or engineering drawings) of the appropriate

monitored Component attributes as specified in Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2. (Part 1.2)

M2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals shall have evidence that its current performance-based maintenance program(s) is in accordance with Requirement R2, which may include but is not limited to Component lists, dated maintenance records, and dated analysis records and results.

M3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System and Automatic Reclosing Components included within its time-based program in accordance with Requirement R3. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance intervals in accordance with Requirement R2 shall have evidence that it has implemented the Protection System Maintenance Program for the Protection System and Automatic Reclosing Components included in its performance-based program in accordance with Requirement R4. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence that it has undertaken efforts to correct identified Unresolved Maintenance Issues in accordance with Requirement R5. The evidence may include but is not limited to work orders, replacement Component orders, invoices, project schedules with completed milestones, return material authorizations (RMAs) or purchase orders.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Compliance Monitoring and Enforcement Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.3. Evidence Retention

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

The Transmission Owner, Generator Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

For Requirement R1, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep its current dated Protection System Maintenance Program, as well as any superseded versions since the preceding compliance audit, including the documentation that specifies the type of maintenance program applied for each Protection System Component Type.

For Requirement R2, Requirement R3, Requirement R4, and Requirement R5, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the two most recent performances of each distinct maintenance activity for the Protection System or Automatic Reclosing Component, or all performances of each distinct maintenance activity for the Protection System or Automatic Reclosing Component since the previous scheduled audit date, whichever is longer.

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

1.4. Additional Compliance Information

None.

2. Violation Severity Levels

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The responsible entity's PSMP failed to specify whether one Component Type is being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1) OR The responsible entity's PSMP failed to include applicable station batteries in a time-based program. (Part 1.1)	The responsible entity's PSMP failed to specify whether two Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1)	The responsible entity's PSMP failed to specify whether three Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1). OR The responsible entity's PSMP failed to include the applicable monitoring attributes applied to each Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Components. (Part 1.2).	The responsible entity failed to establish a PSMP. OR The responsible entity's PSMP failed to specify whether four or more Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1).
R2	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within three years.	NA	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within four years.	The responsible entity uses performance-based maintenance intervals in its PSMP but: 1) Failed to establish the technical justification described within Requirement R2 for the initial use of the performance-based PSMP OR 2) Failed to reduce Countable Events to no more than 4% within five years OR

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
				3) Maintained a Segment with less than 60 Components OR 4) Failed to: • Annually update the list of Components, OR • Annually perform maintenance on the greater of 5% of the Segment population or 3 Components, OR • Annually analyze the program activities and results for each Segment.
R3	For Components included within a time-based maintenance program, the responsible entity failed to maintain 5% or less of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.	For Components included within a time-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.	For Components included within a time-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.	For Components included within a time-based maintenance program, the responsible entity failed to maintain more than 15% of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.
R4	For Components included within a performance-based maintenance program, the responsible entity failed to maintain 5% or less of the annual scheduled maintenance for a specific	For Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the annual scheduled	For Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the annual	For Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 15% of the annual scheduled

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Component Type in accordance with their performance-based PSMP.	maintenance for a specific Component Type in accordance with their performance-based PSMP.	scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP.	maintenance for a specific Component Type in accordance with their performance-based PSMP.
R5	The responsible entity failed to undertake efforts to correct 5 or fewer identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 5, but less than or equal to 10 identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 10, but less than or equal to 15 identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 15 identified Unresolved Maintenance Issues.

E. Regional Variances

None

F. Supplemental Reference Document

The following documents present a detailed discussion about determination of maintenance intervals and other useful information regarding establishment of a maintenance program.

1. PRC-005-2 Protection System Maintenance Supplementary Reference and FAQ — March 2013.
2. Considerations for Maintenance and Testing of Autoreclosing Schemes — November 2012.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. 3. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/05
1a	February 17, 2011	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers	Project 2009-17 interpretation
1a	February 17, 2011	Adopted by Board of Trustees	
1a	September 26, 2011	FERC Order issued approving interpretation of R1 and R2 (FERC's Order is effective as of September 26, 2011)	
1.1a	February 1, 2012	Errata change: Clarified inclusion of generator interconnection Facility in Generator Owner's responsibility	Revision under Project 2010-07
1b	February 3, 2012	FERC Order issued approving interpretation of R1, R1.1, and R1.2 (FERC's Order dated March 14, 2012). Updated version from 1a to 1b.	Project 2009-10 Interpretation
1.1b	April 23, 2012	Updated standard version to 1.1b to reflect FERC approval of PRC-005-1b.	Revision under Project 2010-07

Version	Date	Action	Change Tracking
1.1b	May 9, 2012	PRC-005-1.1b was adopted by the Board of Trustees as part of Project 2010-07 (GOTO).	
2	November 7, 2012	Adopted by Board of Trustees	Project 2007-17 - Complete revision, absorbing maintenance requirements from PRC-005-1.1b, PRC-008-0, PRC-011-0, PRC-017-0
2	October 17, 2013	Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase "or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;" to the second sentence under the "Retirement of Existing	
3	November 7, 2013	Adopted by the NERC Board of Trustees	Revised to address the FERC directive in Order No.758 to include Automatic Reclosing in maintenance programs.
TBD (balloted as 2(X)	TBD	Standard revised in Project 2014-01	Applicability section revised to clarify application of Requirements to BES dispersed power producing resources

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[2]**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	For all unmonitored relays: • Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (see Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. • Alarming for power supply failure (see Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.

[2] For the tables in this standard, a calendar year starts on the first day of a new year (January 1) after a maintenance activity has been completed. For the tables in this standard, a calendar month starts on the first day of the first month after a maintenance activity has been completed.

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[2]**	**Maintenance Activities**
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 1-2 Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.	4 Calendar Months	Verify that the communications system is functional.
	6 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2).	12 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with all of the following: • Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation). (See Table 2) • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).	12 Calendar Years	Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the Protection System

Table 1-3 Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage and current sensing devices not having monitoring attributes of the category below.	12 Calendar Years	Verify that current and voltage signal values are provided to the protective relays.
Voltage and Current Sensing devices connected to microprocessor relays with AC measurements are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2).	No periodic maintenance specified	None.

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply using **Vented Lead-Acid (VLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	18 Calendar Months -or- 6 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **with Valve Regulated Lead-Acid (VRLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	6 Calendar Months	Inspect: • Condition of all individual units by measuring battery cell/unit internal ohmic values.
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Physical condition of battery rack

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	6 Calendar Months -or- 3 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **Nickel-Cadmium (NiCad) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells. • Physical condition of battery rack
	6 Calendar Years	Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(d) Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System station dc supply not using a battery and not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	18 Calendar Months	Inspect: Condition of non-battery based dc supply
	6 Calendar Years	Verify that the dc supply can perform as manufactured when ac power is not present.

Table 1-4(e) Component Type – Protection System Station dc Supply for non-BES Interrupting Devices for SPS, non-distributed UFLS, and non-distributed UVLS systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a SPS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).	When control circuits are verified (See Table 1-5)	Verify Station dc supply voltage.

Table 1-4(f) Exclusions for Protection System Station dc Supply Monitoring Devices and Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2).	No periodic maintenance specified	No periodic verification of station dc supply voltage is required.
Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2).		No periodic inspection of the electrolyte level for each cell is required.
Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2).		No periodic inspection of unintentional dc grounds is required.
Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2).		No periodic verification of float voltage of battery charger is required.
Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2).		No periodic verification of the battery continuity is required.
Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2).		No periodic verification of the intercell and terminal connection resistance is required.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2).		No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2).		No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required.

Table 1-5 Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3) Note: Table requirements apply to all Control Circuitry Components of Protection Systems, and SPSs except as noted.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device.
Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with SPS. (See Table 4-2(b) for SPS which include Automatic Reclosing.)	12 Calendar Years	Verify all paths of the control circuits essential for proper operation of the SPS.
Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays.	12 Calendar Years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with protective functions and/or SPSs whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

Table 2 – Alarming Paths and Monitoring In Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2, alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any alarm path through which alarms in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the "Alarm Path with monitoring" category below. Alarms are reported within 24 hours of detection to a location where corrective action can be initiated.	12 Calendar Years	Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated.
Alarm Path with monitoring: The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated.	No periodic maintenance specified	None.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate. For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self diagnosis and alarming (See Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Voltage and/or current sensing devices associated with UFLS or UVLS systems.	12 Calendar Years	Verify that current and/or voltage signal values are provided to the protective relays.
Protection System dc supply for tripping non-BES interrupting devices used only for a UFLS or UVLS system.	12 Calendar Years	Verify Protection System dc supply voltage.
Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic).
Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices.
Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-BES interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-BES interrupting devices (excludes non-BES interrupting device trip coils).	No periodic maintenance specified	None.
Trip coils of non-BES interrupting devices in UFLS or UVLS systems.	No periodic maintenance specified	None.

Table 4-1 Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Reclosing Relay		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored reclosing relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.
Monitored microprocessor reclosing relay with the following: • Internal self diagnosis and alarming (See Table 2). • Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.

Table 4-2(a) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing Relays that are NOT an Integral Part of an SPS		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Unmonitored Control circuitry associated with Automatic Reclosing that is not an integral part of an SPS.	12 Calendar Years	Verify that Automatic Reclosing, upon initiation, does not issue a premature closing command to the close circuitry.
Control circuitry associated with Automatic Reclosing that is not part of an SPS and is monitored and alarmed for conditions that would result in a premature closing command. (See Table 2)	No periodic maintenance specified	None.

Table 4-2(b) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing Relays that ARE an Integral Part of an SPS		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Close coils or actuators of circuit breakers or similar devices that are used in conjunction with Automatic Reclosing as part of an SPS (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each close coil or actuator is able to operate the circuit breaker or mitigating device.
Unmonitored close control circuitry associated with Automatic Reclosing used as an integral part of an SPS.	12 Calendar Years	Verify all paths of the control circuits associated with Automatic Reclosing that are essential for proper operation of the SPS.
Control circuitry associated with Automatic Reclosing that is an integral part of an SPS whose integrity is monitored and alarmed. (See Table 2)	No periodic maintenance specified	None.

PRC-005 — Attachment A

Criteria for a Performance-Based Protection System Maintenance Program

Purpose: To establish a technical basis for initial and continued use of a performance-based Protection System Maintenance Program (PSMP).

To establish the technical justification for the initial use of a performance-based PSMP:

1. Develop a list with a description of Components included in each designated Segment, with a minimum **Segment** population of 60 Components.
2. Maintain the Components in each Segment according to the time-based maximum allowable intervals established in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 until results of maintenance activities for the Segment are available for a minimum of 30 individual Components of the Segment.
3. Document the maintenance program activities and results for each Segment, including maintenance dates and Countable Events for each included Component.
4. Analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment and develop maintenance intervals.
5. Determine the maximum allowable maintenance interval for each Segment such that the Segment experiences **Countable Events** on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

To maintain the technical justification for the ongoing use of a performance-based PSMP:

1. At least annually, update the list of Components and Segments and/or description if any changes occur within the Segment.
2. Perform maintenance on the greater of 5% of the Components (addressed in the performance based PSMP) in each Segment or 3 individual Components within the Segment in each year.
3. For the prior year, analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment.
4. Using the prior year's data, determine the maximum allowable maintenance interval for each Segment such that the Segment experiences Countable Events on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.
5. If the Components in a Segment maintained through a performance-based PSMP experience 4% or more Countable Events, develop, document, and implement an action plan to reduce the Countable Events to less than 4% of the Segment population within 3 years.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment November 20 – December 19, 2013.

Description of Current Draft

The Project 2014-01, Standards Applicability for Dispersed Generation Resources Standards Drafting Team (DGR SDT) is posting proposed applicability changes to PRC-005-3 for comment and ballot. This draft contains the DGR SDT's recommended changes within the standard, which are intended to clarify application of the Requirements to Bulk Electric System (BES) dispersed power producing resources. Project 2014-01 does not have in its scope any technical content changes beyond revising the applicability to ensure consistent application of the Requirements of PRC-005 to dispersed power-producing resources.

In a parallel effort, the Protection System Maintenance and Testing Standard Drafting Team (PSMT SDT) has posted draft 1 of PRC-005-X for a 45-day comment period, and ballot in the last ten days of the comment period under the new Standards Process Manual (Effective: June 26, 2013).

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Initial Ballot	June – July 2014
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	August – September 2014
Final ballot	October 2014
BOT adoption	November 2014

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms (Glossary) are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, this defined term will be removed from the individual standard and added to the Glossary.

Protection System Maintenance Program (PSMP) — An ongoing program by which Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components are kept in working order and proper operation of malfunctioning components is restored. A maintenance program for a specific Component includes one or more of the following activities:

- Verify — Determine that the Component is functioning correctly.
- Monitor — Observe the routine in-service operation of the Component.
- Test — Apply signals to a Component to observe functional performance or output behavior, or to diagnose problems.
- Inspect — Examine for signs of Component failure, reduced performance or degradation.
- Calibrate — Adjust the operating threshold or measurement accuracy of a measuring element to meet the intended performance requirement.

See Section A.6, Definitions Used in this Standard, for additional definitions that are new or modified for use within this standard.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** **Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance**
2. **Number:** **PRC-005-X**
3. **Purpose:** To document and implement programs for the maintenance of all Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying affecting the reliability of the Bulk Electric System (BES) so that they are kept in working order.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1** Transmission Owner
     - **4.1.2** Generator Owner
     - **4.1.3** Distribution Provider
     - **4.1.4** Balancing Authority
   - **4.2. Facilities:**
     - **4.2.1** Protection Systems and Sudden Pressure Relaying that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)
     - **4.2.2** Protection Systems used for underfrequency load-shedding systems installed per ERO underfrequency load-shedding requirements.
     - **4.2.3** Protection Systems used for undervoltage load-shedding systems installed to prevent system voltage collapse or voltage instability for BES reliability.
     - **4.2.4** Protection Systems installed as a Special Protection System (SPS) for BES reliability.
     - **4.2.5** Protection Systems for the following BES generator Facilities ~~that are part of the BES, including~~ for generators not identified through Inclusion I4 of the BES definition:

The only revisions made to this version of PRC-005 are revisions to section 4.2, to clarify applicability of the Requirements of the standard at generator Facilities. These applicability revisions are intended to clarify and provide for consistent application of the Requirements to BES generator Facilities included in the BES through Inclusion I4 – Dispersed Power Producing Resources.

This version is labeled PRC-005-~~2(~~X~~)~~ for balloting purposes. The 'X' indicates that a version number will be applied at a later time, because multiple versions of PRC-005 are in development to reflect the fact that applicability changes need applied~~y~~ for versions of the standard that are approved (PRC-005-2), pending regulatory approval (PRC-005-3), and in development in Project 2007-17.3. ~~-~~Depending on the timing of approvals of other versions, NERC may file this interim version to provide regulatory certainty for entities as the revised BES definition is implemented.

4.2.5.1 Protection Systems that act to trip the generator either directly or via lockout or auxiliary tripping relays.

4.2.5.2 Protection Systems and Sudden Pressure Relaying for generator step-up transformers for generators that are part of the BES.

~~**4.2.5.3** Protection Systems for transformers connecting aggregated generation, where the aggregated generation is part of the BES (e.g., transformers connecting facilities such as wind farms to the BES).~~

4.2.5.3 Protection Systems and Sudden Pressure Relaying for station service or excitation transformers connected to the generator bus of generators which are part of the BES, that act to trip the generator either directly or via lockout or tripping auxiliary relays.

Rationale for 4.2.5: In order to differentiate between typical BES generator Facilities and BES generators at dispersed power producing facilities, section 4.2.5 was separated into two sections (4.2.5 and 4.2.6). The applicability to non-dispersed power producing facilities has been maintained and can be found in 4.2.5. The applicability to dispersed power producing Facilities has been modified and relocated from 4.2.5 to 4.2.6.

4.2.6 Protection Systems for the following BES generator Facilities for dispersed power producing resources identified through Inclusion I4 of the BES definition:

4.2.6.1 Protection Systems for ~~electrical equipment~~Facilities- used in aggregating dispersed BES generation from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above.

Rationale for 4.2.6: The Facilities listed that are applicable to dispersed power producing facilities are covered within 4.2.6. The intent is to NOT include the individual generating resources in the Protection System Maintenance Program, and as such the Protection Systems within the individual generating resources would not be within the scope of PRC-005. Only Protection Systems on equipment used in aggregating the dispersed BES generation from the point where those resources aggregate to greater than 75MVA to a common point of connection at 100kV would be included in the Protection System Maintenance Program, including the Protection Systems for those transformers used in aggregating generation.

~~4.2.6~~4.2.7 Automatic Reclosing[1], including:

~~4.2.6.1~~4.2.7.1 Automatic Reclosing applied on the terminals of Elements connected to the BES bus located at generating plant substations where the total installed gross generating plant capacity is greater than the gross capacity of the largest BES generating unit within the Balancing Authority Area.

~~4.2.6.2~~4.2.7.2 Automatic Reclosing applied on the terminals of all BES Elements at substations one bus away from generating plants specified in Section 4.2.6.1 when the substation is less than 10 circuit-miles from the generating plant substation.

4.2.6.3. Automatic Reclosing applied as an integral part of an SPS specified in Section 4.2.4.

[1] Automatic Reclosing addressed in Section 4.2.7.1 and 4.2.7.2 may be excluded if the equipment owner can demonstrate that a close-in three-phase fault present for twice the normal clearing time (capturing a minimum trip-close-trip time delay) does not result in a total loss of gross generation in the Interconnection exceeding the gross capacity of the largest BES generating unit within the Balancing Authority Area where the Automatic Reclosing is applied.

5. **Effective Date:** See Implementation Plan.

6. **Definitions Used in this Standard:**

Automatic Reclosing – Includes the following Components:

- Reclosing relay
- Control circuitry associated with the reclosing relay.

Sudden Pressure Relaying – A system that trips an interrupting device(s) to isolate the equipment it is monitoring and includes the following Components:

- Fault pressure relay – a mechanical relay or device that detects rapid changes in gas pressure, oil pressure, or oil flow that are indicative of Faults within liquid-filled, wire-wound equipment
- Control circuitry associated with a fault pressure relay

Unresolved Maintenance Issue – A deficiency identified during a maintenance activity that causes the Component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up corrective action.

Segment – Components of a consistent design standard, or a particular model or type from a single manufacturer that typically share other common elements. Consistent performance is expected across the entire population of a Segment. A Segment must contain at least sixty (60) individual Components.

Component Type –

- Any one of the five specific elements of a Protection System.
- Any one of the two specific elements of Automatic Reclosing.
- Any one of the two specific elements of Sudden Pressure Relaying.

Rationale for the deletion of part of the definition of Component: The SDT determined that it was explanatory in nature and adequately addressed in the Supplementary Reference and FAQ Document.

Component – Any individual discrete piece of equipment included in a Protection System, Automatic Reclosing, or Sudden Pressure Relaying.

Countable Event – A failure of a Component requiring repair or replacement, any condition discovered during the maintenance activities in Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-2, and Table 5, which requires corrective action or a Protection System Misoperation attributed to hardware failure or calibration failure. Misoperations due to product design errors, software errors, relay settings different from specified settings, Protection System Component, Automatic Reclosing, or Sudden

Pressure Relaying configuration or application errors are not included in Countable Events.

B. Requirements and Measures

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a Protection System Maintenance Program (PSMP) for its Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying identified in Section 4.2, Facilities. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning*]

The PSMP shall:

1.1. Identify which maintenance method (time-based, performance-based per PRC-005 Attachment A, or a combination) is used to address each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type. All batteries associated with the station dc supply Component Type of a Protection System shall be included in a time-based program as described in Table 1-4 and Table 3.

1.2. Include the applicable monitored Component attributes applied to each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, Table 4-1 through 4-2, and Table 5 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components.

M1. Each Transmission Owner, Generator Owner and Distribution Provider shall have a documented Protection System Maintenance Program in accordance with Requirement R1.

For each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type, the documentation shall include the type of maintenance method applied (time-based, performance-based, or a combination of these maintenance methods), and shall include all batteries associated with the station dc supply Component Types in a time-based program as described in Table 1-4 and Table 3. (Part 1.1)

For Component Types that use monitoring to extend the maintenance intervals, the responsible entity(s) shall have evidence for each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type (such as manufacturer's specifications or engineering drawings) of the appropriate monitored Component attributes as specified in Tables 1-1 through 1-5, Table 2, Table 3, Table 4-1 through 4-2, and Table 5. (Part 1.2)

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals in its PSMP shall follow the procedure

established in PRC-005 Attachment A to establish and maintain its performance-based intervals. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals shall have evidence that its current performance-based maintenance program(s) is in accordance with Requirement R2, which may include, but is not limited to, Component lists, dated maintenance records, and dated analysis records and results.

Rationale for R3 part 3.1 and 3.1.1.: The SDT, upon further reflection, determined that the PRC-005-3 Implementation Plan actually included a requirement that entities with newly-identified Automatic Reclosing Components implement its PSMP for those Components, and therefore determined that it was more appropriate to include this information in the standard rather than the implementation plan.

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall, except as provided in part 3.1, maintain its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Table 4-1 through 4-2, and Table 5. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

3.1. For each newly-identified Automatic Reclosing Component following a notification under Requirement R6, each Transmission Owner, Generator Owner, and Distribution Provider shall perform maintenance activities or provide documentation of prior maintenance activities according to either 3.1.1 or 3.1.2.

3.1.1. Complete the maintenance activities prescribed within Tables 4-1, 4-2(a), and 4-2(b) for the newly-identified Automatic Reclosing Component prior to the end of the third calendar year following the notification under Requirement R6; or

3.1.2. Provide documentation that the Automatic Reclosing Component was last maintained in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 4-1, 4-2(a), and 4-2(b).

M3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components included within its time-based program in accordance with Requirement R3. The evidence may include, but is not limited to, dated maintenance records, dated

maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

Rationale for R4 part 4.1 and 4.1.1.: The SDT, upon further reflection, determined that the PRC-005-3 Implementation Plan actually included a requirement that entities with newly-identified Automatic Reclosing Components implement its PSMP for those Components, and therefore determined that it was more appropriate to include this information in the standard rather than the implementation plan.

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall, except as provided in part 4.1, implement and follow its PSMP for its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components that are included within the performance-based program(s). *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

4.1. For each newly-identified Automatic Reclosing Component following a notification under Requirement R6, each Transmission Owner, Generator Owner, and Distribution Provider shall perform maintenance activities or provide documentation of prior maintenance activities according to either 4.1.1 or 4.1.2.

4.1.1. Complete the maintenance activities prescribed within Tables 4-1, 4-2(a), and 4-2(b) for the newly-identified Automatic Reclosing Component prior to the end of the third calendar year following the notification under Requirement R6; or

4.1.2. Provide documentation that the Automatic Reclosing Component was last maintained in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 4-1, 4-2(a), and 4-2(b).

M4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance intervals in accordance with Requirement R2 shall have evidence that it has implemented the Protection System Maintenance Program for the Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components included in its performance-based program in accordance with Requirement R4. The evidence may include, but is not limited to, dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

R5. Each Transmission Owner, Generator Owner, and Distribution Provider shall demonstrate efforts to correct identified Unresolved Maintenance Issues. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence that it has undertaken efforts to correct identified Unresolved Maintenance

Issues in accordance with Requirement R5. The evidence may include, but is not limited to, work orders, replacement Component orders, invoices, project schedules with completed milestones, return material authorizations (RMAs) or purchase orders.

Rationale for R6: The information addressed in Requirement R6 is necessary for Transmission Owners, Generator Owners, and Distribution Provides to accurately apply Section 4.2.7, Applicability. The Balancing Authority is the entity that maintains the information and should have the responsibility to provide this information to the applicable entities. The drafting team reconsidered the inclusion of the Balancing Authority and determined it is appropriate to include the requirement the standard. This requirement may be relocated to another standard during future reviews of standards for quality and content.

The periodicity was chosen to balance the needs of the Transmission Owner, Generator Owner, and Distribution Provider to obtain the information with the needs of the Balancing Authority to provide an accurate gross capacity (considering retirement or installation of generating units and/or changes in its Balancing Authority Area) in order to properly include Automatic Reclosing in a PSMP.

R6. Each Balancing Authority shall, at least once every calendar year with not more than 15 calendar months between notifications, notify each Transmission Owner, Generator Owner, and Distribution Provider within its Balancing Authority Area of the gross capacity, in MW or MVA, of the largest BES generating unit within the Balancing Authority Area. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M6. Each Balancing Authority shall have dated documentation that it notified each Transmission Owner, Generator Owner, and Distribution Provider in accordance with Requirement R6. Examples of evidence may include, but are not limited to, copies of correspondence, such as e-mails or memoranda.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time

since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Transmission Owner, Generator Owner, Distribution Provider, and Balancing Authority shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

For Requirement R1, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep its current dated Protection System Maintenance Program, as well as any superseded versions since the preceding compliance audit, including the documentation that specifies the type of maintenance program applied for each Protection System Component Type.

For Requirement R2, Requirement R3, Requirement R4, and Requirement R5, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the most recent performance of each distinct maintenance activity for the Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component, or all performances of each distinct maintenance activity for the Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component since the previous scheduled audit date, whichever is longer.

For Requirement R6, the Balancing Authority shall keep documentation for three calendar years that it provided information identifying the largest BES generating unit to the Transmission Owners, Generator Owners, and Distribution Providers in its Balancing Authority Area.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

Table of Compliance Elements

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The entity's PSMP failed to specify whether one Component Type is being addressed by time-based or performance-based maintenance, or a combination of both (part 1.1).	The entity's PSMP failed to specify whether two Component Types are being addressed by time-based or performance-based maintenance, or a combination of both (part 1.1).	The entity's PSMP failed to specify whether three Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (part 1.1). OR The entity's PSMP failed to include the applicable monitoring attributes applied to each Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-2, and Table 5 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Components (part 1.2).	The entity failed to establish a PSMP. OR The entity's PSMP failed to specify whether four or more Component Types are being addressed by time-based or performance-based maintenance, or a combination of both (part 1.1). OR The entity's PSMP failed to include applicable station batteries in a time-based program (part 1.1).
R2	The entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within three years.	NA	The entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within four years.	The entity uses performance-based maintenance intervals in its PSMP but: 1) Failed to establish the technical justification described within Requirement R2 for the initial use of the performance-based PSMP OR 2) Failed to reduce Countable Events to no more than 4% within five years OR

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
				3) Maintained a Segment with less than 60 Components OR 4) Failed to: • Annually update the list of Components, OR • Annually perform maintenance on the greater of 5% of the Segment population or 3 Components, OR • Annually analyze the program activities and results for each Segment.
R3	For Components included within a time-based maintenance program, the entity failed to maintain 5% or less of the total Components included within a specific Component Type in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-2, and Table 5. For Automatic Reclosing Components added to a time-based maintenance program per information from the Balancing	For Components included within a time-based maintenance program, the entity failed to maintain more than 5% but 10% or less of the total Components included within a specific Component Type in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-2, and Table 5. For Automatic Reclosing Components added to a time-based maintenance program per	For Components included within a time-based maintenance program, the entity failed to maintain more than 10% but 15% or less of the total Components included within a specific Component Type in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-2, and Table 5. For Automatic Reclosing Components added to a time-based maintenance program per	For Components included within a time-based maintenance program, the entity failed to maintain more than 15% of the total Components included within a specific Component Type in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-2, and Table 5. For Automatic Reclosing Components added to a time-

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Authority, the entity failed to maintain 5% or less of the total Components in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 4-1 through 4-2.	information from the Balancing Authority, the entity failed to maintain more than 5% but 10% or less of the total Components in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 4-1 through 4-2.	information from the Balancing Authority, the entity failed to maintain more than 10% but 15% or less of the total Components in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 4-1 through 4-2.	based maintenance program per information from the Balancing Authority, the entity failed to maintain more than 15% of the total Components in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 4-1 through 4-2.
R4	For Components included within a performance-based maintenance program, the entity failed to maintain 5% or less of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP. For Automatic Reclosing Components added to a performance-based maintenance program per information from the Balancing Authority, the entity failed to maintain 5% or less of the total Components in accordance with their performance-based PSMP.	For Components included within a performance-based maintenance program, the entity failed to maintain more than 5% but 10% or less of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP. For Automatic Reclosing Components added to a performance-based maintenance program per information from the Balancing Authority, the entity failed to maintain more than 5% but 10% or less of the total Components in accordance with their performance-based PSMP.	For Components included within a performance-based maintenance program, the entity failed to maintain more than 10% but 15% or less of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP. For Automatic Reclosing Components added to a performance-based maintenance program per information from the Balancing Authority, the entity failed to maintain more than 10% but 15% or less of the total Components in accordance with their performance-based PSMP.	For Components included within a performance-based maintenance program, the entity failed to maintain more than 15% of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP. For Automatic Reclosing Components added to a performance-based maintenance program per information from the Balancing Authority, the entity failed to maintain more than 15% of the total Components in accordance with their performance-based PSMP.

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The entity failed to undertake efforts to correct 5 or fewer identified Unresolved Maintenance Issues.	The entity failed to undertake efforts to correct greater than 5 but less than or equal to 10 identified Unresolved Maintenance Issues.	The entity failed to undertake efforts to correct greater than 10 but less than or equal to 15 identified Unresolved Maintenance Issues.	The entity failed to undertake efforts to correct greater than 15 identified Unresolved Maintenance Issues.
R6				The entity failed to notify each Transmission Owner, Generator Owner, and Distribution Provider within its Balancing Authority Area at least once every calendar year of the gross capacity, in MW or MVA, of the largest BES generating unit within the Balancing Authority Area. OR The entity had more than 15 calendar months between notifications to each Transmission Owner, Generator Owner, and Distribution Provider of the gross capacity, in MW or MVA, of the largest BES generating unit within the Balancing Authority Area.

D. Regional Variances

None.

E. Interpretations

None.

F. Supplemental Reference Documents

The following documents present a detailed discussion about determination of maintenance intervals and other useful information regarding establishment of a maintenance program.

1. *Supplementary Reference and FAQ - PRC-005-X Protection System Maintenance,* Protection System Maintenance and Testing Standard Drafting Team (April 2014)
2. *Considerations for Maintenance and Testing of Auto-reclosing Schemes*, NERC System Analysis and Modeling Subcommittee, and NERC System Protection and Control Subcommittee (November 2012)

Sudden Pressure Relays and Other Devices that Respond to Non-Electrical Quantities – SPCS Input for Standard Development in Response to FERC Order No. 758, NERC System Protection and Control Subcommittee (December 2013)

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. 3. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/05
1a	February 17, 2011	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers	Project 2009-17 interpretation
1a	February 17, 2011	Adopted by Board of Trustees	

Version	Date	Action	Change Tracking
1a	September 26, 2011	FERC Order issued approving interpretation of R1 and R2 (FERC's Order is effective as of September 26, 2011)	
1.1b	May 9, 2012	PRC-005-1.1b was adopted by the Board of Trustees as part of Project 2010-07 (Generator Requirements at the Transmission Interface).	
2	November 7, 2012	Adopted by Board of Trustees	Project 2007-17 - Complete revision, absorbing maintenance requirements from PRC-005-1.1b, PRC-008-0, PRC-011-0, PRC-017-0
2	October 17, 2013	Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase "or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;" to the second sentence under the "Retirement of Existing…"	
TBD (balloted as 4(X)	TBD	Standard revised in Project 2014-01	Applicability section revised to clarify application of Requirements to BES dispersed power producing resources
~~1a~~	~~September 26, 2011~~	~~FERC Order issued approving interpretation of R1 and R2 (FERC's Order is effective as of September 26, 2011)~~	
~~1.1a~~	~~February 1, 2012~~	~~Errata change: Clarified inclusion of generator interconnection Facility in Generator Owner's responsibility~~	~~Revision under Project 2010-07~~

Version	Date	Action	Change Tracking
~~1b~~	~~February 3, 2012~~	~~FERC Order issued approving interpretation of R1, R1.1, and R1.2 (FERC's Order dated March 14, 2012). Updated version from 1a to 1b.~~	~~Project 2009-10 Interpretation~~
~~1.1b~~	~~April 23, 2012~~	~~Updated standard version to 1.1b to reflect FERC approval of PRC-005-1b.~~	~~Revision under Project 2010-07~~

Version	Date	Action	Change Tracking
~~1.1b~~	~~May 9, 2012~~	~~PRC-005-1.1b was adopted by the Board of Trustees as part of Project 2010-07 (Generator Requirements at the Transmission Interface).~~	
~~2~~	~~November 7, 2012~~	~~Adopted by Board of Trustees~~	~~Project 2007-17 - Complete revision, absorbing maintenance requirements from PRC-005-1.1b, PRC-008-0, PRC-011-0, PRC-017-0~~
~~2~~	~~October 17, 2013~~	~~Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase "or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;" to the second sentence under the "Retirement of Existing~~	
3	November 7, 2013	Adopted by the NERC Board of Trustees	Revised to address the FERC directive in Order No.758 to include Automatic Reclosing in maintenance programs.
3.1	February 12, 2014	Approved by the Standards Committee	Errata changes to correct capitalization of defined terms

Version	Date	Action	Change Tracking
4			Project 2007-17.3 – Revised to address the FERC directive in Order No. 758 to include sudden pressure relays in maintenance programs.
TBD (balloted as 2(X)	TBD	.Standard revised in Project 2014-01.	Applicability section revised to clarify application of Requirements to BES dispersed power producing resources

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**[2]	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	For all unmonitored relays: • Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (see Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. • Alarming for power supply failure (see Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.

[2] For the tables in this standard, a calendar year starts on the first day of a new year (January 1) after a maintenance activity has been completed. For the tables in this standard, a calendar month starts on the first day of the first month after a maintenance activity has been completed.

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**[2]	**Maintenance Activities**
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 1-2 Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.	4 Calendar Months	Verify that the communications system is functional.
	6 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2).	12 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with all of the following: • Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation). (See Table 2) • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).	12 Calendar Years	Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the Protection System

Table 1-3 Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage and current sensing devices not having monitoring attributes of the category below.	12 Calendar Years	Verify that current and voltage signal values are provided to the protective relays.
Voltage and Current Sensing devices connected to microprocessor relays with AC measurements are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2).	No periodic maintenance specified	None.

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply using **Vented Lead-Acid (VLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	18 Calendar Months -or- 6 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **with Valve Regulated Lead-Acid (VRLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	6 Calendar Months	Inspect: • Condition of all individual units by measuring battery cell/unit internal ohmic values.
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Physical condition of battery rack

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	6 Calendar Months -or- 3 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **Nickel-Cadmium (NiCad) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells. • Physical condition of battery rack

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	6 Calendar Years	Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(d) Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System station dc supply not using a battery and not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	18 Calendar Months	Inspect: Condition of non-battery based dc supply
	6 Calendar Years	Verify that the dc supply can perform as manufactured when ac power is not present.

Table 1-4(e) Component Type – Protection System Station dc Supply for non-BES Interrupting Devices for SPS, non-distributed UFLS, and non-distributed UVLS systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a SPS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).	When control circuits are verified (See Table 1-5)	Verify Station dc supply voltage.

Table 1-4(f) Exclusions for Protection System Station dc Supply Monitoring Devices and Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2).	No periodic maintenance specified	No periodic verification of station dc supply voltage is required.
Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2).		No periodic inspection of the electrolyte level for each cell is required.
Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2).		No periodic inspection of unintentional dc grounds is required.
Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2).		No periodic verification of float voltage of battery charger is required.
Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2).		No periodic verification of the battery continuity is required.
Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2).		No periodic verification of the intercell and terminal connection resistance is required.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2).		No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2).		No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required.

Table 1-5 Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3) Note: Table requirements apply to all Control Circuitry Components of Protection Systems, and SPSs except as noted.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device.
Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with SPS. (See Table 4-2(b) for SPS which include Automatic Reclosing.)	12 Calendar Years	Verify all paths of the control circuits essential for proper operation of the SPS.
Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays.	12 Calendar Years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with protective functions and/or SPSs whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

Table 2 – Alarming Paths and Monitoring In Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2, alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any alarm path through which alarms in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the "Alarm Path with monitoring" category below. Alarms are reported within 24 hours of detection to a location where corrective action can be initiated.	12 Calendar Years	Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated.
Alarm Path with monitoring: The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated.	No periodic maintenance specified	None.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate. For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (See Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
• Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2).		
Voltage and/or current sensing devices associated with UFLS or UVLS systems.	12 Calendar Years	Verify that current and/or voltage signal values are provided to the protective relays.
Protection System dc supply for tripping non-BES interrupting devices used only for a UFLS or UVLS system.	12 Calendar Years	Verify Protection System dc supply voltage.
Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic).
Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices.
Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-BES interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-BES interrupting devices (excludes non-BES interrupting device trip coils).	No periodic maintenance specified	None.
Trip coils of non-BES interrupting devices in UFLS or UVLS systems.	No periodic maintenance specified	None.

Table 4-1 Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Reclosing Relay		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored reclosing relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.
Monitored microprocessor reclosing relay with the following: • Internal self-diagnosis and alarming (See Table 2). • Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.

Table 4-2(a) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing Relays that are NOT an Integral Part of an SPS		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Unmonitored Control circuitry associated with Automatic Reclosing that is not an integral part of an SPS.	12 Calendar Years	Verify that Automatic Reclosing, upon initiation, does not issue a premature closing command to the close circuitry.
Control circuitry associated with Automatic Reclosing that is not part of an SPS and is monitored and alarmed for conditions that would result in a premature closing command. (See Table 2)	No periodic maintenance specified	None.

Table 4-2(b) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing Relays that ARE an Integral Part of an SPS		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Close coils or actuators of circuit breakers or similar devices that are used in conjunction with Automatic Reclosing as part of an SPS (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each close coil or actuator is able to operate the circuit breaker or mitigating device.
Unmonitored close control circuitry associated with Automatic Reclosing used as an integral part of an SPS.	12 Calendar Years	Verify all paths of the control circuits associated with Automatic Reclosing that are essential for proper operation of the SPS.
Control circuitry associated with Automatic Reclosing that is an integral part of an SPS whose integrity is monitored and alarmed. (See Table 2)	No periodic maintenance specified	None.

Table 5 Maintenance Activities and Intervals for Sudden Pressure Relaying		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any fault pressure relay.	6 Calendar Years	Verify the pressure or flow sensing mechanism is operable.
Control circuitry associated with Sudden Pressure Relaying from the fault pressure relay to the interrupting device trip coil(s).	12 Calendar Years	Verify all paths of the control circuits that are essential for proper operation of the Sudden Pressure Relaying.

PRC-005 — Attachment A

Criteria for a Performance-Based Protection System Maintenance Program

Purpose: To establish a technical basis for initial and continued use of a performance-based Protection System Maintenance Program (PSMP).

To establish the technical justification for the initial use of a performance-based PSMP:

1. Develop a list with a description of Components included in each designated Segment, with a minimum **Segment** population of 60 Components.
2. Maintain the Components in each Segment according to the time-based maximum allowable intervals established in Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-2, and Table 5 until results of maintenance activities for the Segment are available for a minimum of 30 individual Components of the Segment.
3. Document the maintenance program activities and results for each Segment, including maintenance dates and Countable Events for each included Component.
4. Analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment and develop maintenance intervals.
5. Determine the maximum allowable maintenance interval for each Segment such that the Segment experiences **Countable Events** on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

To maintain the technical justification for the ongoing use of a performance-based PSMP:

1. At least annually, update the list of Components and Segments and/or description if any changes occur within the Segment.
2. Perform maintenance on the greater of 5% of the Components (addressed in the performance based PSMP) in each Segment or 3 individual Components within the Segment in each year.
3. For the prior year, analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment.
4. Using the prior year's data, determine the maximum allowable maintenance interval for each Segment such that the Segment experiences Countable Events on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

If the Components in a Segment maintained through a performance-based PSMP experience 4% or more Countable Events, develop, document, and implement an action plan to reduce the Countable Events to less than 4% of the Segment population within 3 years.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC BES Kickoff Webinar

PLEASE WAIT
WE WILL BEGIN SHORTLY

May 2, 2014

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC BES Kickoff Webinar

May 2, 2014

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC BES Kickoff

Overview of the BES Definition

Carter Edge, Director of Coordinated Activities, REMG
Bob Cummings, Director of Reliability Initiatives and System Analysis, NERC

NERC BES Kickoff Webinar

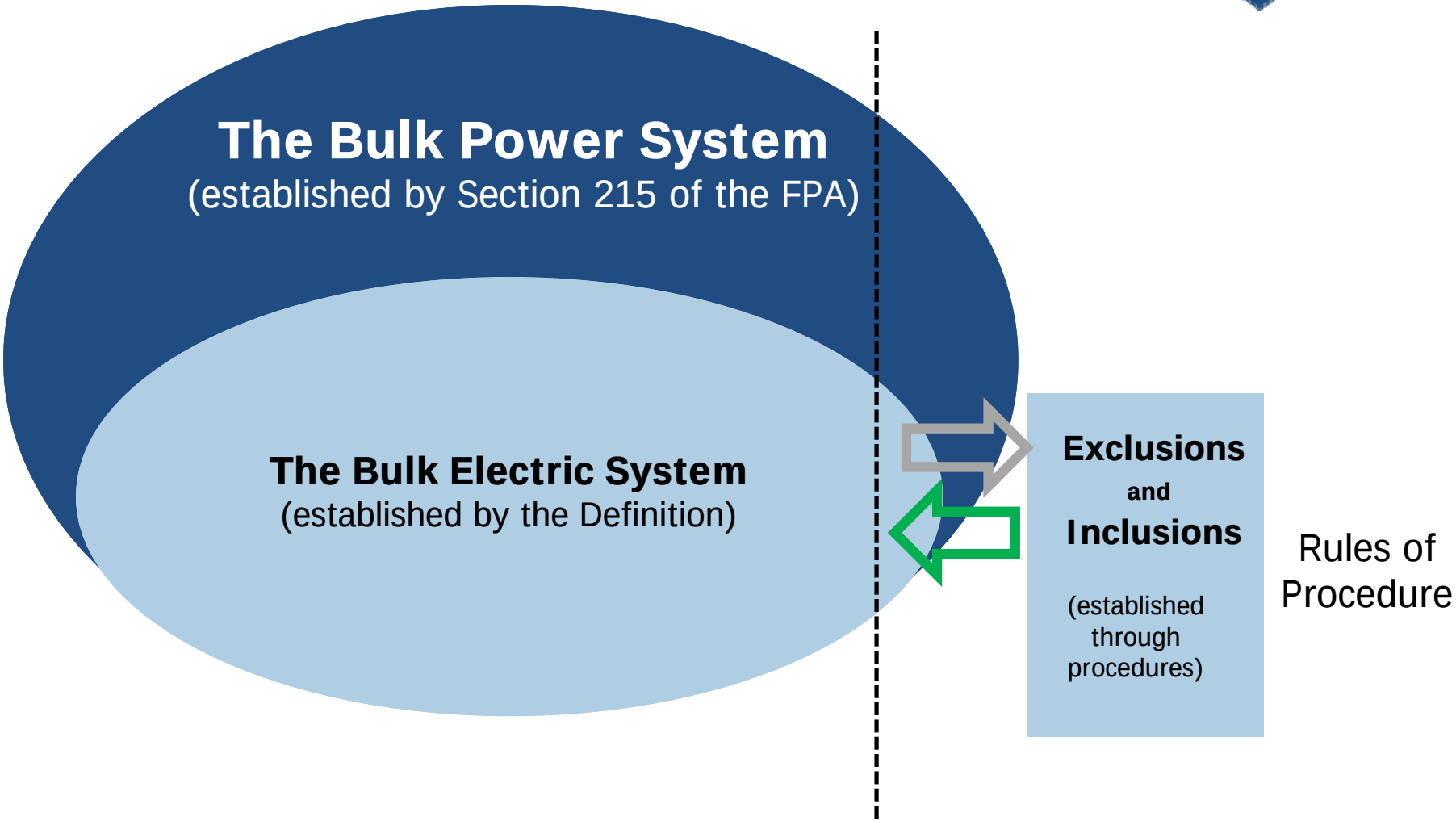
May 2, 2014

RELIABILITY | ACCOUNTABILITY

BES Definition at a Glance

- Consistent, uniform way to determine BES assets
- Effective 7/1/2014
- Transition period through 7/2016
- ERO enterprise common process and tool for implementation
- Documents and training readily available
- BES web page – one stop shopping
- Regional and NERC staff resources available to answer detailed questions and implementation

What is the Bulk Electric System?



BES 'Core' Definition

Bulk Electric System (BES): Unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.

- Establishes the overall demarcation point between BES and non-BES Elements.

Inclusions

Provide additional clarification for the purposes of identifying specific Elements that are included in the BES.

I1. BES Transformers

I2. Real Power Resources

I3. Blackstart Resources

I4. Dispersed power producing resources meeting certain criteria

I5. Reactive Power Resources

Exclusions

Provide additional clarification for the purposes of identifying specific Elements that may be excluded from the BES.

E1. Radial Systems

E2. Retail Generation

E3. Local Networks

E4. Reactive Power Devices installed solely for retail customers

How to Apply the BES Definition, Inclusions, and Exclusions

Consistent methodology outlined in the BES Definition Reference Document

STEP 1: CORE DEFINITION

STEP 2: INCLUSIONS

STEP 3: EXCLUSIONS

STEP 3: EXCLUSIONS should be applied in the following sequence:

- **E2 Retail Generation** (supersedes **I2 Real Power Resources**)
- **E4 Retail Reactive Power Devices** (supersedes **I5 Reactive Power Resources**)
- **E3 Local Networks** (does not exclude interconnection facilities or generators)
- **E1 Radial Systems** (does not exclude interconnection facilities or generators)

BES Notifications

- Applies to newly self-identified inclusions to and exclusions from the BES
- Assures that entities are appropriately implementing the revised definition
- Compliance obligations cease for facilities excluded from the BES
- 24-month implementation period to bring newly-identified Facilities included in the BES into compliance

Self-Determination Notification Information Requirements

Each notification **should at a minimum include the following:**

- Current one-line diagrams
- For **E2 Retail Generation** Exclusion notifications
  - Net Capacity Transactional Data (12 months of hourly data)
  - Standby, back-up and maintenance power service documentation
- For **E3 Local Network** Exclusion notifications
  - Power Flow Transactional Data (24 months of hourly data)

BES Exceptions

Considerations:

- Applicable to all Exception Requests
- Applicable to specific Elements or groups of Elements

Must demonstrate that the requested facilities **are** (for inclusions) or **are not** (for exclusions) necessary for the reliable operation of the interconnected transmission system

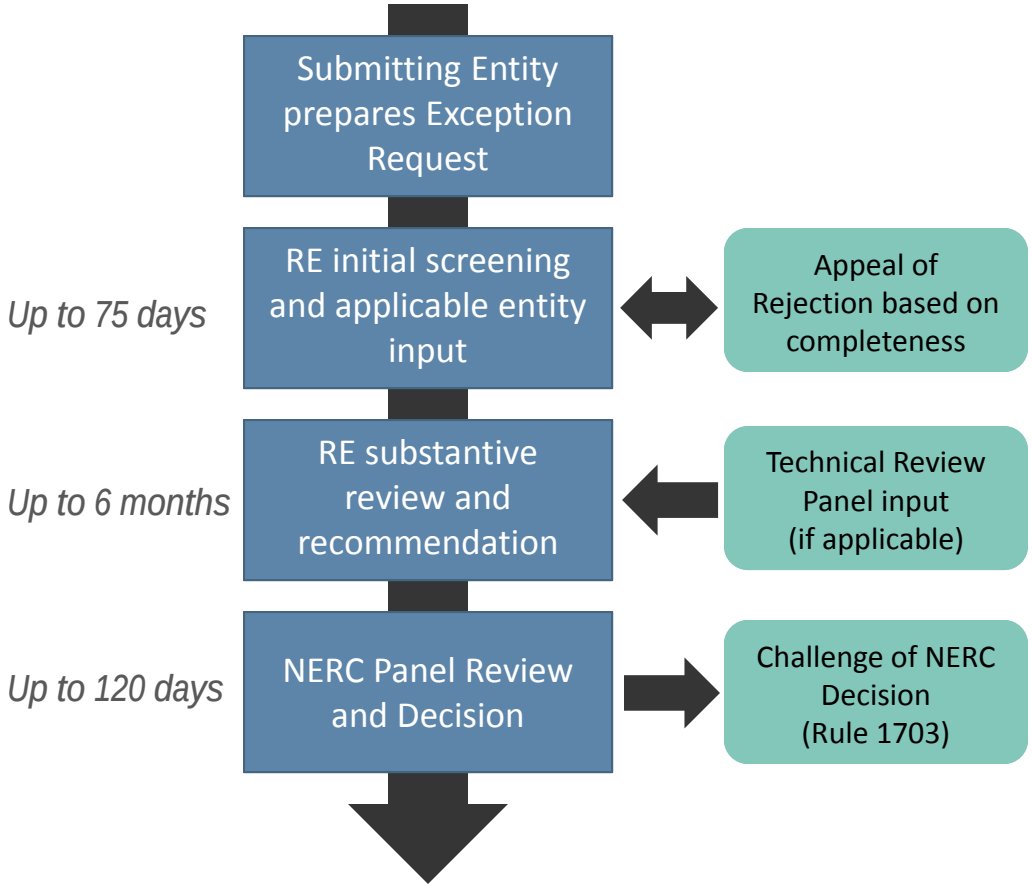
Who can Submit an Exception Request?

- Owner of the Element(s)
- Regional Entity
- Entity with Scope of Responsibility for the Element(s) under consideration:
  - Regional Entity
  - Planning Authority
  - Reliability Coordinator
  - Transmission Operator
  - Transmission Planner
  - Balancing Authority

The Exception Request Process

The Main Steps in the Exception Process:

- Exception Request Submittal
- Regional Entity (RE) Initial Review
- Regional Entity Substantive Review and Recommendation
- NERC Review and Final Decision



Many Resources to Assist You

- **Bulk Electric System Definition Reference Document**

  Describes the application of the BES Definition

- **BES Notification Review Guidelines**

  Describes how ERO Enterprise staff will review Self-Determined Notifications submitted through BESnet

- **BES Exception Request Evaluation Guidelines**

  Describes how ERO Enterprise staff will review Exception Requests submitted through BESnet

- **BES Implementation Reference Document**

  Outlines standards applicability and registration expectations

Many Resources to Assist You

- **BESnet Application Users Guide**

  Manual for the online BESnet application

- **Frequently Asked Questions (FAQ)**

  Explains application, submittal, and process for BES Definition implementation

- **FERC Orders 773 and 773-A**

  Regulations approving modified BES definition

- **NERC Rules of Procedure**

  Section 500 and Appendix 5C

- **Various White Papers**

  Providing Technical Justification

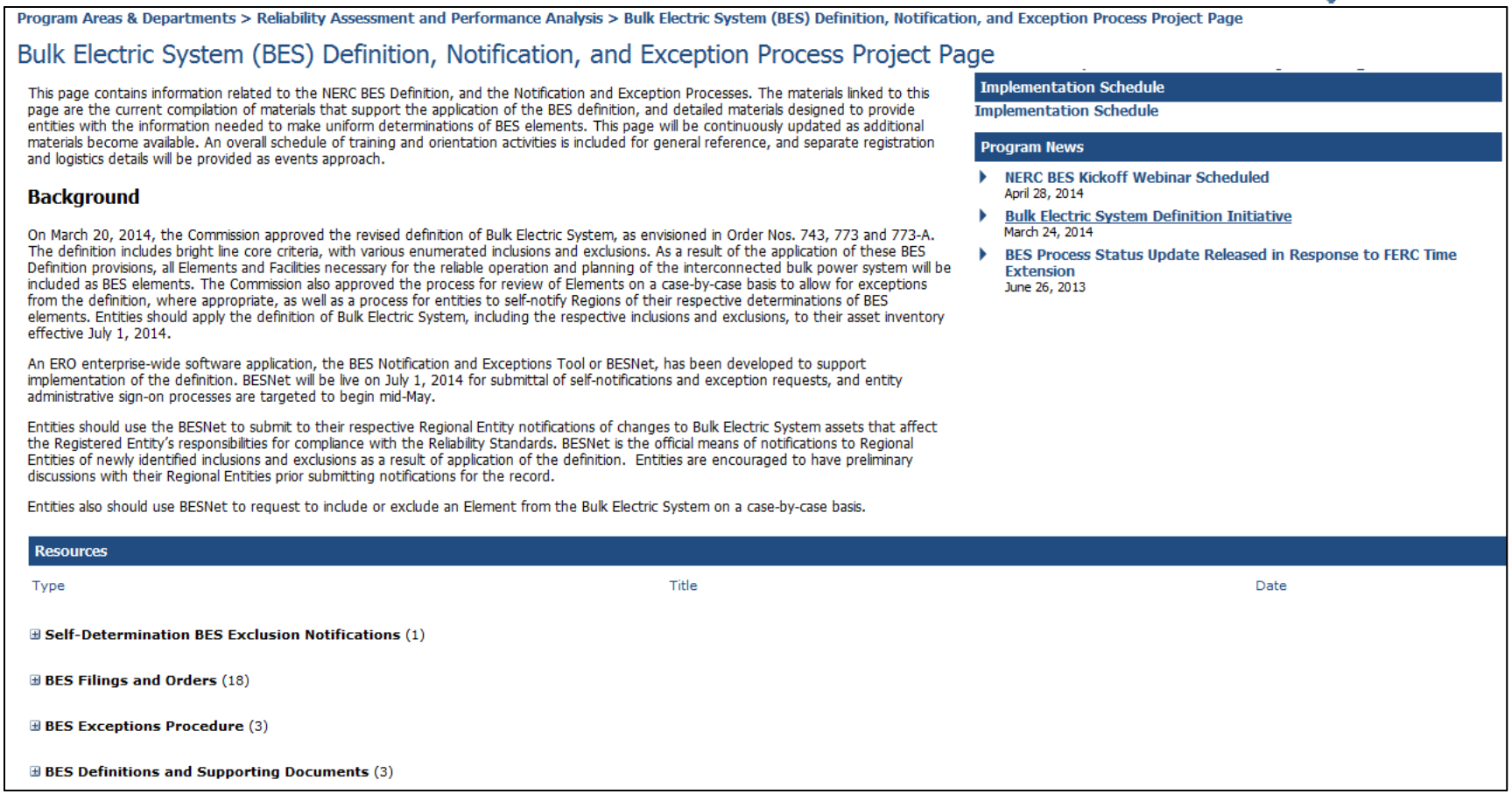
For Additional Information

…and most important,

HOW?

1. *Go to www.nerc.com*
2. *Under **Program Areas and Departments**, click [Reliability Assessment and Performance Analysis]*
3. *From there, click [Bulk Electric System (BES) Definition, Notification, and Exception Process Project]*

For Additional Information



Program Areas & Departments > Reliability Assessment and Performance Analysis > Bulk Electric System (BES) Definition, Notification, and Exception Process Project Page

Bulk Electric System (BES) Definition, Notification, and Exception Process Project Page

This page contains information related to the NERC BES Definition, and the Notification and Exception Processes. The materials linked to this page are the current compilation of materials that support the application of the BES definition, and detailed materials designed to provide entities with the information needed to make uniform determinations of BES elements. This page will be continuously updated as additional materials become available. An overall schedule of training and orientation activities is included for general reference, and separate registration and logistics details will be provided as events approach.

Background

On March 20, 2014, the Commission approved the revised definition of Bulk Electric System, as envisioned in Order Nos. 743, 773 and 773-A. The definition includes bright line core criteria, with various enumerated inclusions and exclusions. As a result of the application of these BES Definition provisions, all Elements and Facilities necessary for the reliable operation and planning of the interconnected bulk power system will be included as BES elements. The Commission also approved the process for review of Elements on a case-by-case basis to allow for exceptions from the definition, where appropriate, as well as a process for entities to self-notify Regions of their respective determinations of BES elements. Entities should apply the definition of Bulk Electric System, including the respective inclusions and exclusions, to their asset inventory effective July 1, 2014.

An ERO enterprise-wide software application, the BES Notification and Exceptions Tool or BESNet, has been developed to support implementation of the definition. BESNet will be live on July 1, 2014 for submittal of self-notifications and exception requests, and entity administrative sign-on processes are targeted to begin mid-May.

Entities should use the BESNet to submit to their respective Regional Entity notifications of changes to Bulk Electric System assets that affect the Registered Entity's responsibilities for compliance with the Reliability Standards. BESNet is the official means of notifications to Regional Entities of newly identified inclusions and exclusions as a result of application of the definition. Entities are encouraged to have preliminary discussions with their Regional Entities prior submitting notifications for the record.

Entities also should use BESNet to request to include or exclude an Element from the Bulk Electric System on a case-by-case basis.

Implementation Schedule

Implementation Schedule

Program News

- NERC BES Kickoff Webinar Scheduled
  April 28, 2014
- Bulk Electric System Definition Initiative
  March 24, 2014
- BES Process Status Update Released in Response to FERC Time Extension
  June 26, 2013

Resources

Type	Title	Date
⊞ **Self-Determination BES Exclusion Notifications** (1)		
⊞ **BES Filings and Orders** (18)		
⊞ **BES Exceptions Procedure** (3)		
⊞ **BES Definitions and Supporting Documents** (3)		

http://www.nerc.com/pa/RAPA/Pages/BES.aspx

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC BES Kickoff

Overview of BESnet

Justin Lofquist, ERO Enterprise Project Manager, NERC

NERC BES Kickoff Webinar

May 2, 2014

RELIABILITY | ACCOUNTABILITY

Bulk Electric System Notifications and Exceptions Tool

- Centralized, Web-based application
  - Hosted in Tier IV data facility
  - Highly secure, fully redundant
- User base
  - Registered and Unregistered Entities
  - Regional Entities
  - NERC

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Actions

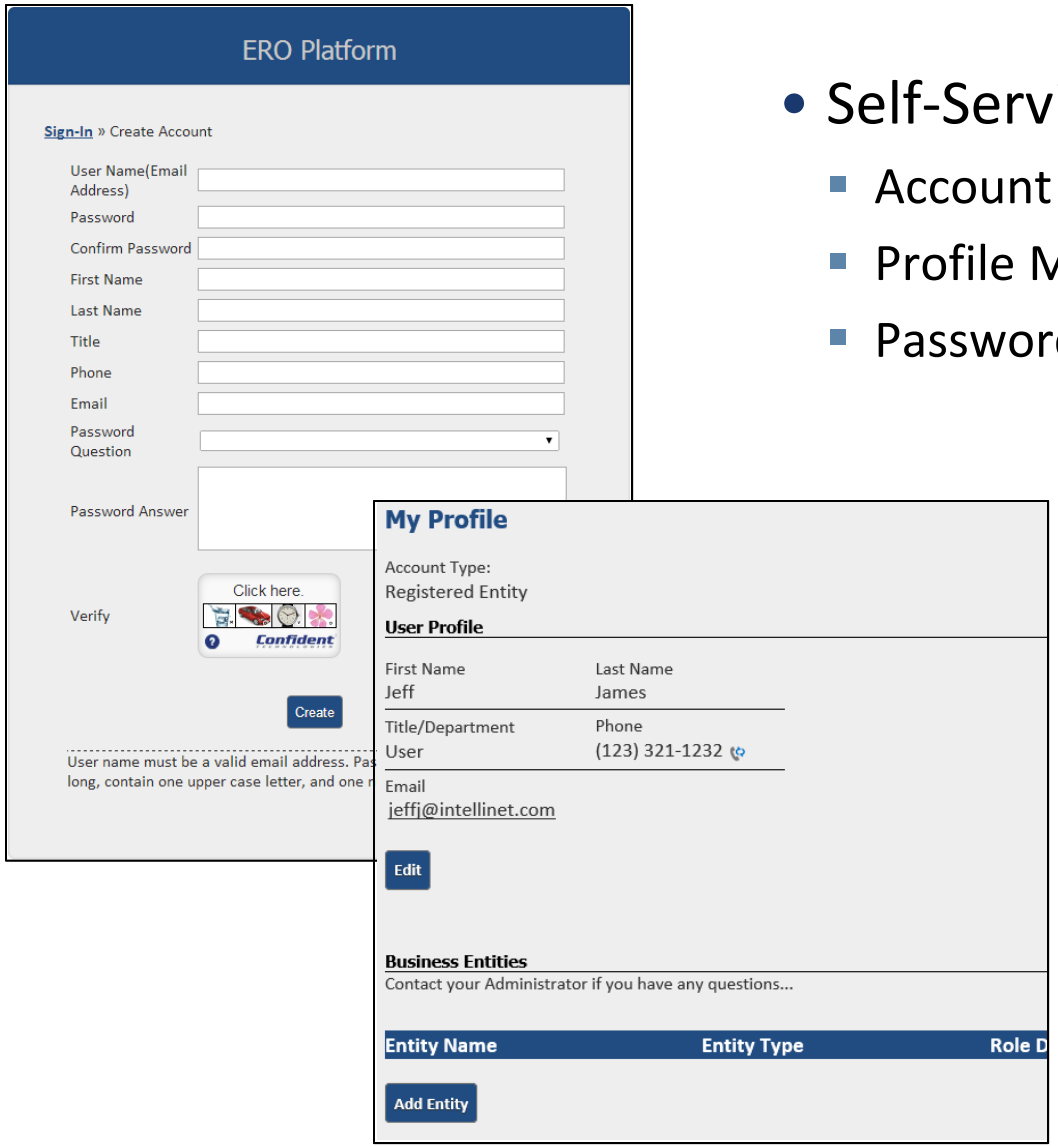
Home | User | Create Exception Request | Create Self Determination | Reports

- Automation of NERC Rules of Procedure Appendix 5c
  - Registered and Unregistered Entities:
    - Submission, Appeals and Challenges
  - Regional Entities
    - Initial and Substantive Reviews, Recommendations
  - NERC
    - Proposed and Final Decisions, Certification

Actions (cont.)

- Notifications of Self-Determination
  - Submission
  - Regional and NERC review
- Account Management
- Reporting
  - Process Performance
  - Exception Request and Self-Determinations status

Accounts



- Self-Service
  - Account Creation
  - Profile Management
  - Password Resets

- Multi-Entity Management
  - Single user to Multiple Entities

- Distributed Administration
  - Administrator per Entity

Dashboard

Exception Requests

Show in Dashboard

Archived: ☐ Withdrawn: ☐ Split: ☐ Self Determination In NERC Review: ☐ Filter

Show 10 entries

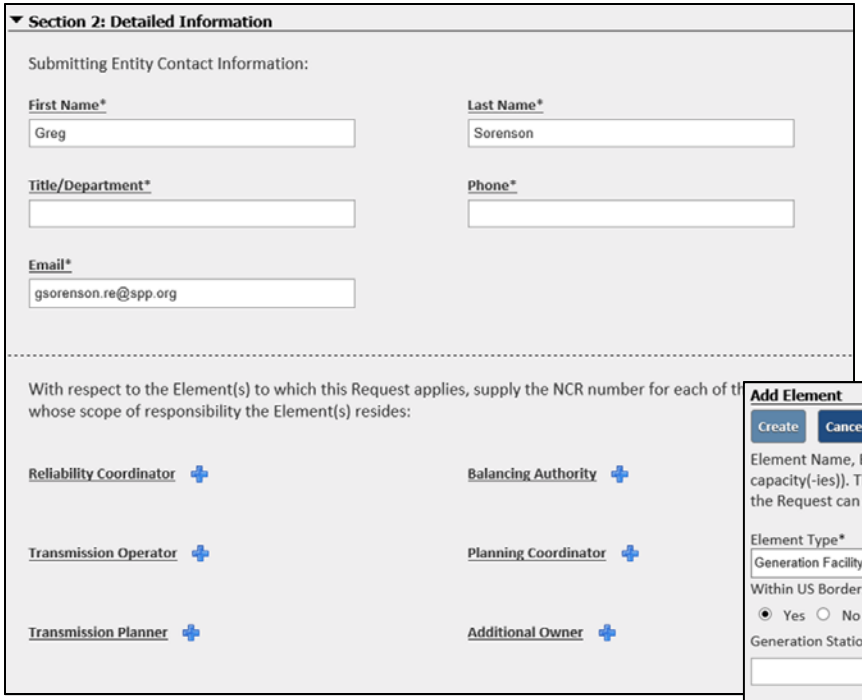
ID	Status	Type	Submitted	Submitting Entity	Region	Next Action Due
2014-FRCC-NCR00005-Exception00002	Certified - Notification of Change	Exception Request	02/28/2014 11:43:15 EST	Calpine Corporation	FRCC	01/01/2017 - Next Certification
d5a4f648-f548-4708-b9f4-d8429236b156	Rejected	Exception Request	02/28/2014 09:50:50 EST	BP Energy Company	WECC	04/14/2014 - Appeal
d5a4f648-f548-4708-b9f4-d8429236b156	Rejected	Exception Request	02/28/2014 09:50:50 EST	BP Energy Company	WECC	04/14/2014 - Appeal
414a5d9d-d02a-42ab-8a53-cd53b316d1e9	Under Appeal	Exception Request	02/28/2014 09:50:51 EST	BP Energy Company	WECC	04/14/2014 - Appeal
414a5d9d-d02a-42ab-8a53-cd53b316d1e9	Under Appeal	Exception Request	02/28/2014 09:50:51 EST	BP Energy Company	WECC	04/14/2014 - Appeal
d363baaa-6ee7-4487-9861-b1cfa0ccdd4d	Final Decision	Exception Request	02/28/2014 09:50:55 EST	BP Energy Company	WECC	04/14/2014 - Final Decision
d363baaa-6ee7-4487-9861-b1cfa0ccdd4d	Final Decision	Exception Request	02/28/2014 09:50:55 EST	BP Energy Company	WECC	04/14/2014 - Final Decision
d363baaa-6ee7-4487-9861-b1cfa0ccdd4d	Final Decision	Exception Request	02/28/2014 09:50:55 EST	BP Energy Company	WECC	04/14/2014 - Final Decision
d363baaa-6ee7-4487-9861-b1cfa0ccdd4d	Final Decision	Exception Request	02/28/2014 09:50:55 EST	BP Energy Company	WECC	04/14/2014 - Final Decision
c7ed7e2e-c443-41af-aba3-1bbf2c17f66c	Substantive Review	Exception Request	02/28/2014 09:50:53 EST	BP Energy Company	WECC	04/14/2014 - Initial Review

Showing 1 to 10 of 19 entries

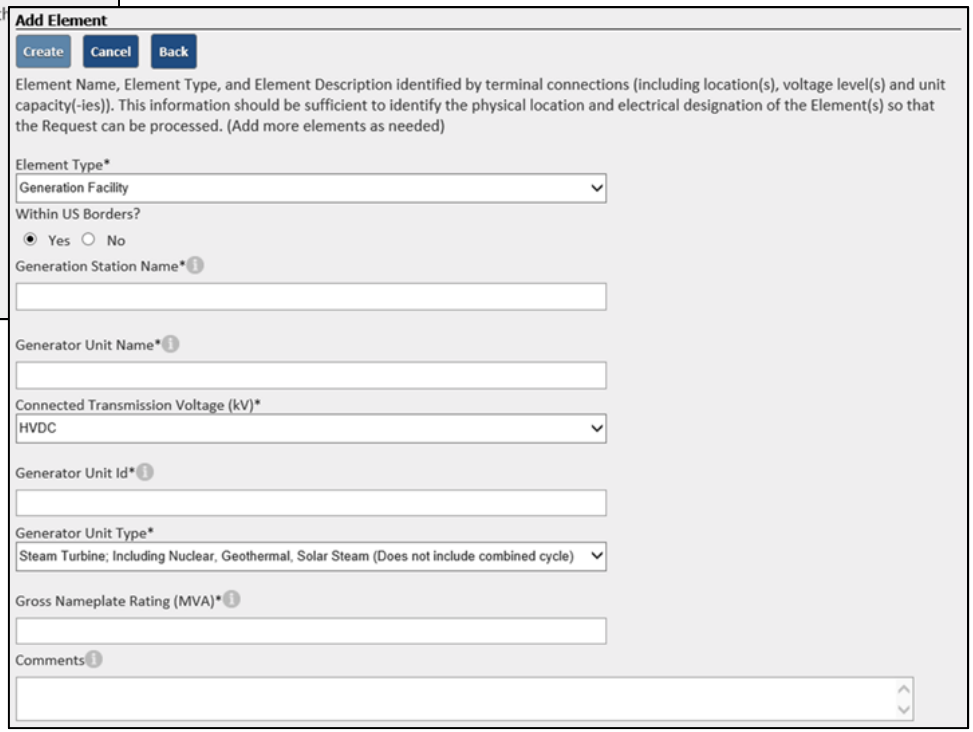
First Previous 1 2 Next Last

- Main Application Page
  - All Exception Requests and Self-Determinations relevant to user's Entity, based on role
    - Submitting Entity
    - Owning Entity
    - Functional Relationship (e.g. RC, BA)

Creating Exception Requests

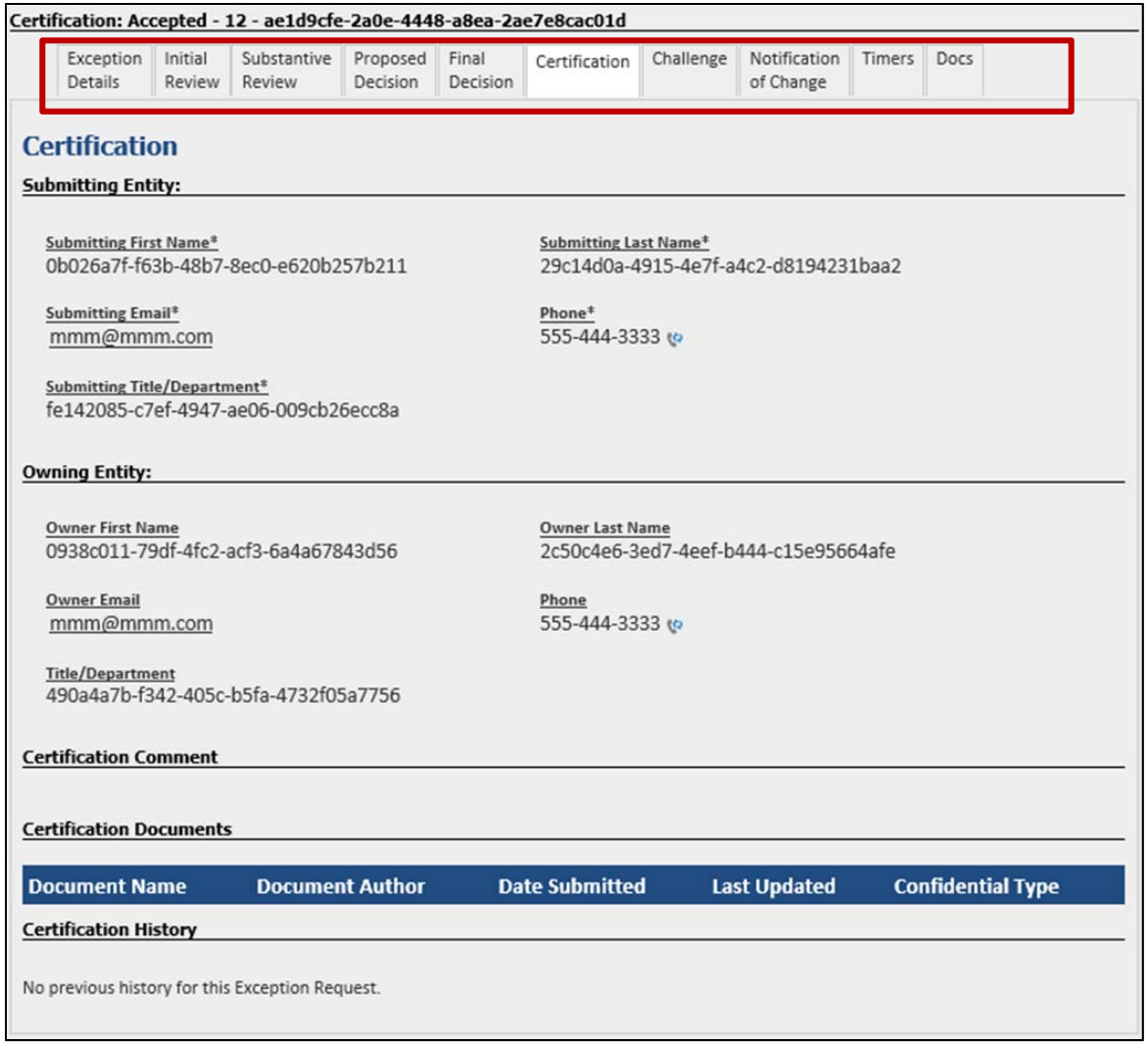


- Exception Request Details
  - Identify Entities within the Scope of Responsibility for an Exception Request



- Add Elements to Exception Request
  - Input Element Characteristics

Exception Requests in Certification


Certification: Accepted - 12 - ae1d9cfe-2a0e-4448-a8ea-2ae7e8cac01d

Exception Details | Initial Review | Substantive Review | Proposed Decision | Final Decision | Certification | Challenge | Notification of Change | Timers | Docs

Certification

Submitting Entity:

Submitting First Name*
0b026a7f-f63b-48b7-8ec0-e620b257b211

Submitting Last Name*
29c14d0a-4915-4e7f-a4c2-d8194231baa2

Submitting Email*
mmm@mmm.com

Phone*
555-444-3333

Submitting Title/Department*
fe142085-c7ef-4947-ae06-009cb26ecc8a

Owning Entity:

Owner First Name
0938c011-79df-4fc2-acf3-6a4a67843d56

Owner Last Name
2c50c4e6-3ed7-4eef-b444-c15e95664afe

Owner Email
mmm@mmm.com

Phone
555-444-3333

Title/Department
490a4a7b-f342-405c-b5fa-4732f05a7756

Certification Comment

Certification Documents

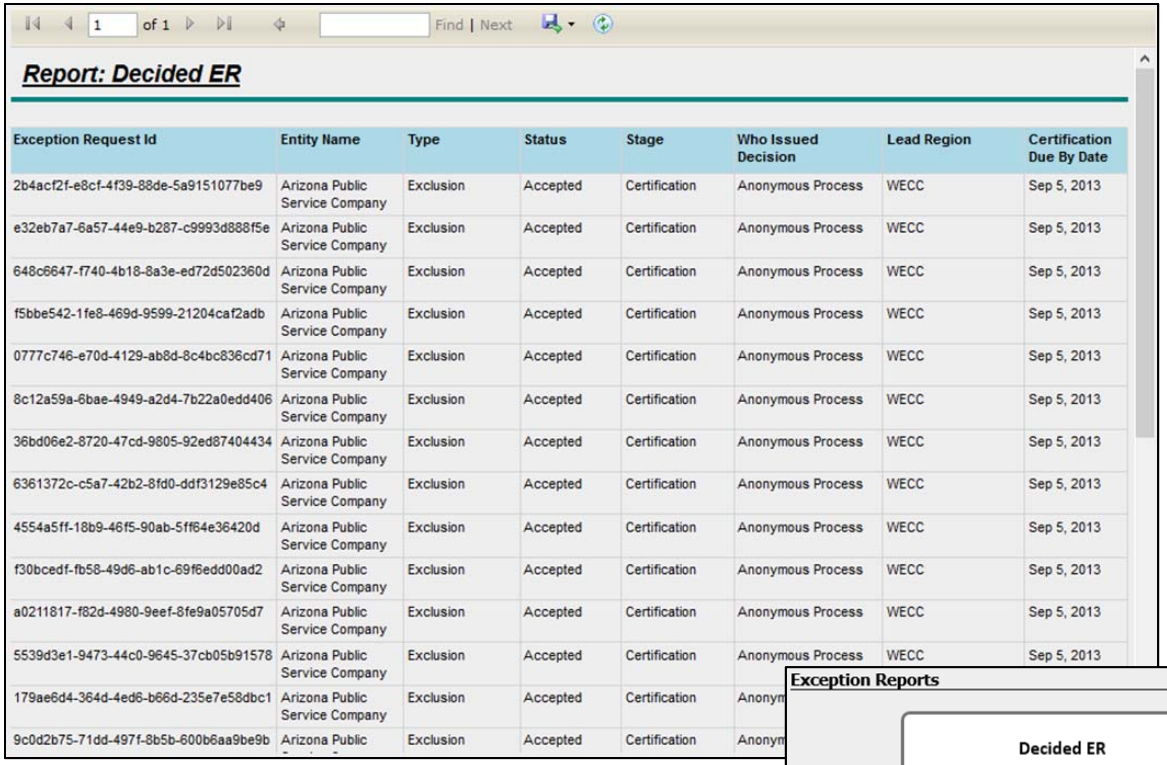
Document Name	Document Author	Date Submitted	Last Updated	Confidential Type

Certification History

No previous history for this Exception Request.

- Exception Request in Certification
  - Full process executed
    - Initial Review
    - Substantive Review
    - Proposed Decision
    - Final Decision
    - Certification

Reporting

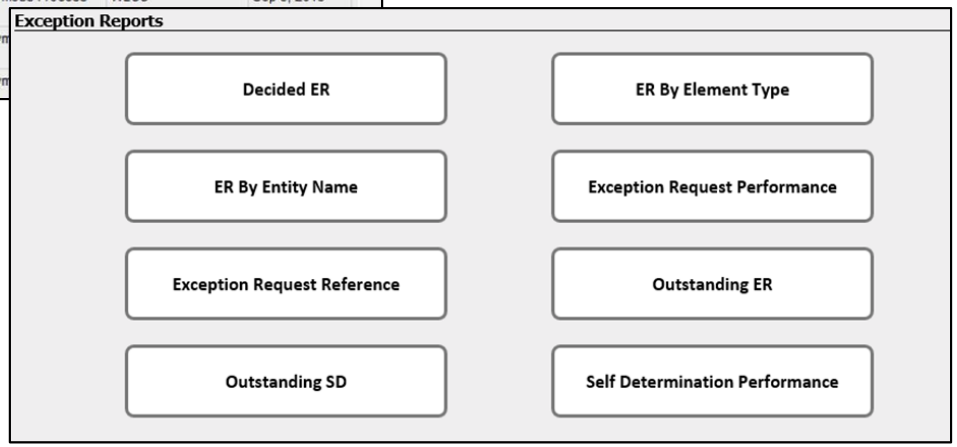


1 of 1 Find | Next

Report: Decided ER

Exception Request Id	Entity Name	Type	Status	Stage	Who Issued Decision	Lead Region	Certification Due By Date
2b4acf2f-e8cf-4f39-88de-5a9151077be9	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonymous Process	WECC	Sep 5, 2013
e32eb7a7-6a57-44e9-b287-c9993d888f5e	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonymous Process	WECC	Sep 5, 2013
648c6647-f740-4b18-8a3e-ed72d502360d	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonymous Process	WECC	Sep 5, 2013
f5bbe542-1fe8-469d-9599-21204caf2adb	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonymous Process	WECC	Sep 5, 2013
0777c746-e70d-4129-ab8d-8c4bc836cd71	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonymous Process	WECC	Sep 5, 2013
8c12a59a-6bae-4949-a2d4-7b22a0edd406	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonymous Process	WECC	Sep 5, 2013
36bd06e2-8720-47cd-9805-92ed87404434	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonymous Process	WECC	Sep 5, 2013
6361372c-c5a7-42b2-8fd0-ddf3129e85c4	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonymous Process	WECC	Sep 5, 2013
4554a5ff-18b9-46f5-90ab-5ff64e36420d	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonymous Process	WECC	Sep 5, 2013
f30bcedf-fb58-49d6-ab1c-69f6edd00ad2	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonymous Process	WECC	Sep 5, 2013
a0211817-f82d-4980-9eef-8fe9a05705d7	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonymous Process	WECC	Sep 5, 2013
5539d3e1-9473-44c0-9645-37cb05b91578	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonymous Process	WECC	Sep 5, 2013
179ae6d4-364d-4ed6-b66d-235e7e58dbc1	Arizona Public Service Company	Exclusion	Accepted	Certification	Anonym		
9c0d2b75-71dd-497f-8b5b-600b6aa9be9b	Arizona Public	Exclusion	Accepted	Certification	Anonym		

- Multiple Report Types



- Security trimmed to return only authorized records

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC BES Kickoff

Review of BES Implementation Schedule

Andy Rodriquez, Director for RAPA, NERC

NERC BES Kickoff Webinar

May 2, 2014

RELIABILITY | ACCOUNTABILITY

Key Dates

May 12, 2014	BESnet system available for each registered entity's BESnet Administrator to create an ERO Platform account and/or request access to BESnet	*Access requests will be reviewed by Regional BESnet Administrators*
May 30, 2014	BESnet system available for each registered entity's BESnet users to create an ERO Platform account and/or request access to BESnet	*Access requests will be reviewed by Entity BESnet Administrators*
July 1, 2014	BESnet system available users to submit Self-Determined Notifications and Exception Requests	*Notifications and Exceptions will be processed by Regions and NERC*

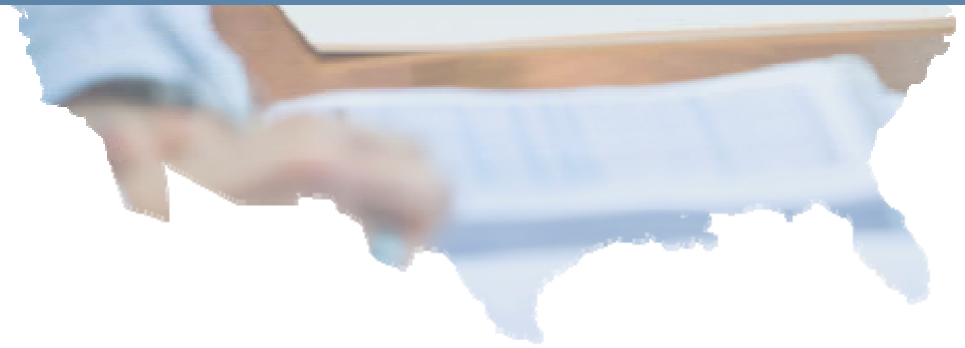
Training Activities

- **Regional BES Training and Workshops (confirmed)**
  - March 17-18 – SERC Compliance Seminar (completed)
  - March 25 – RF Compliance Seminar (completed)
  - April 21-22 – FRCC BES Workshop (completed)
  - May 21 – TRE Standards and Compliance Workshop
  - May 27-30 – NPCC 2014 Spring Compliance and Standards Workshop
  - May 28 – MRO Reliability Conference
  - June 3-5 – WECC Compliance Users Group
  - June 12 – SPP BES Definition and BESnet Tool Webinar

Training Activities

- **NERC BES Training and Workshops (in planning)**
  - May 9 – Posting of BESnet Video Training Modules
  - May 9 – Posting of BESnet User Guides
  - May 15-30 – Posting of BES Business Process Video Training Modules
  - June 2 – BES Business Process Q&A Webinar
  - June 10 – Standing Committee Q&A Workshop
  - June 16 – BES Business Process Q&A Webinar
  - June 23 – BES Business Process Q&A Webinar
  - June 30 – BES Business Process Q&A Webinar
  - June TBD – NERC BESnet Training Webinar

Questions and Answers



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

BESNet Training Manual

Pre-Implementation Account Management for Registered Entities

May 9, 2014
Version 1-0

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction 3

BESNet Program Cautions 4

Version History 5

User Account Management 6

- Introduction 6
- Creating a New Account 6
  - Creating Account Step 1: User Name and Password 6
  - Creating Account Step 2: Verify Account 8
- Logging Into the BESNet Application 10
  - Selecting the User's Entity to Use 11
- Setting up Your BESNet Application Account 12
  - Account Setup Step 1: Select Account Type 12
  - Account Setup Step 2: Association of Account with Entities 13
- Editing Your User Profile 16
- Password Management 17
  - Changing User Password 17
  - Forgot/Resetting the User Password 18
- Managing Your User Account Properties 21
- Logging Out 22

Administrator User Account Management 23

- Administrative User Management 23
  - Vetting New Users 23
  - User Role Management 24

Introduction

NOTE: This pre-implementation manual ONLY addresses Account Management for Registered Entities. As we near the July 1, 2014, implementation date, additional sections will be made available regarding other parts of the process and application.

Entity Administrator accounts should be the first accounts set up within the BESnet Application. Once the Primary Compliance Contact has established his or her Entity Administrator account, they can then work with the other individuals within their companies to set up additional User and Administrator accounts.

This user manual provides a guided walkthrough to illustrate the BES Notifications and Exceptions Tool (BESNet). The system provides a workflow-based process that emulates the BES Exceptions Procedure, as outlined in NERC RoP Appendix 5, to route, evaluate and take actions on Exception Requests and Self-Determined Notifications.

Users have the ability to login to a secure portal and create both Exception Requests and Self-Determination Notifications. Depending upon the selection, the user is provided with the appropriate Exception or Self-Determination form to which they are able to provide details regarding the Request / Notification. Each form captures the relevant details for the Submitting and Owning Entities, Inclusion and Exclusion rules, Element Descriptions and one or more elements.

Upon completion of the form, the Entity is able to submit the Request / Notification. The system will automatically notify all appropriate parties of the submission. This includes Submitting and Owning Entities, Scope of Responsibility Entities, Regional Entities and NERC. BESNet provides facilities for Regional Entities to acknowledge notification elements and process Exception Requests, request and receive supplemental information, alert and notify participants, issue recommendations, and monitor periodic re-certification of requests. In addition, NERC can create proposed and final decisions, as well as manage appeals to those decisions.

Queries have been created for accessing information about Exception Requests and Notifications enabling the BESNet to produce a list of facilities and Elements for which: 1) exceptions to the definition have been granted and 2) self-determination Notifications have been submitted. NERC will publicly post reports on its website that will provide interested persons, including applicable governmental authorities, information regarding submitted Exception Requests that may be of interest to them.

BESNet Program Cautions

The following cautions should be followed when using the BESNet program.

A. DO NOT use the back button in your browser.

B. Be sure to scroll right and left within your browser (depending on your screen resolution) to ensure that all required information can be entered in the browser.

Version History

The following is the history of changes to this document.

Version	Date	Change(s) Made	Change Tracking
1-0	May 9, 2014	Initial Release – User Account Management Section only	

User Account Management

Introduction

The BESNet application operates within the framework of the ERO Enterprise Platform which includes several applications such as the NERC Standards Balloting System.

Note – If you already have an ERO Platform Account (for the new Standards Balloting System), please proceed to Setting up New Account in the BESNet Application section of this User Guide.

Creating a New Account

If you do not have an existing ERO Platform user ID, you will need to create a new account for the BESNet application. The new user must supply user profile information and identify the organization the user represents.

Once an account is created, an administrator will vet the user as a person for role-based, individual access to the system. Once vetted, a user will be notified through email that they can login to the system.

Creating Account Step 1: User Name and Password

Navigate to the BESnet application. Contact your Entity BESnet Administrator for the URL to the application.

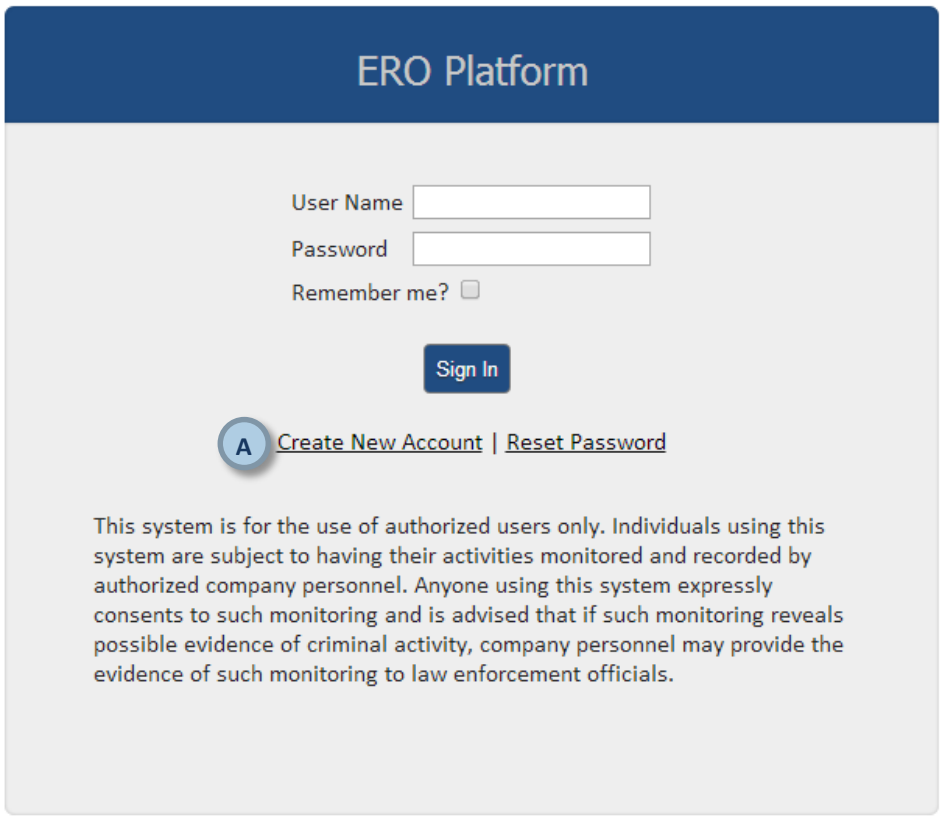


Figure 1: ERO Platform Login Screen

A. Click on **Create New Account** (A). The following screen will appear.

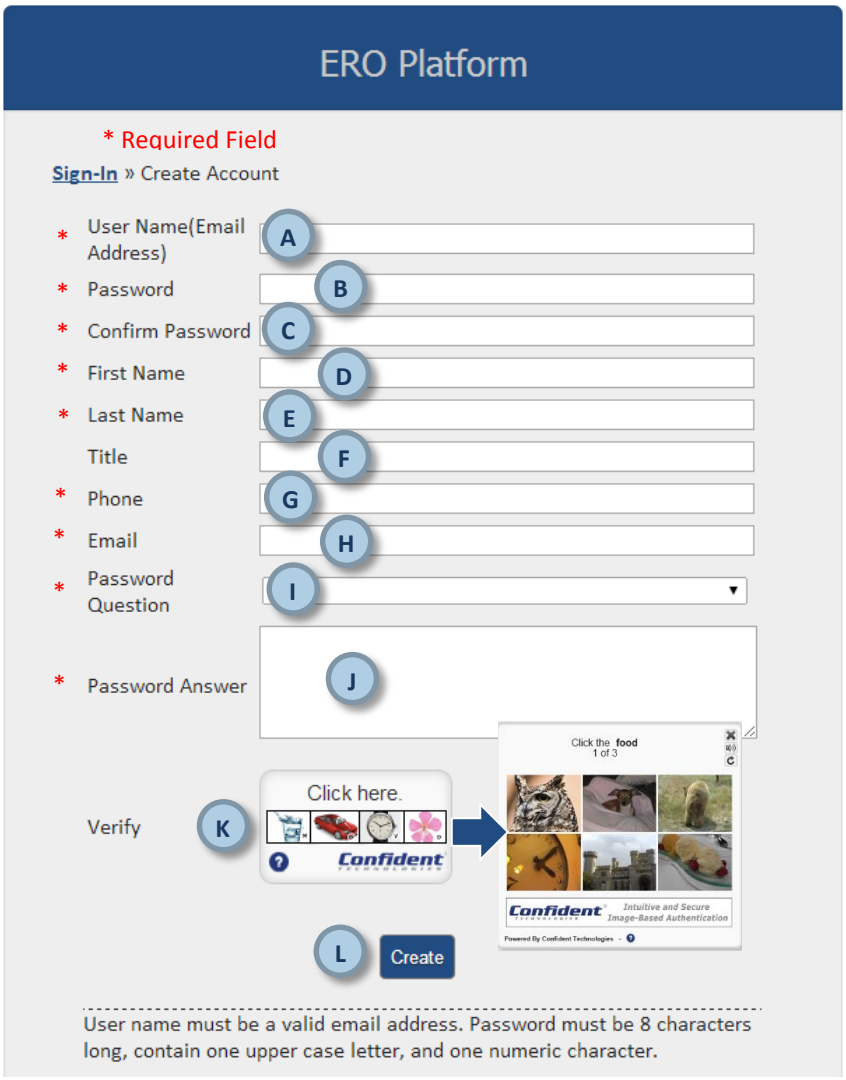


Figure 2: Create Account Screen

To create a new account,

A. Enter a **User Name** (MUST be a business email address - this can be the same email in step H).
B. Enter a **Password**. As the on-screen instructions indicate, this password:
    a. Must be at least eight (8) characters in length.
    b. Must contain at least one uppercase letter.
    c. Must contain at least one numeric character.
C. Re-enter the **Password**.
D. Enter the user's **First Name**.
E. Enter the user's **Last Name**.
F. Enter the user's **Title**.
G. Enter a valid business **Phone Number** where the user may be reached.
H. Enter an **Email Address**. This ***MUST*** be a valid email address, as it will be used to send ***ALL*** notifications of actions and status updates within the system. Both **User Name** and **Email Address** may be the same.
NOTE: Changing this field does not change a user's username.
I. For security purposes, select a **Password Question** from the list of questions.
J. Enter the **Password Answer** to the security question (I).
K. Select the **Verify** icon (K). Several images display. Select the correct image of each description as instructed until all three pictures have been verified.
L. Click the **Create** button (L).

Creating Account Step 2: Verify Account

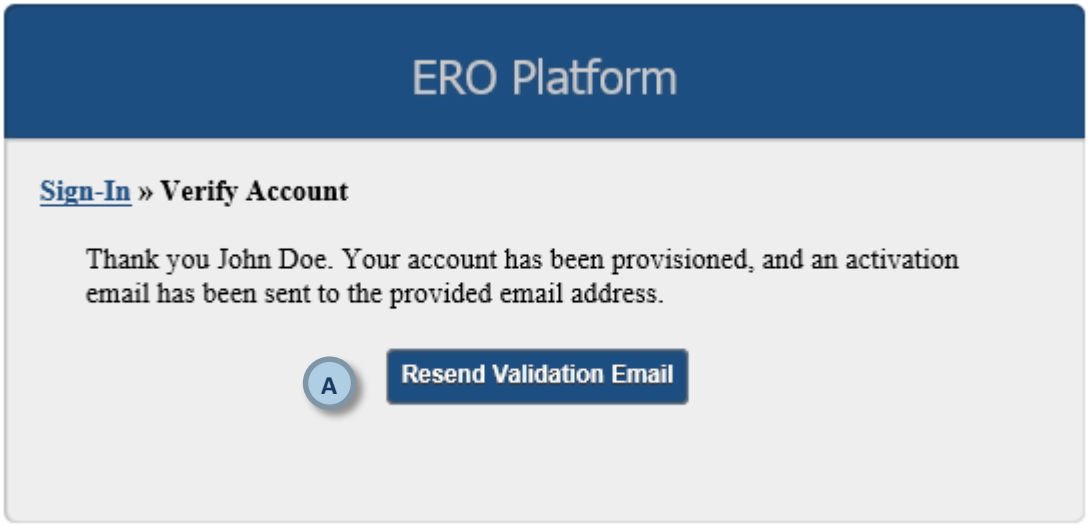


Figure 3: Verify Account Screen

Upon successful verification of the account information provided on the **Create Account** form, a verification email will be sent to the email account used to create your user account.

A. If you have not received the activation email, SELECT the **Resend Validation Email** (A) to have the activation email resent to the email address provided.

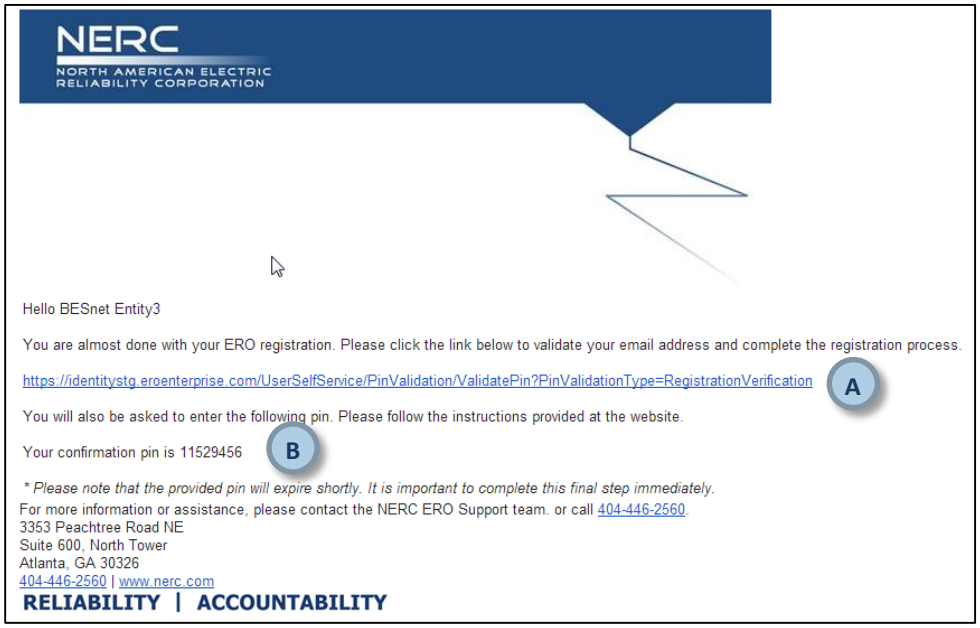


Figure 4: Sample Activation E-Mail

A. Click on the **link** (A) provided in the verification email above. The following screen will appear:

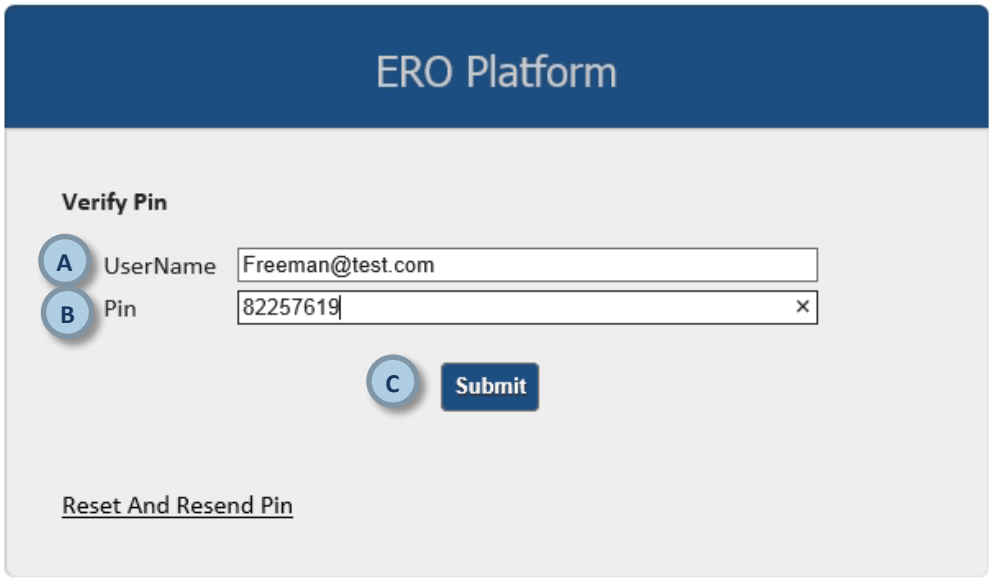


Figure 5: PIN Verification Screen

A. Enter your **User Name** (A).
B. Enter the **PIN** (B) contained in the verification email.
C. Click **Submit** (C).

PIN Expiration Procedure

If the PIN has expired, the following screen will appear:

NOTE: PINs expire 60 minutes after issuance.

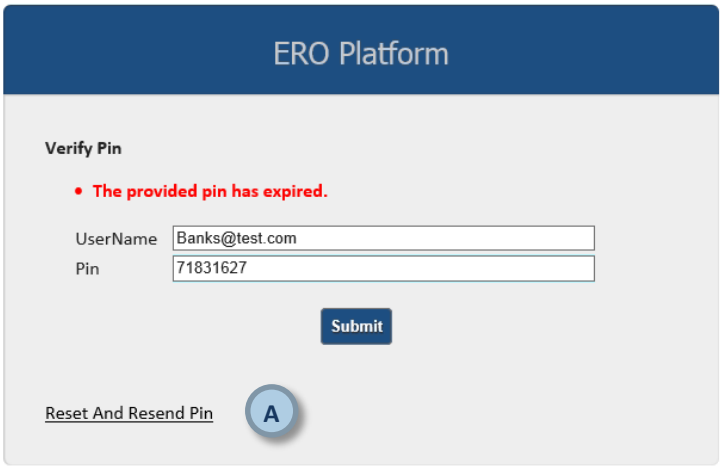


Figure 6: PIN Expiration Screen

A. Click on **Reset and Resend PIN** (A). A new verification email will be sent with a new PIN.

Once you have successfully created a user ID and it has been verified, the **ERO Platform Screen** will appear.

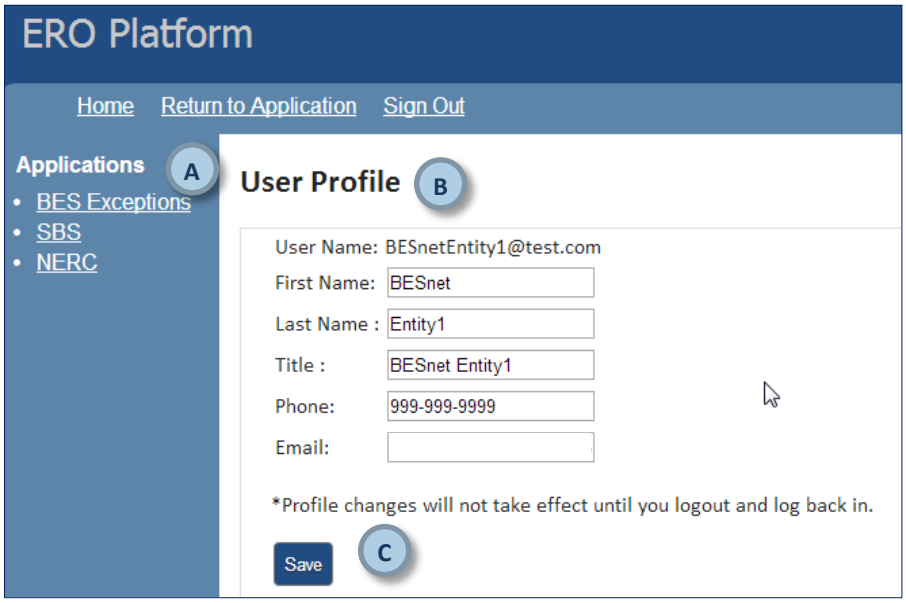


Figure 7: ERO Platform Screen

A. To enter the BESNet application, click on **BES Exceptions** (A).
B. At this screen, you also have the opportunity to modify your **User Profile** (B).If you have updated your profile, click **Save** (C) to save the changes.
Note: You will have to logout of the application and log back in for the profile changes to take effect.

Logging Into the BESNet Application

For users who already have an account, navigate to the BESnet application. Contact your Entity BESnet Administrator if you do not have the URL to the application.

A. Enter the **User Name** (A).
B. Enter the **Password** (B) entered during the user registration process defined in Section **Creating a New Account.**
C. If desired, check the **Remember me?** (C) Checkbox, which gives permission for the system to remember the credentials entered.
D. Once completed with these fields, complete the login process by pressing the **Sign In** (D) button.

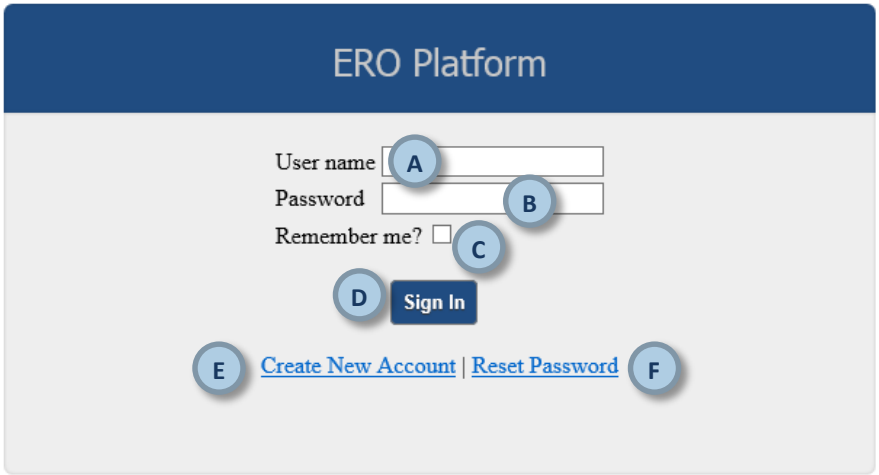


Figure 8: ERO Platform Log-In Screen

For users who do not have an account:

E. Click the **Create New Account** (E) link. See Section **Creating a New Account** for more details.

To reset your password.

F. Click the **Reset Password** (F) link. See Section **Resetting the User Password** for more details.

Selecting the User's Entity to Use

If the User has been vetted as a representative for more than one Entity, the User will first be prompted to select the Entity they wish to represent for the current session. Users who are only vetted for a single Entity will skip this step.

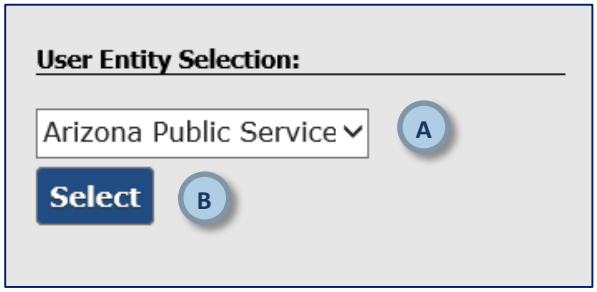


Figure 9: User Entity Selection Screen

To identify the Entity the User will represent during this session:

A. Select the **Entity Name** (A) from the Entity list. Only those for which this User has been vetted will appear.
B. Click the **Select** (B) button.

Setting up Your BESNet Application Account

Once your BESNet User ID has been established, you will need to finish setting up the functions of the new account. Navigate to the BESnet application. Contact your Entity BESnet Administrator is you do not have the URL to the application.

You will be shown your user profile.

Select the BES Exceptions tab on the left (A) of the **ERO Enterprise Platform Entry Page**.

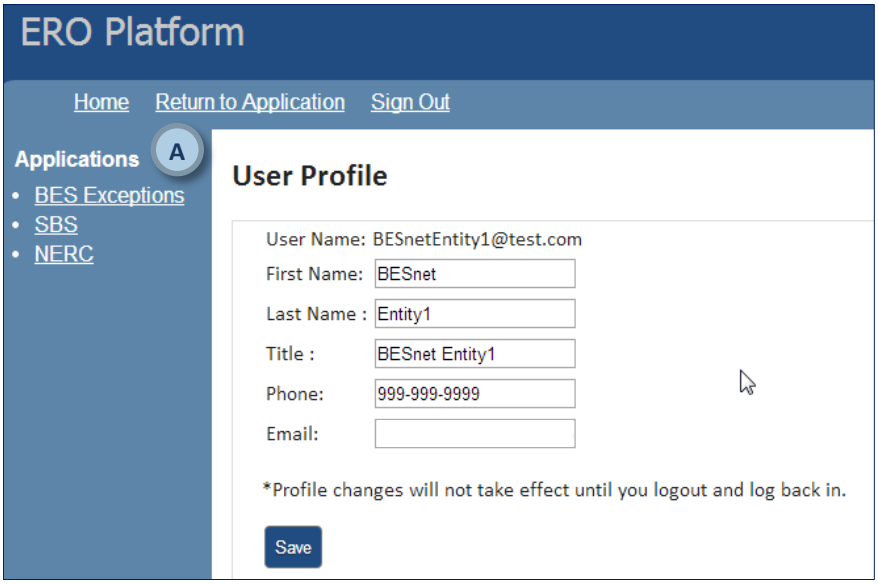


Figure 10: ERO Enterprise Platform Entry Page

Account Setup Step 1: Select Account Type

You must select an **Account Type**. Registered Entities may only select the Registered Entity account type.

A. Select Registered Entity as your **Account Type** (A).

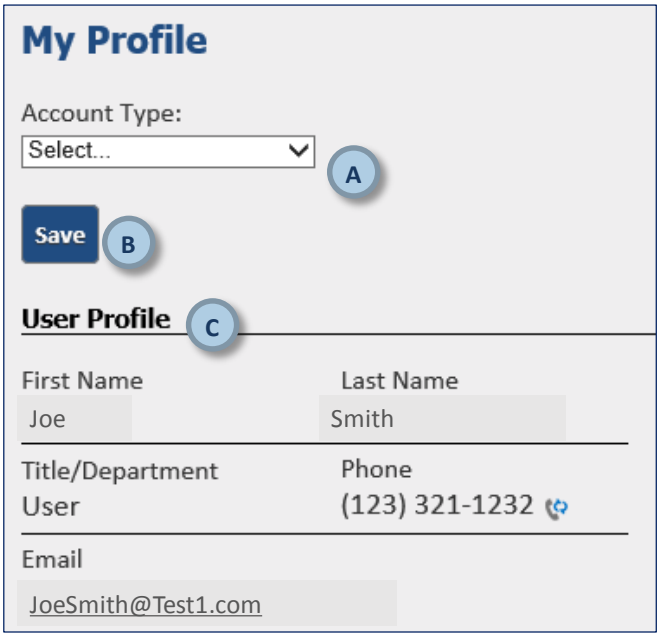


Figure 11: Account Type Selection Screen

Account Type	Description
Registered Entity	Accounts for members of the entities registered with NERC and/or the national Regions. Includes members of submitting, owning, and scope of responsibility entities.

NOTE: Each user account may only be created for a single account type. Account type selection is only available one time following new account creation. ***The account type cannot be changed once it has been selected.***

B. Click the **Save** button (B). This will take you to the **My Profile** screen.

NOTE: The user's profile information entered during the first step of account creation appears in the ***User Profile*** *area (C).*

Account Setup Step 2: Association of Account with Entities

The next step in the registration process is to associate the user's account with one or more Entities on the **My Profile Screen**.

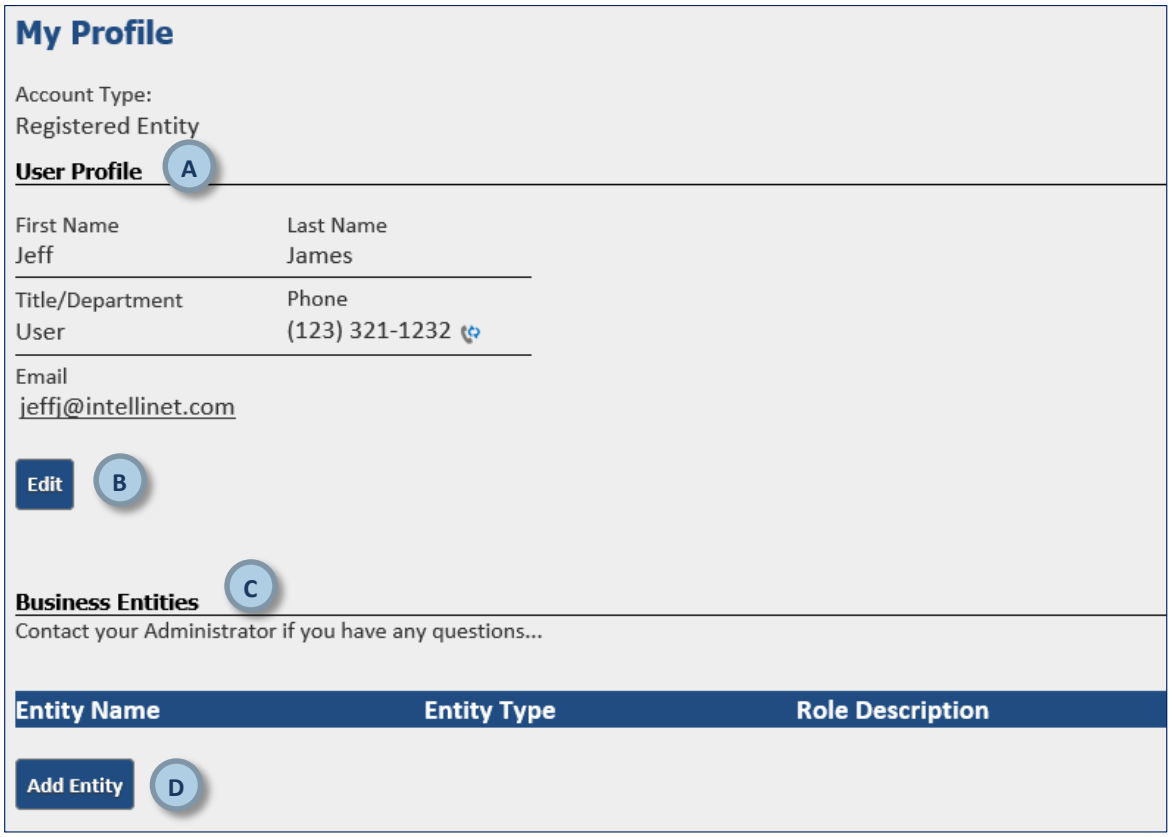


Figure 12: My Profile Screen

The next step in the registration process is to associate the account with one or more Entities.

A. View the User Profile information in the **User Profile** section (A).
B. If desired, edit the **User Profile** information by clicking the **Edit** button (B). See the **Editing Your User Profile** section for further details.
C. View the listing of the **Business Entities** (C) with which the account is currently associated in the **Business Entities** list. When initially registering, this list will be empty.
D. To associate the account with an Entity, click the **Add Entity** button (D). This displays the **Entity Listing Screen** allowing you to select the Entities to be applicable to this User.

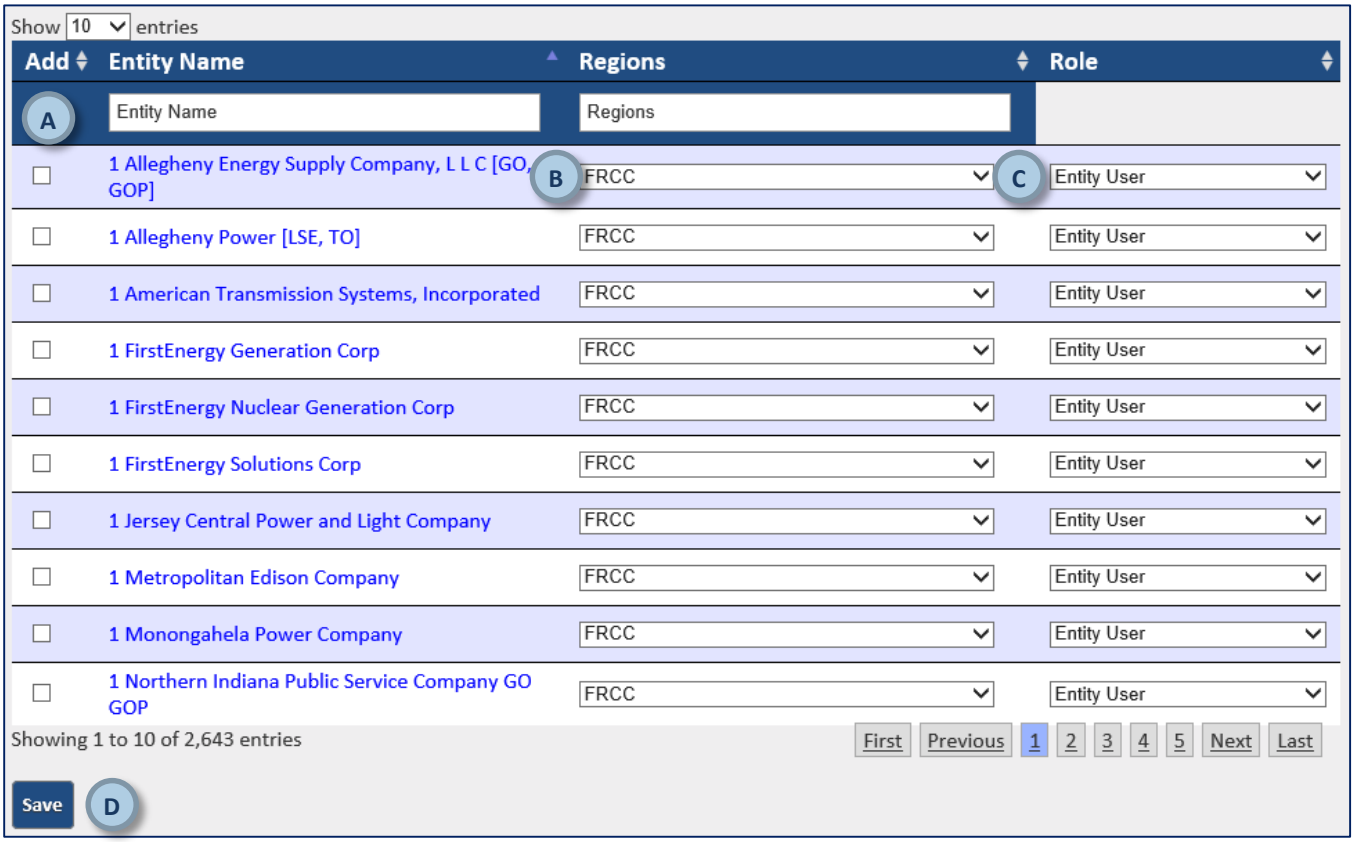


Figure 13: Entity Selection Screen

A. From this list, select the Entity to associate with the account by clicking the checkbox to the left of the Entity record, in the **Add** column (A).
   a. The Entity listing can be filtered by typing in the **Entity Name** filter textbox in the header (directly beneath the **Entity Name** label).

B. Select the **Region** (B) that will be responsible for vetting the user account if an administrator for this Registered Entity does not yet exist in the system. (If there is an Entity Administrator role already associated to the Registered Entity, a vetting request will be sent to that Entity Administrator).

   NOTE: Choosing the Regional Entity in this screen does not associate a Registered Entity to a Region within the system; this is only used for vetting requests for account access.

   NOTE: If you do not see your Entity listed in the list, contact your Regional Entity.

C. Select the **Role** (C) the account will perform for that Entity. Roles are:
   a. Entity User: A general user of the system.
   b. Entity Administrator: A user who has the ability to vet user accounts for that Registered Entity, as well as perform all functions of the Entity User role.

   NOTE: The system does not allow a user to change his or her role for an Entity. Instead, the Entity Administrator must remove the user's association with the Entity, after which the user must submit a new request to be associated to the Entity with the new role.

D. **Repeat steps A through C for each Entity to be associated with the account**. When complete, click the **Save** button(D). This will bring up the **Vetting Request Confirmation Screen**. This confirms that your request has been submitted to be vetted by the Entity Administrator(s) associated for each selected Entity (See the **Vetting Users** section for further detail), and the following screen will be displayed.

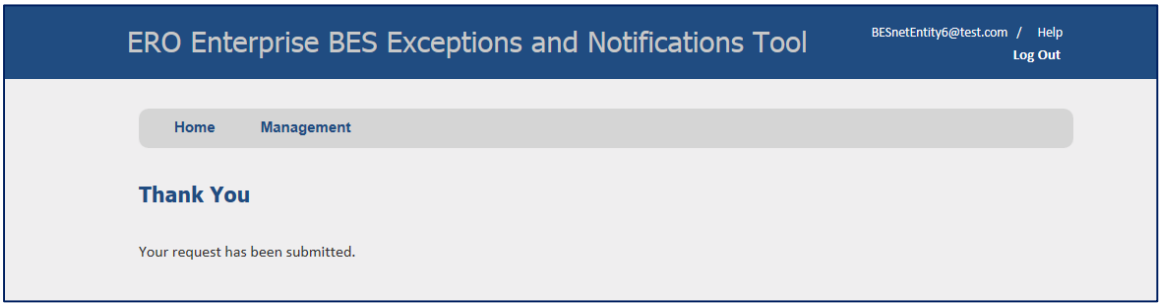


Figure 14: Vetting Request Confirmation Screen

The Entity User will be notified by e-mail when each association request has been vetted (approved or rejected).

If a request for association with an Entity has been rejected, there will be an e-mail notification that you have been rejected.

If the User has not received a vetting response within five business days, contact your Regional Entity or your Entity Administrator.

Once the account user has received notification that the request has been vetted and approved, the user will see the Entities associated with his account in the **My Profile Screen (A)**.

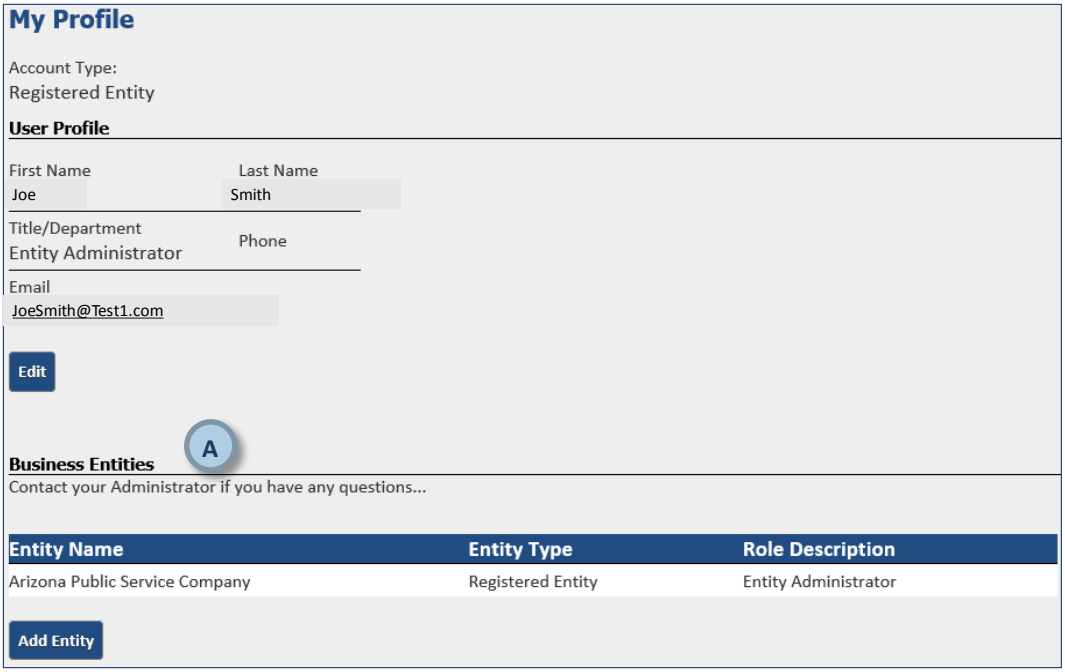


Figure 15: My Profile Screen with Entity Association

The user can then access the information for that Entity in the BESNet application.

Editing Your User Profile

To update your User Profile, enter the desired update(s) in the appropriate field on the **User Profile Screen** and press **Save** (A).

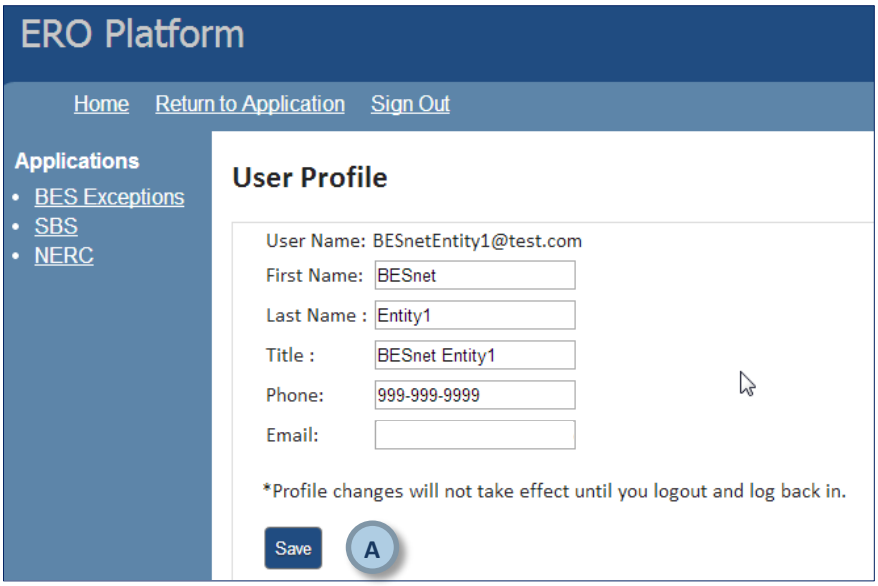


Figure 16: User Profile Screen

If your profile changes have been successful, the **Profile Update Confirmation Screen** will be displayed.

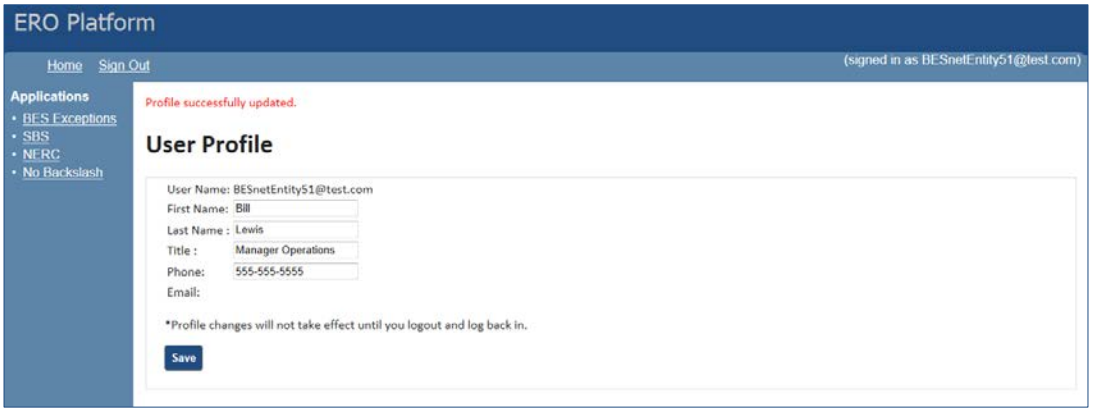


Figure 17: Profile Update Confirmation Screen

Log out and back into the BESNet application.

NOTE: Profile changes will NOT take effect until you log out and log back into the BESNet application.

Password Management

Changing User Password

A. If a User wishes to change his password, he should hover over the **User** tab in the header of the **BESNet Dashboard** and then click on the **My Profile** tab in the dropdown. This will bring you to the **My Profile Screen**.

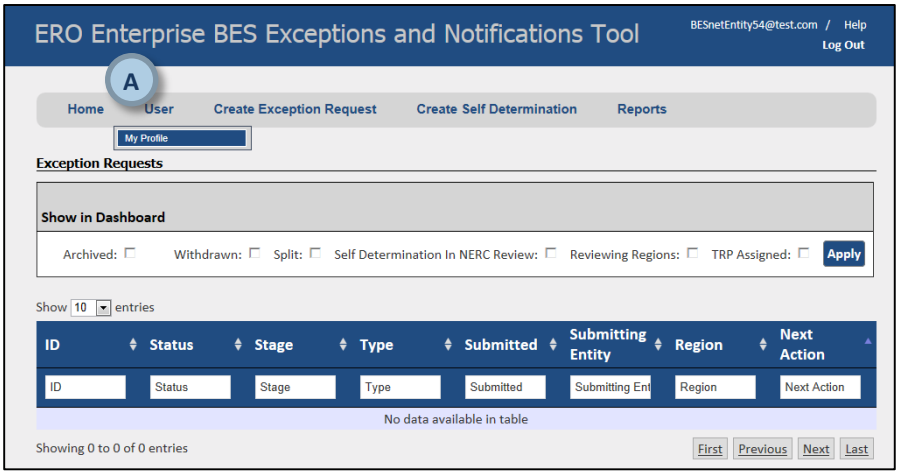


Figure 18: BESNet Home Page

B. Click on the **Edit** button (A) on the **My Profile Screen**. This will bring you to the **User Profile Screen**.

Figure 19: My Profile Screen

C. Click on the **Reset Password** link (A) under **Password** on the **User Profile Screen**.

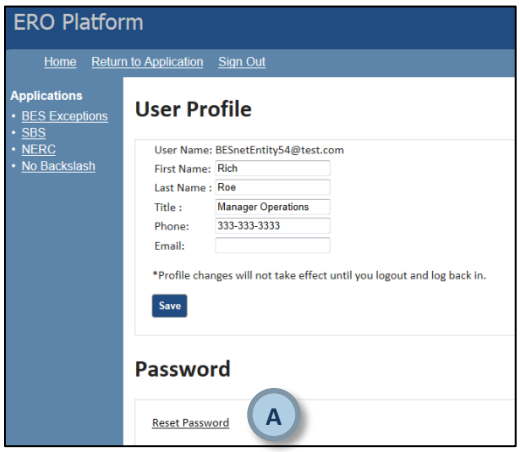


Figure 20: User Profile Screen

D. Continue from **Step B** of the **Forgot/Resetting the User Password** instructions below.

Forgot/Resetting the User Password

If a user has forgotten his password, the password must be reset.

A. To reset a user's password, the user should select **Reset Password** (A) from the **ERO Platform Log-In Screen**. The system then displays the **Password Reset Screen**.

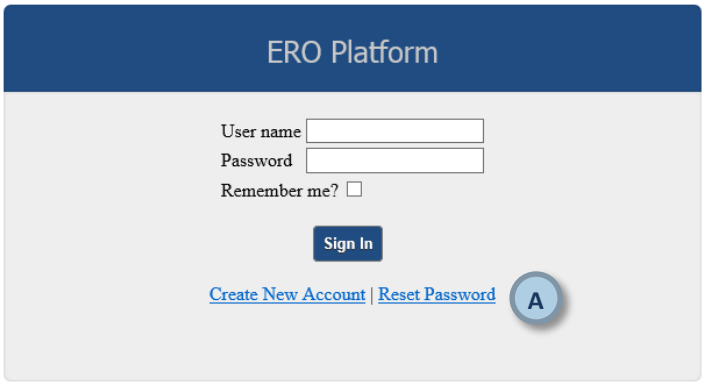


Figure 21: ERO Platform Log-In Screen

B. From the **Password Reset Screen**, the user can
- Enter the **User Name** (A).
- Enter the **Email Address** (B) associated to the Account
- Select the **Verify** icon (C). Several images display. Select the correct image of each description as instructed until all three pictures have been verified.
- Click the **Submit** (D) button.

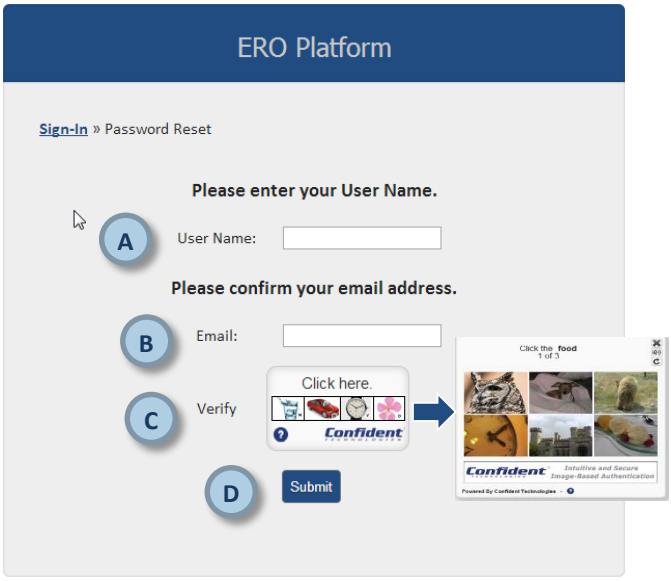


Figure 22: Password Reset Screen

C. The BESNet application will send a **Password Reset Request E-mail** to the user and display the **Password Reset Validation Screen**. If necessary, the User can request that the **Password Reset Request E-mail** be resent pressing the **Resend Validation Email** (A).

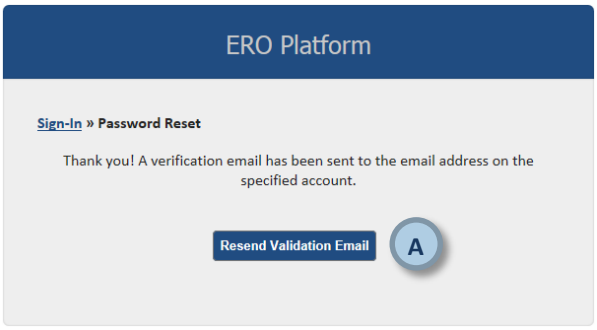


Figure 23: Password Reset Validation Screen

D. The User should then copy the **Confirmation Pin** (A) and click on the **URL** (B) for to change the password

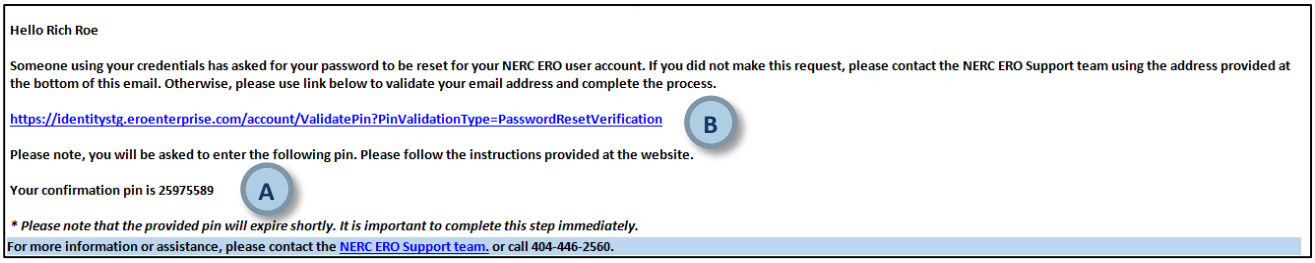


Figure 24: Password Reset Request E-mail

E. The User should then enter his **User Name** (A) and paste the **PIN** (B) on the **Verify Pin Screen** and press **Submit** (C).

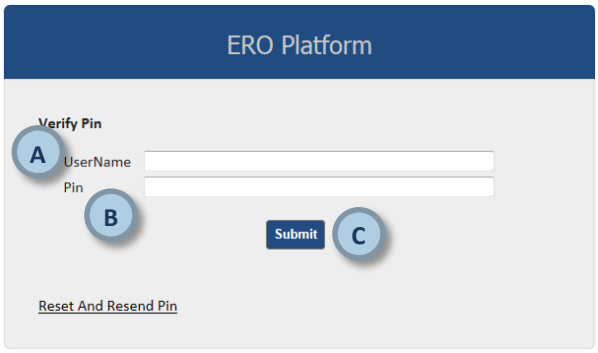


Figure 25: Verify Pin Screen

F. Once the PIN has been entered, the User must enter the **Password Answer** (A) selected during the registration process and click the **Submit Question** (B) button on the **Password Recovery Screen.**

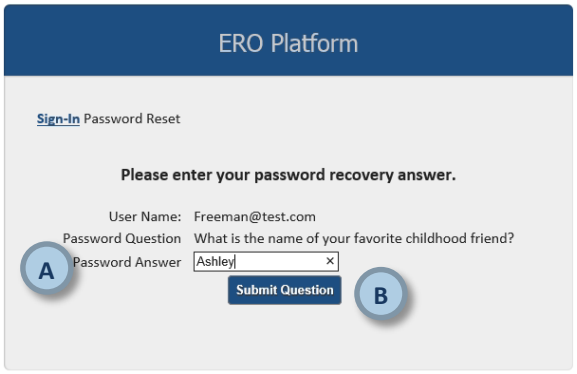


Figure 26: Password Recovery Screen

G. The User should then enter the desired **New Password** (A), Confirm Password (B), and click the **Save Password** (C) button on the **Enter Net Password Screen**.

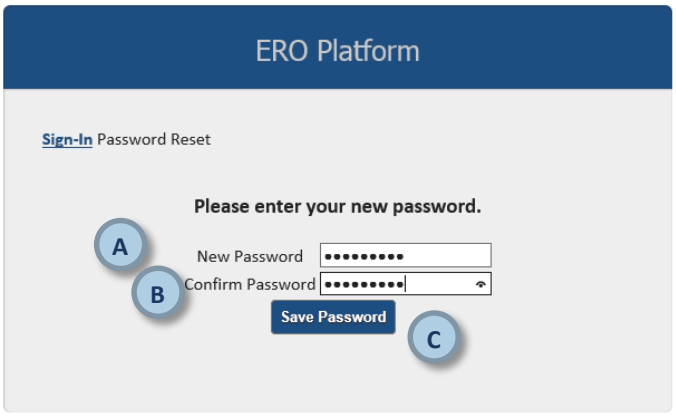


Figure 27: Enter New Password Screen

H. The BESNet application will send a **Password Change Confirmation E-mail** to the user and display the **User Profile Screen**.

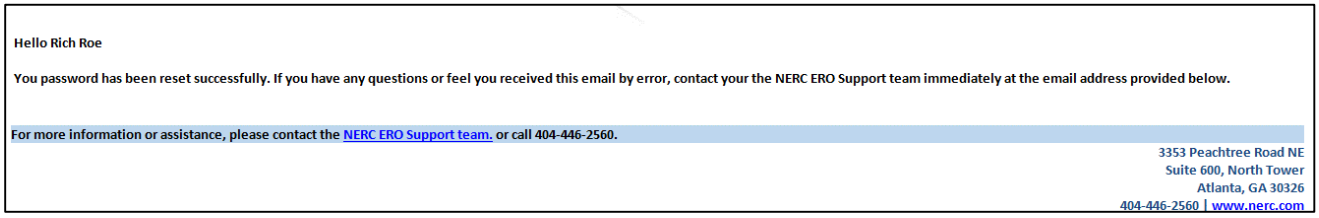


Figure 28: Password Change Confirmation E-mail

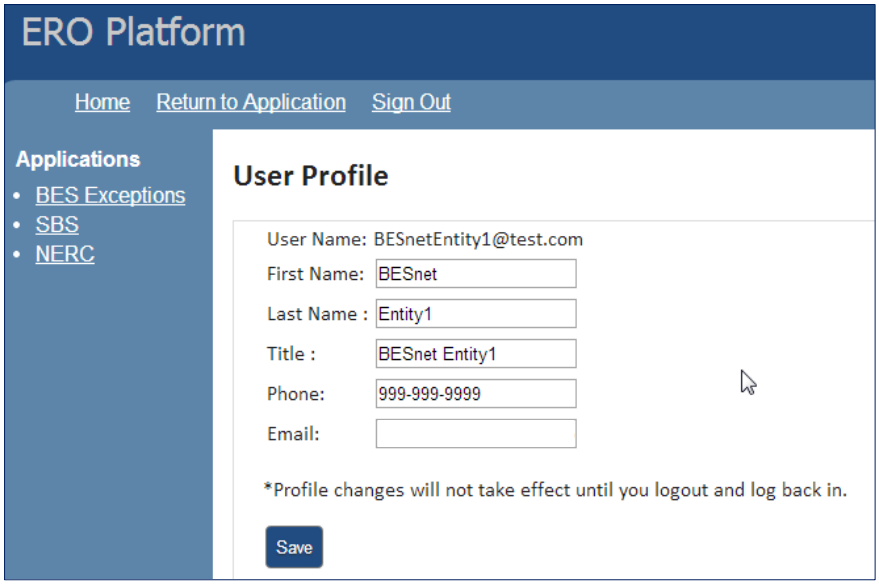


Figure 29: User Profile Screen

Managing Your User Account Properties

A User of the BESNet application can manage their account properties whenever they are logged on to the system. This allows them to edit their user profile or associate themselves with a new Entity. User can access their user account properties in one of two ways:

A. Clicking on the **User Name** in the upper right corner of the BESNet application screen.

Figure 30: BES Application Screen Header

A. Selecting **User > My Profile** from the dashboard menu.

Figure 31: Dashboard Menu Detail

These will display the **User Profile Management** screen.

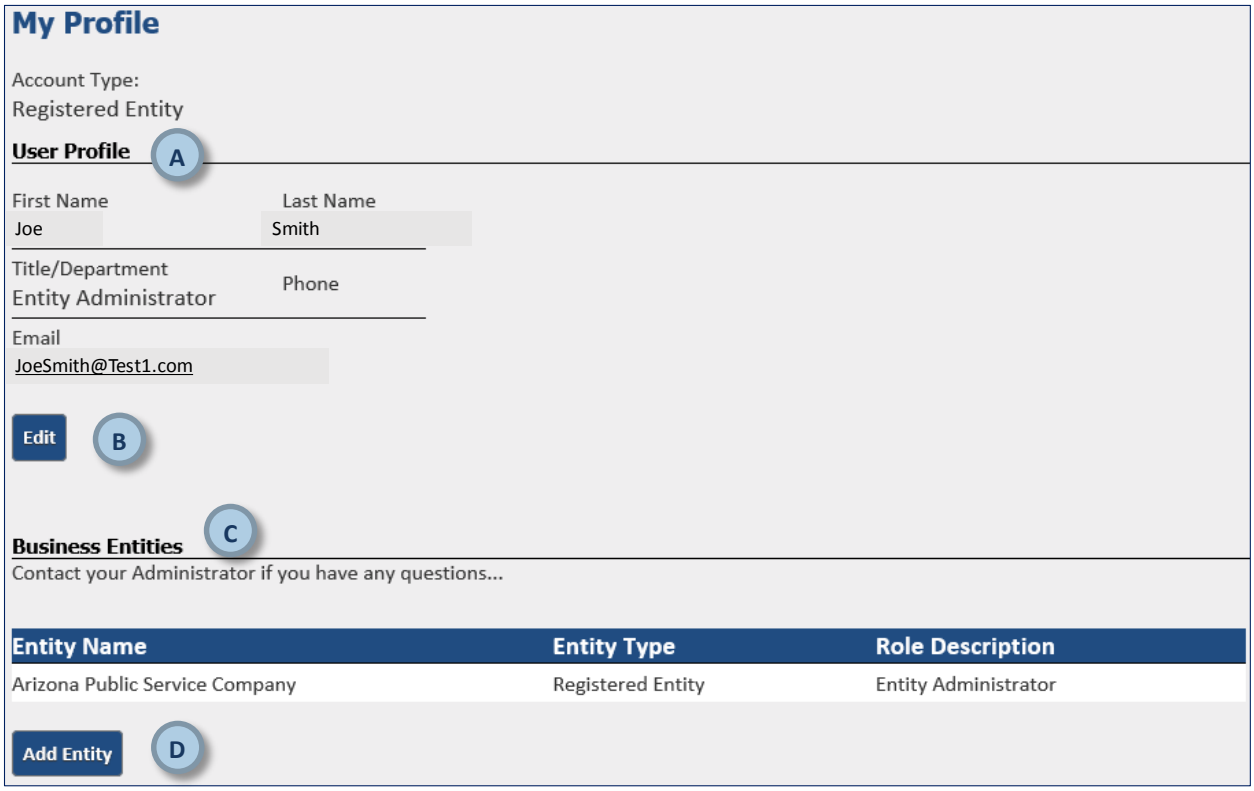


Figure 32: User Profile Management Screen

From here the user can:

A. View the **User Profile** (A) information.
B. Edit the **User Profile** information by clicking the **Edit** button (B).
C. View the listing of **Business Entities** (C) for which the user has access or has requested access.
D. Add an additional Business Entity request, by clicking the **Add Entity** (D) button.

Logging Out

To log out of the system, click the **Log Out** link (A) at the upper right of the BESNET system screen.

Figure 33: BESNet System Screen Header

Administrator User Account Management

Administrative User Management

The Administrator of a Registered Entity has the ability to vet new user account requests and manage users' roles within the Entity.

The Administrator will be notified by email of new user account requests.

To perform this function, on the **BESNet Dashboard** the Administrator should click **User** > **User Administration** pull-down menu (A).

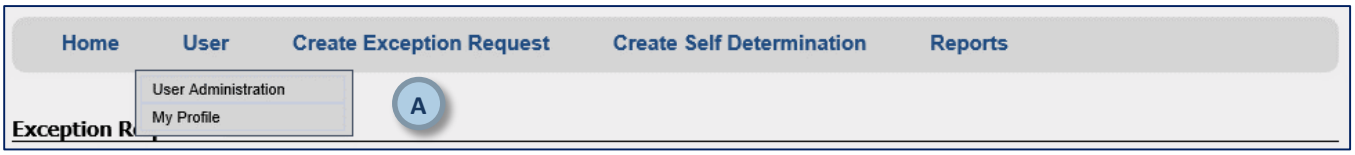


Figure 34: BESNet Dashboard Header

Vetting New Users

On the **User Management Screen**, the Administrator will see a **Vet Requests** list, containing a listing of all users who have requested accounts associated with the Registered Entity for which the user has Administrative privileges.

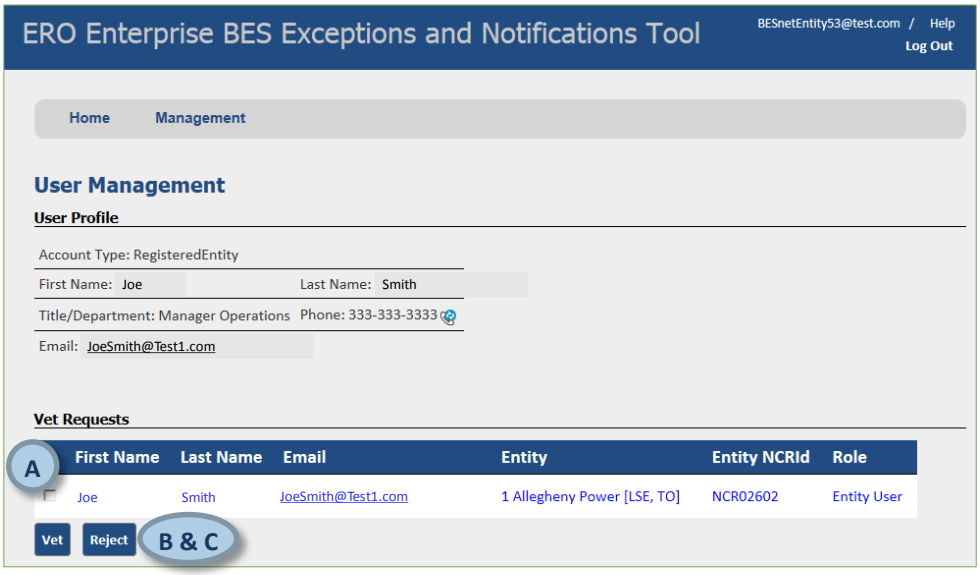


Figure 35: User Management Screen

A. Check the checkbox (A) next to each record to select it as one to approve or reject.
B. To approve the selected request(s), click the **Vet** button (B).
C. To reject the selected request(s), click the **Reject** button (C).

The decision to approve or reject the request will be e-mailed to the user.

User Role Management

The Administrator is responsible for management of the roles of all of the users within his purview.

A. To perform this function, on the **BESNet Dashboard** the Administrator should click **User** > **User Administration** pull-down menu (A). This will bring you to the User Management Screen

Figure 36: BESNet Dashboard Header

The **User Management** on the lower part of the **User Management Screen** displays a list of all users for which the user has Administrator privileges.

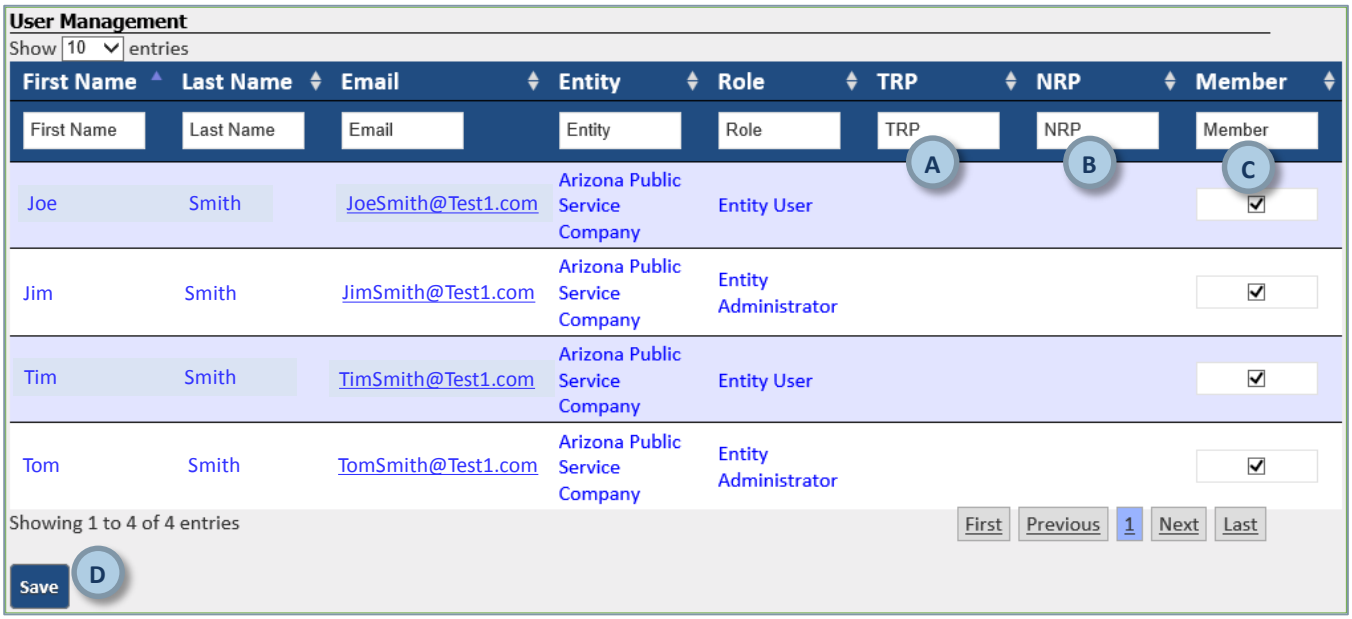


Figure 37: User Management Screen

A. The **Technical Review Panel** (TRP) membership can only be set by a **Regional Administrator**, and therefore cannot be set here.
B. The **NERC Review Panel** (NRP) membership can only be set by a **NERC Administrator**, and therefore cannot be set here.
C. To disassociate a user account from the Entity, uncheck the **Member** checkbox (C) for that account/Entity relationship. By default, all vetted members appear checked in the **Member** checkbox (C).
D. Once all the role changes have been made, click the **Save** button (D).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Request for Public Comment on Proposed Request for Data or Information

Survey Regarding the Scope of the Term "BES Cyber Asset"

5/30/2014

RELIABILITY | ACCOUNTABILITY

Introduction and Survey Scope

The North American Electric Reliability Corporation ("NERC") requests public comment by 8:00 p.m. EST, July 14, 2014 on its proposal to collect data (the "Data Request") pursuant to Section 1600 of the NERC *Rules of Procedure* ("ROP")[1] regarding the scope of the term "BES Cyber Asset," as defined in NERC's *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary"). Comments must be submitted in an electronic document to BESCyberAssetSurvey@nerc.net.

After the close of this comment period, NERC will make any necessary revisions to the proposed Data Request based on comments received and submit the proposed Data Request, as revised, along with the comments received, NERC's evaluation of the comments, and recommendations, to the NERC Board of Trustees for authorization to issue the Data Request. Upon NERC Board of Trustees approval, the proposed Data Request will be issued and become mandatory.

In accordance with Section 1600 of the ROP, NERC may request data or information from Registered Entities that is necessary to meet NERC's obligations under Section 215 of the Federal Power Act, as authorized by Section 39.2(d)[2] of the regulations of the Federal Energy Regulatory Commission ("FERC" or "Commission").

The purpose of the proposed Data Request is to respond to FERC's directive from Order No. 791[3] to conduct a survey regarding the scope of the term "BES Cyber Asset" and submit an informational filing based on the data collected. Specifically, in Order No. 791, FERC approved new and modified Critical Infrastructure Protection ("CIP") Reliability Standards, referred to as the CIP Version 5 Standards, as well as new and modified terms to be incorporated into the NERC Glossary. Among others, FERC approved the following definition for the term "BES Cyber Asset":

> A Cyber Asset that if rendered unavailable, degraded, or misused would, *within 15 minutes of its required operation, misoperation, or non-operation*, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (*Emphasis added*)

To better understand the scope and reach of the term "BES Cyber Asset," the Commission directed NERC to conduct a survey of responsible entities during the implementation period for the CIP Version 5 Reliability Standards to determine the types of Cyber Assets that are included

[1] NERC's *Rules of Procedure* are available at: http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20111117.pdf.

[2] 18 C.F.R. § 39.2(d) (2013).

[3] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013).

or excluded from the definition of BES Cyber Asset due to the 15-minute parameter.[4] Based on the survey data, NERC is required to explain, in an informational filing due within one year of the effective date of Order No. 791, the following: (1) specific ways in which entities determine which Cyber Assets meet the 15-minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition.[5] This proposed Data Request is designed to satisfy the Commission's directive to conduct a survey of responsible entities on the scope of the term "BES Cyber Asset" and to collect the data necessary for the informational filing.

This request for public comment satisfies NERC's obligation under Section 1602.2 of the ROP to post a proposed Data Request for a 45-day public comment period prior to obtaining NERC Board of Trustee authorization to issue the Data Request.[6] In accordance with Section 1602.2.1 of the ROP, this request for public comment contains the following information:

1. a description of the data or information to be requested, how the data or information will be used, and how the availability of the data or information is necessary for NERC to meet its obligations under applicable laws and agreements;

2. a description of how the data or information will be collected and validated;

3. a description of the entities (by functional class and jurisdiction) that will be required to provide the data or information ("Reporting Entities");

4. the schedule or due date for the data or information;

5. a description of any restrictions on disseminating the data or information (e.g., "confidential," "critical energy infrastructure information," "aggregating" or "identity masking"); and

6. an estimate of the relative burden imposed on the reporting entities to accommodate the data or information request.

[4] Order No. 791 at PP 123-125.

[5] Order No. 791 at P 124.

[6] Consistent with Section 1602.1, NERC provided the proposed Data Request to the Commission's Office of Electric Reliability on April 18, 2014.

NERC Contact Information

If you have any questions regarding this request for public comment, please contact Scott Mix, CIP Technical Manager, Critical Infrastructure Department, at 215-853-8204 or by e-mail at Scott.Mix@nerc.net.

Alternate NERC Point(s) of Contact:

Nicholas Santora
CIP Cybersecurity Specialist
Critical Infrastructure Division
404.446.9690
Nicholas.Santora@nerc.net

Felek Abbas
CIP Compliance Auditor, CIP & Operations Assurance
202-400-3017
Felek.Abbas@nerc.net

Marisa Hecht
Standards Developer, Standards
404-446-9620
Marisa.Hecht@nerc.net

Ryan Stewart
Standards Developer, Standards
202-844-8091
Ryan.Stewart@nerc.net

Authority

Under Section 215 of the Federal Power Act (16 U.S.C. § 824o), Congress entrusted FERC with the duties of approving and enforcing rules to ensure the reliability of the Nation's Bulk Power System, and with the duties of certifying an Electric Reliability Organization ("ERO") that would be charged with developing and enforcing mandatory Reliability Standards, subject to FERC approval. NERC was certified as the ERO on July 20, 2006. NERC's authority for issuing this survey is derived from Section 215 of the Federal Power Act, and from the following sources:

Section 39.2(d) of the Commission's regulations (18 C.F.R. §39.2(d)), which provides:

> Each user, owner or operator of the Bulk-Power System within the United States (other than Alaska and Hawaii) shall provide the Commission, the Electric Reliability Organization and the applicable Regional Entity such information as is necessary to implement section 215 of the Federal Power Act as determined by the Commission and set out in the Rules of the Electric Reliability Organization and each applicable Regional Entity. The Electric Reliability Organization and each Regional Entity shall provide the Commission such information as is necessary to implement section 215 of the Federal Power Act.

NERC Rules of Procedure Section 1600, which provides:

> ***1601. Scope of a NERC or Regional Entity Request for Data or Information***
>
> *Within the United States, NERC and regional entities may request data or information that is necessary to meet their obligations under Section 215 of the Federal Power Act, as authorized by Section 39.2(d) of the Commission's regulations, 18 C.F.R. § 39.2(d). In other jurisdictions NERC and regional entities may request comparable data or information, using such authority as may exist pursuant to these rules and as may be granted by ERO governmental authorities in those other jurisdictions. The provisions of Section 1600 shall not apply to requirements contained in any Reliability Standard to provide data or information; the requirements in the Reliability Standards govern. The provisions of Section 1600 shall also not apply to data or information requested in connection with a compliance or enforcement action under Section 215 of the Federal Power Act, Section 400 of these Rules of Procedure, or any procedures adopted pursuant to those authorities, in which case the Rules of Procedure applicable to the production of data or information for compliance and enforcement actions shall apply.*

1602. Procedure for Authorizing a NERC Request for Data or Information

1. *NERC shall provide a proposed request for data or information or a proposed modification to a previously-authorized request, including the information specified in paragraph 1602.2.1 or 1602.2.2 as applicable, to the Commission's Office of Electric Reliability at least twenty-one (21) days prior to initially posting the request or modification for public comment. Submission of the proposed request or modification to the Office of Electric Reliability is for the information of the Commission. NERC is not required to receive any approval from the Commission prior to posting the proposed request or modification for public comment in accordance with paragraph 1602.2 or issuing the request or modification to reporting entities following approval by the Board of Trustees.*

2. *NERC shall post a proposed request for data or information or a proposed modification to a previously authorized request for data or information for a forty-five (45) day public comment period.*

2.1. *A proposed request for data or information shall contain, at a minimum, the following information: (i) a description of the data or information to be requested, how the data or information will be used, and how the availability of the data or information is necessary for NERC to meet its obligations under applicable laws and agreements; (ii) a description of how the data or information will be collected and validated; (iii) a description of the entities (by functional class and jurisdiction) that will be required to provide the data or information ("reporting entities"); (iv) the schedule or due date for the data or information; (v) a description of any restrictions on disseminating the data or information (e.g., "confidential," "critical energy infrastructure information," "aggregating" or "identity masking"); and (vi) an estimate of the relative burden imposed on the reporting entities to accommodate the data or information request.*

2.2. *A proposed modification to a previously authorized request for data or information shall explain (i) the nature of the modifications; (ii) an estimate of the burden imposed on the reporting entities to accommodate the modified data or information request, and (iii) any other items from paragraph 1.1 that require updating as a result of the modifications.*

3. *After the close of the comment period, NERC shall make such revisions to the proposed request for data or information as are appropriate in light of the comments. NERC shall submit the proposed request for data or information, as revised, along with the comments received, NERC's evaluation of the comments and recommendations, to the Board of Trustees.*

4. *In acting on the proposed request for data or information, the Board of Trustees may authorize NERC to issue it, modify it, or remand it for further consideration.*

5. *NERC may make minor changes to an authorized request for data or information without board approval. However, if a reporting entity objects to NERC in writing to such changes within 21 days of issuance of the modified request, such changes shall require board approval before they are implemented.*

6. *Authorization of a request for data or information shall be final unless, within thirty (30) days of the decision by the Board of Trustees, an affected party appeals the authorization under this Section 1600 to the ERO governmental authority.*

1603. Owners, Operators, and Users to Comply

Owners, operators, and users of the bulk power system registered on the NERC Compliance Registry shall comply with authorized requests for data and information. In the event a reporting entity within the United States fails to comply with an authorized request for data or information under Section 1600, NERC may request the Commission to exercise its enforcement authority to require the reporting entity to comply with the request for data or information and for other appropriate enforcement action by the Commission. NERC will make any request for the Commission to enforce a request for data or information through a non-public submission to the Commission's enforcement staff.

1605. Confidentiality

If the approved data or information request includes a statement under Section 1602.1.1(v) that the requested data or information will be held confidential or treated as Critical Energy Infrastructure Information, then the applicable provisions of Section 1500 will apply without further action by a Submitting Entity. A Submitting Entity may designate any other data or information as Confidential Information pursuant to the provisions of Section 1500, and NERC or the Regional Entity shall treat that data or information in accordance with Section 1500. NERC or a Regional Entity may utilize additional protective procedures for handling particular requests for data or information as may be necessary under the circumstances.

1606. Expedited Procedures for Requesting Time-Sensitive Data or Information

1. *In the event NERC or a Regional Entity must obtain data or information by a date or within a time period that does not permit adherence to the time periods specified in Section 1602, the procedures specified in Section 1606 may be used to obtain the data or information. Without limiting the circumstances in which the procedures in Section*

1606 may be used, such circumstances include situations in which it is necessary to obtain the data or information (in order to evaluate a threat to the reliability or security of the Bulk Power System, or to comply with a directive in an order issued by the Commission or by another Applicable Governmental Authority) within a shorter time period than possible under Section 1602. The procedures specified in Section 1606 may only be used if authorized by the NERC Board of Trustees prior to activation of such procedures.

2. *Prior to posting a proposed request for data or information, or a modification to a previously-authorized request, for public comment under Section 1606, NERC shall provide the proposed request or modification, including the information specified in paragraph 1602.2.1 or 1602.2.2 as applicable, to the Commission's Office of Electric Reliability. The submission to the Commission's Office of Electric Reliability shall also include an explanation of why it is necessary to use the expedited procedures of Section 1606 to obtain the data or information. The submission shall be made to the Commission's Office of Electric Reliability as far in advance, up to twenty-one (21) days, of the posting of the proposed request or modification for public comments as is reasonably possible under the circumstances, but in no event less than two (2) days in advance of the public posting of the proposed request or modification.*

3. *NERC shall post the proposed request for data or information or proposed modification to a previously-authorized request for data or information for a public comment period that is reasonable in duration given the circumstances, but in no event shorter than five (5) days. The proposed request for data or information or proposed modification to a previously-authorized request for data or information shall include the information specified in Section 1602.2.1 or 1602.2.2, as applicable, and shall also include an explanation of why it is necessary to use the expedited procedures of Section 1606 to obtain the data or information.*

4. *The provisions of Sections 1602.3, 1602.4, 1602.5 and 1602.6 shall be applicable to a request for data or information or modification to a previously-authorized request for data or information developed and issued pursuant to Section 1606, except that (a) if NERC makes minor changes to an authorized request for data or information without Board approval, such changes shall require Board approval if a Reporting Entity objects to NERC in writing to such changes within five (5) days of issuance of the modified request; and (b) authorization of the request for data or information shall be final unless an affected party appeals the authorization of the request by the Board of Trustees to the Applicable Governmental Authority within five (5) days following the decision of the Board of Trustees authorizing the request, which decision shall be promptly posted on NERC's website.*

Proposed Data Request

NERC proposes to issue the Data Request provided below to comply with FERC's directives from Order No. 791 to conduct a survey of responsible entities during the implementation period for the CIP Version 5 Reliability Standards to determine the types of Cyber Assets that are included or excluded from the definition of BES Cyber Asset. The proposed Data Request has two parts.

In Part 1 of the Data Request, NERC requests that Balancing Authorities, Distribution Providers (as described in Applicability Section 4.1.2 of Reliability Standard CIP-003-5), Generator Operators, Generator Owners, Interchange Coordinators or Interchange Authorities, Reliability Coordinators, Transmission Operators, and Transmission Owners, as applicable, provide data on (1) the number of Control Centers, transmission stations or substations, or generation plants that they own or operate; and (2) the types and number of Cyber Assets at each of those locations (i.e., their Control Centers, Transmission stations or substations, or generation plants) that are included or excluded from the definition of BES Cyber Asset.

To lessen the burden on entities in responding to Part 1 of the Data Request and aid NERC's analysis of the data, NERC has created tables to be completed by applicable entities that list the Cyber Assets commonly installed and used at Control Centers, transmission stations or substations, or generation plants. For an explanation of the listed Cyber Assets and examples of their functional uses, please refer to Attachment 1 hereto.

In Part 2 of the Data Request, NERC requests that applicable entities provide a description of the process they are using or will use to determine if a particular Cyber Asset is categorized as a BES Cyber Asset, including how an entity determines if a particular piece of equipment is a Cyber Asset, and whether the Cyber Asset meets the 15-minute parameter.

Below is the proposed Data Request:

***Part 1**: Please provide the information requested below with respect to the Cyber Assets contained in your Control Centers, transmission stations or substations, and generation plants, as applicable.*

I. *Control Centers:*

For purposes of identifying Control Centers under this survey, if you have separate locations that contain the operating elements (i.e., control room where System Operators interact with HMI devices) and data centers (i.e., "computer rooms" containing servers, data communications and data storage), please count each location separately in the count of Control Center locations. Alternatively, if you have a one-to-one relationship between the operating and data centers, and they are located in the same building or location, only count those as a single location.

a. *Please specify the total number of Control Centers you own or operate: _____*

   i. *Please specify the number of Control Centers you own or operate that meet the description of a Control Center in Section 1 (High Impact Rating) of Attachment 1 to CIP-002-5.1: _____*

   ii. *Please specify the number of Control Centers you own or operate that meet the description of a Control Center in Section 2 (Medium Impact Rating) of Attachment 1 to CIP-002-5.1: _____*

   iii. *Please specify the number of Control Centers you own or operate that meet the description of a Control Center in Section 3 (Low Impact Rating) of Attachment 1 to CIP-002-5.1: _____*

   iv. *If the total number of Control Centers you own or operate identified above does not equal the sum of High, Medium, and Low Impact Control Centers identified in parts i, ii, and iii, please explain why:*

   _____

   _____

b. *Please complete the tables below for each Control Center you own or operate that contain the specified Cyber Assets in the ranges provided. (For example, if you have two Control Centers, one of which has three application servers and meets the description in Section 2.12 of Attachment 1 to CIP-002-5.1 (Medium Impact) and the other with 11 application servers that meets the description in Section 1.3 of Attachment 1 (High Impact), you would complete the two separate tables, one for the Medium Impact Control Center and one for the High Impact*

Control Center. For the Medium Impact Control Center table you would enter X in the row for application servers under the 1-4 column and indicate it is a Medium Impact Control Center, and in a separate table, mark an X under the 10-19 column and indicate it is a High Impact Control Center.) In addition, many of the Cyber Assets performing the functions described below perform multiple functions. When responding to the survey, only account for each Cyber Asset once, picking the most applicable function performed by the Cyber Asset.

(For an example of how to complete the tables, please see Attachment 2, hereto.)

For Cyber Assets that Meet the Definition of BES Cyber Asset at Control Centers ***Type of Control Center: _____ (Select High, Medium, or Low)***							
Type of Cyber Asset	***Number of Cyber Assets at Each Control Center***						
	0	*1-4*	*5-9*	*10-19*	*20-39*	*40-59*	*> 60*
Application Servers							
Data Servers							
HMI Workstations							
Network Printer							
Data Acquisition							
Data interchange							
PDC							
Computer Networking							
Communications Processing							
Diagnostic							
Fault Recorder							
Historian							
Situational Awareness							
Precision Time Device							
Training Simulator							
Development & Testing							
Infrastructure Support							
Marketing Systems							

Physical Access Control System							
Locally Mounted Physical Security							
*Other **							

** Please describe the type and function(s) of the Cyber Asset(s):*

_____

_____

For Cyber Assets that do <u>NOT</u> Meet the Definition of BES Cyber Asset at Control Centers							
Type of Control Center: _____ (Select High, Medium, or Low)							
Type of Cyber Asset	***Number of Cyber Assets at Each Control Center***						
	0	*1-4*	*5-9*	*10-19*	*20-39*	*40-59*	*> 60*
Application Servers							
Data Servers							
HMI Workstations							
Network Printer							
Data Acquisition							
Data interchange							
PDC							
Computer Networking							
Communications Processing							
Diagnostic							
Fault Recorder							
Historian							
Situational Awareness							

Precision Time Device							
Training Simulator							
Development & Testing							
Infrastructure Support							
Marketing Systems							
Physical Access Control System							
Locally Mounted Physical Security							
*Other **							

** Please describe the type and function(s) of the Cyber Asset(s):*

_____

_____

c. *Please describe the functions performed by the Cyber Assets that do not meet the 15-minute impact threshold, and the rationale for not including them.*

_____

_____

d. *Please also describe, if applicable, why Cyber Assets or functions performed by the Cyber Assets are excluded from the definition of BES Cyber Asset for a reason other than the 15-minute impact threshold.*

_____

_____

II. ***Transmission Station / Substation:***

a. *Please specify the total number of transmission stations and substations you own or operate:* _____

i. *Please specify the number of transmission stations and substations you own or operate that meet the description of a transmission station or substation in Section 2 (Medium Impact Rating) of Attachment 1 to CIP-002-5.1: _____*

ii. *Please specify the number of transmission stations and substations you own or operate that meet the description of a transmission station or substation in Section 3 (Low Impact Rating) of Attachment 1 to CIP-002-5.1: _____*

iii. *If the total number of transmission stations and substations you own or operate identified above does not equal the sum of Medium and Low Impact transmission stations and substations identified in parts i and ii, please explain why:*

_____

_____

b. *Please complete the tables below for each Medium Impact transmission station or substation you own or operate that contain the specified Cyber Assets in the ranges provided. For Low Impact transmission stations or substations you own or operate, you do not have to use a separate table for each station or substation. Instead, please add up the number of Cyber Assets by device-type at all Low Impact stations or substations and mark an X under the range that includes the number of these Cyber Assets. In addition, many Cyber Assets perform multiple functions. When responding to the survey, only account for each Cyber Asset once, picking the most applicable function performed by the Cyber Asset.*

For Cyber Assets that Meet the Definition of BES Cyber Asset at <u>Medium</u> Impact Transmission Stations or Substations							
Type of Cyber Asset	***Number of Cyber Assets at Each Medium Impact Transmission Station or Substation***						
	0	*1-9*	*10-24*	*25-49*	*50-99*	*100-149*	*> 150*
IED / Relay							
RTU							
Controller (PLC)							
Data Concentrator							
Meter / indicator							
Intelligent							

instrumentation							
Tap Changer							
HMI Workstation							
Network Printer							
Computer Networking							
Communications Processing							
Equipment Diagnostic / Maintenance							
Fault Recorder							
PMU							
PDC							
Historian							
Precision Time Device							
Development & Testing							
Infrastructure Support							
Physical Access Control System							
Locally Mounted Physical Security							
*Other **							

** Please describe the type and function(s) of the Cyber Asset(s):*

_____

_____

For Cyber Assets that do <u>NOT</u> Meet the Definition of BES Cyber Asset at <u>Medium</u> Impact Transmission Stations or Substations							
Type of Cyber Asset	***Number of Cyber Assets at Each Medium Impact Transmission Station or Substation***						
	0	*1-9*	*10-24*	*25-49*	*50-99*	*100-149*	*> 150*
IED / Relay							

RTU							
Controller (PLC)							
Data Concentrator							
Meter / indicator							
Intelligent instrumentation							
Tap Changer							
HMI Workstation							
Network Printer							
Computer Networking							
Communications Processing							
Equipment Diagnostic / Maintenance							
Fault Recorder							
PMU							
PDC							
Historian							
Precision Time Device							
Development & Testing							
Infrastructure Support							
Physical Access Control System							
Locally Mounted Physical Security							
*Other **							

** Please describe the type and function(s) of the Cyber Asset(s):*

_____

_____

(For these tables, the number range of Cyber Assets will change depending on number of Low Impact Transmission Stations or Substations the entity provides.)

For Cyber Assets that Meet the Definition of BES Cyber Asset at Low Impact Transmission Stations or Substations							
Type of Cyber Asset	***Number of Cyber Assets at Low Impact Transmission Stations or Substations***						
	0	*1-9*	*10-24*	*25-49*	*50-99*	*100-149*	*> 150*
IED / Relay							
RTU							
Controller (PLC)							
Data Concentrator							
Meter / indicator							
Intelligent instrumentation							
Tap Changer							
HMI Workstation							
Network Printer							
Computer Networking							
Communications Processing							
Equipment Diagnostic / Maintenance							
Fault Recorder							
PMU							
PDC							
Historian							
Precision Time Device							
Development & Testing							
Infrastructure Support							
Physical Access Control System							
Locally Mounted Physical Security							

*Other **							

** Please describe the type and function(s) of the Cyber Asset(s):*

_____

_____

For Cyber Assets that do <u>NOT</u> Meet the Definition of BES Cyber Asset at <u>Low</u> Impact Transmission Stations or Substations							
Type of Cyber Asset	***Number of Cyber Assets at Low Impact Transmission Stations or Substations***						
	0	*1-9*	*10-24*	*25-49*	*50-99*	*100-149*	*> 150*
IED / Relay							
RTU							
Controller (PLC)							
Data Concentrator							
Meter / indicator							
Intelligent instrumentation							
Tap Changer							
HMI Workstation							
Network Printer							
Computer Networking							
Communications Processing							
Equipment Diagnostic / Maintenance							
Fault Recorder							
PMU							
PDC							
Historian							
Precision Time Device							

Development & Testing							
Infrastructure Support							
Physical Access Control System							
Locally Mounted Physical Security							
*Other **							

** Please describe the type and function(s) of the Cyber Asset(s):*

_____

_____

c. *Please describe the functions performed by the Cyber Assets that do not meet the 15-minute impact threshold, and the rationale for not including them.*

_____

_____

_____

d. *Please also describe, if applicable, why Cyber Assets or functions performed by the Cyber Assets are excluded from the definition of BES Cyber Asset for a reason other than the 15-minute impact threshold.*

_____

_____

III. ***Generation Plants****:*

a. *Please specify the total number of generation plants you own or operate: _____*

i. *Please specify the number of generation plants you own or operate that meet the description of a generation plant in Section 2 (Medium Impact Rating) of Attachment 1 to CIP-002-5.1: _____*

ii. *Please specify the number of generation plants you own or operate that meet the description of a generation plant in Section 3 (Low Impact Rating) of Attachment 1 to CIP-002-5.1: _____*

iii. *If the total number of generation plants you own or operate identified above does not equal the sum of Medium and Low Impact generation plants identified in parts i and ii, please explain why:*

_____

_____

b. *Please complete the tables below for each generation plant you own or operate that contain the specified Cyber Assets in the ranges provided. When completing each table, please indicate whether the generation plant is Medium or Low Impact. In addition, many Cyber Assets perform multiple functions. When responding to the survey, only account for each Cyber Asset once, picking the most applicable function performed by the Cyber Asset.*

For Cyber Assets that Meet the Definition of BES Cyber Asset at Generation Plants ***Type of Generation Plant: _____ (Select Medium or Low)***							
Type of Cyber Asset	***Number of Cyber Assets at Each Generation Plant***						
	0	*1-24*	*25-99*	*100-499*	*500-999*	*1000-2999*	*> 3000*
Controller (PLC)							
Distributed Control System (DCS)							
Sensor / Actuator / Transmitter							
Meter / Indicator							
HMI Workstation							
Application Server							
Network Printer							
Data Server							
Historian							
Computer Networking							
Equipment Diagnostic /							

Maintenance							
Fault Recorder							
IED / Relay							
RTU							
PMU							
PDC							
Precision Time Device							
Development & Testing							
Infrastructure Support							
Physical Access Control System							
Locally Mounted Physical Security							
*Other **							

** Please describe the type and function(s) of the Cyber Asset(s):*

_____

_____

For Cyber Assets that do <u>NOT</u> Meet the Definition of BES Cyber Asset at Generation Plants Type of Generation Plant: _____ (Select Medium or Low)							
Type of Cyber Asset	***Number of Cyber Assets at Each Generation Plant***						
	0	*1-24*	*25-99*	*100-499*	*500-999*	*1000-2999*	*> 3000*
Controller (PLC)							
Distributed Control System (DCS)							
Sensor / Actuator / Transmitter							
Meter / Indicator							

HMI Workstation							
Application Server							
Network Printer							
Data Server							
Historian							
Computer Networking							
Equipment Diagnostic / Maintenance							
Fault Recorder							
IED / Relay							
RTU							
PMU							
PDC							
Precision Time Device							
Development & Testing							
Infrastructure Support							
Physical Access Control System							
Locally Mounted Physical Security							
*Other **							

** Please describe the type and function(s) of the Cyber Asset(s):*

_____

_____

c. *Please describe the functions performed by the Cyber Assets that do not meet the 15-minute impact threshold, and the rationale for not including them.*

_____

_____

d. *Please also describe, if applicable, why Cyber Assets or functions performed by the Cyber Assets are excluded from the definition of BES Cyber Asset for a reason other than the 15-minute impact threshold.*

_____

_____

_____

_____

IV. *Other Locations:*

a. *If you have any other Cyber Assets that control BES Elements outside of Control Centers, transmission stations or substations, and generation plants, please describe their location and function, and explain whether they meet the definition of BES Cyber Asset.*

_____

_____

Part 2 *– Please describe the process you are using or will use to determine if a particular Cyber Asset meets the definition of BES Cyber Asset. Please also describe any challenges you have encountered while creating or executing your process.*

_____

_____

Which systems or network components associated with BES Cyber Systems would not be considered in scope of the CIP standards? Are these systems considered programmable? If not, what are their characteristics?

_____

_____

How would you define programmable electronic device?

_____

_____

Information Required by ROP Section 1602.2

1. **A description of the data or information to be requested, how the data or information will be used, and how the availability of the data or information is necessary for NERC to meet its obligations under applicable laws and agreements.**

    a. *A Description of the Data or Information Requested*

A description of the data or information to be requested is provided above. A link to a document showing the drop-down menus is provided on the web page where this request is posted.

    b. *How the data or information will be used*

NERC will use the data to complete the informational filing that NERC must submit to the Commission by February 3, 2015. As noted above, in Order No. 791, the Commission directed NERC to conduct a survey of responsible entities during the implementation period for the CIP Version 5 Reliability Standards to determine the types of Cyber Assets that are included or excluded from the definition of BES Cyber Asset. NERC is required to submit an informational filing within one year of the effective date of Order No. 791 explaining, based on the survey data, the following: (1) specific ways in which entities determine which Cyber Assets meet the 15-minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition. NERC will also use information learned from the Transition Study for the informational filing.

    c. *How is the availability of the data or information necessary for NERC to meet its obligations under applicable laws and agreements*

As noted above, the proposed Data Request will provide NERC the data and information needed to comply with FERC's directive in Order No. 791 to conduct a survey and submit an informational filing based on that survey.

2. **A description of how the data or information will be collected and validated.**

NERC will identify the Registered Entities required to comply with the CIP Version 5 Reliability Standards and will prepare the survey, provide instruction to the identified registered entities for submitting the data, and collect and sort the data. NERC will compare the list of Registered Entities with the Data Request respondents to ensure that responses are received as requested. NERC staff will further validate the data provided.

3. **A description of the entities that will be required to provide the data or information ("Reporting Entities").**

All U.S. Balancing Authorities, Distribution Providers (as described in Applicability Section 4.1.2 of Reliability Standard CIP-003-5), Generator Operators, Generator Owners, Interchange Coordinators or Interchange Authorities, Reliability Coordinators, Transmission Operators, and Transmission Owners required to comply with the CIP Version 5 Reliability Standards must respond to the proposed Data Request.

4. **The schedule or due date for the data or information.**

NERC proposes to require Reporting Entities to respond to the proposed Data Request within 70 days of its issuance.

NERC expects to present the proposed Data Request for NERC Board of Trustees approval at the meeting of the Board of Trustees on August 13-14, 2014. Upon NERC Board of Trustees approval, the proposed Data Request will be issued and become mandatory.

5. **A description of any restrictions on disseminating the data or information (e.g., "confidential," "critical energy infrastructure information," "aggregating" or "identity masking").**

NERC's treatment of confidential information is governed by Section 1500 of the ROP. Although the proposed Data Request does not require the disclosure of confidential or critical energy infrastructure information, any confidential information obtained will be protected in accordance with Section 1500. Further, none of the individual responses to the proposed Data Requests will be publicly posted or shared. In the informational filing with the Commission, NERC will only present aggregated data.

6. **An estimate of the relative burden imposed on the reporting entities to accommodate the data or information request:**

The proposed Data Request is a one-time request for information with respect to an issue that applicable entities will already be reviewing as part of their transition to compliance with the CIP Version 5 Reliability Standards. The incremental burden for this one-time data collection will be the effort required to complete the survey based on the information learned during their transition activities. For small entities, the burden would expected to be minimal, approximately 40 hours total per entity to complete the Data Request, whereas for larger entities, the estimated time to complete the Data Request is estimated at less than 100 hours total per entity.

Request for Comments

Please provide comments on the substance and scope of the proposed Data Request. Comments are due by 8:00 p.m. EST on July 14, 2014. Comments must be submitted in an electronic document to BESCyberAssetSurvey@nerc.net.

In addition to any overall comments on the proposed Data Request, comments on the following would be appreciated:

1) Please describe any additional equipment types that should be included in the tables in Part 1 of the Data Request.

2) Are the ranges for numbers of Cyber Assets provided in the tables in Part 1 of the Data Requests appropriate to capture useable data from the survey?

ATTACHMENT 1

Explanation and Functional Uses of Asset Types

The following is a description of the Cyber Assets commonly installed and used at Control Centers, transmission stations or substations, or generation plants. The Cyber Assets listed here include BES Cyber Assets, as well as support systems and Electronic Control and monitoring Systems (EACMS) and Physical Access Control Systems (PACS).

Many of the Cyber Assets described below perform multiple functions. When responding to the survey, only account for each Cyber Asset once, picking the most applicable function performed by the Cyber Asset.

1. **Control Center**

- **Application Server**: Traditional computer nodes used for executing Bulk Electric System operations applications such as status monitoring, limit checking, alarm generation, log management, automatic generation control (AGC), economic dispatch, interchange scheduling, unit scheduling, state estimation, contingency analysis, power flow analysis, switching studies, etc.
- **Data Server:** Similar to an application server, but primarily used to provide data to application servers. Data servers include "traditional" servers running database software with locally attached storage, as well as network-attached storage servers (disk servers).
- **HMI (Human Machine Interface) Workstation**: A workstation computer consisting of display and keyboard attached to a small computer. HMI Workstations are used to provide human grid operators with status and values, and allow them to enter parameters to control the process.
- **Network Printer**: A printer that is attached directly to the network, and is therefore shared by multiple users and applications.
- **Data Acquisition Server**: Communications front-end processors used to communicate to other computer sites, control centers, field devices, or generation plants by receiving data from remote sites, process the data into local format, and store it for local use. Some data acquisition servers contain specialized hardware used to communicate to field devices; other data acquisition servers receive data via computer network connections.
- **Data Interchange**: Communications servers (e.g. ICCP servers) used to communicate intersite data between control centers and other facilities that serve a BES function.
- **Phasor Data Concentrator (PDC)**: A device that manages data feeds from multiple Phasor Measurement Units (PMUs).

- **Computer Networking Devices**: Hardware used to provide connectivity between other computers. Examples include hubs, switches, routers, firewalls, intrusion detection/prevention systems, terminal servers, security event and incident management systems, EACMS, etc.
- **Communications Processing Devices**: Devices used to perform protocol conversions, encapsulate serial data into a routable protocol, encrypt communications, etc.
- **Diagnostic Devices**: Devices used to troubleshoot hardware or software; at a control center diagnostic devices are most often attached to the local area network but could be attached to other Cyber Assets. Diagnostic devices can be normal Cyber Assets such as laptop computers or specialized diagnostic equipment.
- **Fault Recorder**: Device used to detect faults and record the electrical behavior of the transmission elements for after-the-fact analysis.
- **Historian**: Generally, a combination of compute server and data server with specialized software used for storing a historical record of Bulk Electric System operations data. Historians also can be used to provide access to data outside of the control center without impacting the control center processing.
- **Situational Awareness**: Systems used to provide situational awareness in a real-time Bulk Electric System operations environment (e.g. video mapboards, tile mapboard controllers, video trending).
- **Precision Time Device:** Device (e.g. Symmetricom TrueTime) used to synchronize the time on electronic equipment with a highly accurate reference such as a GPS master clock.
- **Training Simulator**: Computers (including application servers, database servers, HMI) that are used to train operators on various power system operations scenarios, and to test new operational procedures for validity.
- **Development & Testing**: Computers (including application servers, database servers, HMI) that are used to develop and test new application programs, database updates, and power system model changes prior to their inclusion in the real-time operations environment.
- **Infrastructure Support**: Computers that provide support functions to other Cyber Assets, such as domain name system (DNS), active directory, certificate management, administrative workstations, patch management, etc.
- **Marketing Systems**: Systems supporting marketing functions that may be located inside ESPs containing BES Cyber Systems. Examples include OASIS calculators, market pricing systems, market clearing systems, market billing systems, etc.
- **Physical Access Control System**: A Cyber Asset that controls, alerts, or logs access to the Physical Security Perimeter.

- **Locally Mounted Physical Security Device:** Devices typically located outside the Physical Security Perimeter (PSP) that control access to the PSP, such as motion sensors, electronic lock control mechanisms, badge readers, etc.
- **Other**: Any other computer node not described above. Please specify the application or function.

2. Transmission Station / Substation

- **Intelligent Electronic Device (IED) / Relay**: IED or relay device protection system used to sense fault conditions (e.g., on transmission lines), and take rapid autonomous actions to isolate the fault to prevent cascading fault conditions or equipment damage
- **Remote Terminal Unit (RTU)**: A device or system used to send telemetry data from the substation to the control center, and to receive control commands from the control center.
- **Programmable Logic Controller (PLC)**: Substation automation device used to coordinate actions taken by multiple IEDs, or when processing capabilities beyond the capability of an IED are required.
- **Data Concentrator**: A device or system used to collect data from multiple IEDs and provide a single data interface to the RTU.
- **Meter / Indicator**: A device used to provide local readout of values (e.g., bus voltage) or indication of status (e.g., breaker open/close). Meters / indicators may also collect and transmit values to other Cyber Assets.
- **Intelligent instrumentation**: Primary instrumentation used to sense values (e.g., voltage, current) or status (e.g., breaker or switch position). Primarily used by IEC 61850 enabled substations.
- **Tap Changer**: A device located on a transformer that allows the transformer winding ratio to be controlled remotely.
- **HMI Workstation**: A workstation computer consisting of display and keyboard attached to a small computer. HMI Workstations are used to provide human operators with status and values, and allow them to enter parameters to control the process.
- **Network Printer**: A printer that is attached directly to the network, and is therefore shared by multiple users and applications.
- **Computer Networking Devices**: Hardware used to provide connectivity between other computers. Examples include hubs, switches, routers, firewalls, intrusion detection/prevention systems, terminal servers, EACMS etc.
- **Communications Processing Devices**: Devices used to perform protocol conversions, encapsulate serial data into a routable protocol, encrypt communications, etc.

- **Equipment Diagnostic / Maintenance**: Devices used to monitor the behavior of the substation computers, calibrate the instrumentation, or diagnose problems with the control or networking components.
- **Fault Recorder**: Device used to detect faults and record the electrical behavior of the transmission elements for after-the-fact analysis.
- **Phasor Measurement Unit** (**PMU)**: A device that performs high-speed monitoring and analysis of voltage and current values and waveforms. In some cases, PMU data is used for after-the-fact analysis; in other cases, PMU data is used for real-time autonomous control.
- **Phasor Data Concentrator** (**PDC)**: A device that manages data feeds from multiple PMUs.
- **Historian**: Generally, a combination of compute server and data server with specialized software used for storing a historical record of Bulk Electric System operations data. Historians also can be used to provide access to data outside of the control center without impacting the control center processing.
- **Precision Time Device:** Device (e.g. Symmetricom TrueTime) used to synchronize the time on electronic equipment with a highly accurate reference such as a GPS master clock.
- **Development & Testing**: Computers (including application servers, database servers, HMI) that are used to develop and test new application programs, and database updates prior to their inclusion in the real-time operations environment.
- **Infrastructure Support**: Computers that provide support functions to other Cyber Assets, such as domain name system (DNS), active directory, certificate management, administrative workstations, patch management, etc.
- **Physical Access Control System**: A Cyber Asset that controls, alerts, or logs access to the Physical Security Perimeter.
- **Locally Mounted Physical Security Device:** Devices typically located outside the Physical Security Perimeter (PSP) that control access to the PSP, such as motion sensors, electronic lock control mechanisms, badge readers, etc.
- **Other**: Any other computer node not described above. Please specify the application or function.

3. <u>Generation Plants</u>

- **Controller (PLC)**: First level control system, used to coordinate the actions of a specific set of sensors and actuators. Controllers are programmed to take the input of specific sensors, process their data, and send output control commands to actuators, generally with a feedback loop to assess the impact of the control action, and take additional

control actions if necessary. Individual controllers send status and values to higher level controllers and application servers for supervisory control and display to operators.

- **Distributed Control System (DCS)**: Modules, processors, communications relays, and other sub-components that control the plant and allow operators at HMI interfaces to manipulate the plant.
- **Sensor / Actuator / Transmitter**: Primary input and output elements in a distributed control system. Sensors sense process values (e.g., pressure, temperature); actuators invoke changes in the process (e.g., open and close valves, change the speed of motors), and transmitters provide the local interface between the sensor and actuator to the control system hardware. Modern sensors and actuators contain embedded transmitters, older sensors and actuators require transmitters to translate analog signals to digital signals, or to allow the analog control signals to travel longer distances.
- **Meter / Indicator**: Device used to provide local readout of values (e.g., pressure, temperature) or indication of status (e.g., valve position). Meters / indicators may also collect and transmit values to other Cyber Assets.
- **HMI Workstation**: A workstation computer consisting of display and keyboard attached to a small computer. HMI Workstations are used to provide human operators with status and values, and allow them to enter parameters to control the process.
- **Network Printer**: A printer that is attached directly to the network, and is therefore shared by multiple users and applications.
- **Application Server**: Traditional computer nodes used for executing Bulk Electric System operations applications such as plant optimization, or to coordinate the action of multiple independent control systems.
- **Data Server**: Similar to an application server, but primarily used to provide data to application servers. Data servers include "traditional" servers running database software with locally attached storage, as well as network-attached storage servers (disk servers).
- **Historian**: Generally, a combination of compute server and data server with specialized software used for storing a historical record of Bulk Electric System operations data. Historians also can be used to provide access to data outside of the control center without impacting the control center processing.
- **Computer Networking Devices**: Hardware used to provide connectivity between other computers. Examples include hubs, switches, routers, firewalls, intrusion detection/prevention systems, terminal servers, EACMS, etc.
- **Equipment Diagnostic / Maintenance Devices**: Devices used to monitor the behavior of the generation plant computers, calibrate the instrumentation, or diagnose problems with the control or networking components.
- **Fault Recorder**: Device used to detect faults and record the electrical behavior of the transmission elements for after-the-fact analysis.

- **IED / Relay**: IED or relay device protection system used to sense fault conditions (e.g., on a generator bus), and take rapid autonomous actions to isolate the fault to prevent cascading fault conditions or equipment damage.
- **Remote Terminal Unit (RTU):** A device or system used to send telemetry data from the substation to the control center, and to receive control commands from the control center.
- **Phasor Measurement Unit (PMU)**: A device that performs high-speed monitoring and analysis of voltage and current values and waveforms. In some cases, PMU data is used for after-the-fact analysis; in other cases, PMU data is used for real-time autonomous control.
- **Phasor Data Concentrator (PDC):** A device that manages data feeds from multiple PMUs.
- **Precision Time Device:** Device (e.g. Symmetricom TrueTime) used to synchronize the time on electronic equipment with a highly accurate reference such as a GPS master clock.
- **Development & Testing**: Computers (including application servers, database servers, HMI) that are used to develop and test new application programs, and database updates prior to their inclusion in the real-time operations environment.
- **Infrastructure Support**: Computers that provide support functions to other Cyber Assets, such as domain name system (DNS), active directory, certificate management, administrative workstations, patch management, etc.
- **Physical Access Control System**: A Cyber Asset that controls, alerts, or logs access to the Physical Security Perimeter.
- **Locally Mounted Physical Security Device:** Devices typically located outside the Physical Security Perimeter (PSP) that control access to the PSP, such as motion sensors, electronic lock control mechanisms, badge readers, etc.
- **Other**: Any other computer node not described above. Please specify the application or function.

ATTACHMENT 2

Example of Completed Table for Part 1 of the Data Request

The following provides an example of how to complete the tables under Part 1 of the data request. This example addresses Control Centers for illustration purposes.

Assume an entity, which owns and operates both transmission Facilities and generation plants, has the following three Control Centers:

1) a primary Control Center used to perform the functions of a Transmission Operator that meets the description in Section 1.3 of Attachment 1 to CIP-002-5.1;

2) a backup Control Center used to perform the functions of a Transmission Operator that meets the description in Section 1.3 of Attachment 1 to CIP-002-5.1; and

3) a Control Center used to perform the functions of the Generator Operator that meets the description in Section 2.11 of Attachment 1 to CIP-002-5.1.

The Control Centers have the following equipment:

Primary Transmission Control Center

6 HMI workstations (production)
2 database servers (production)
4 front-end processors for telemetry and control (production)
2 data exchange processors for exchanging ICCP information (production)
2 AGC application servers (production)
2 real-time contingency analysis application servers (production)
2 study contingency analysis application servers (production)
1 historian (production)
1 long-term forecasting application server (production)
1 mapboard controller (production)
10 video trending displays (production)
2 network switches (production)
2 network printer (production)
2 HMI workstation (development / testing)
1 database server (development / testing)
1 application server (development / testing)
1 historian (development / testing)
1 network switch (development / testing)
1 network printer (development / testing)

Backup Transmission Control Center:

4 HMI workstations (production)

1 database servers (production)
2 front-end processors for telemetry and control (production)
1 data exchange processors for exchanging ICCP information (production)
1 AGC application servers (production)
1 real-time contingency analysis application servers (production)
1 study contingency analysis application servers (production)
6 video trending displays (production)
1 network switches (production)
1 network printer (production)

Generation Control Center
4 HMI workstations (production)
2 database servers (production)
2 data exchange processors for exchanging ICCP information (production)
2 application servers (production)
1 historian (production)
2 network switches (production)
2 network printer (production)

The entity would complete Part 1.1 of the Data Request as follows:

Part 1: Please provide the information requested below with respect to the Cyber Assets contained in your Control Centers, transmission stations or substations, and generation plants, as applicable.

I. Control Centers:

For purposes of identifying Control Centers under this survey, if you have separate locations that contain the operating elements (i.e., control room where System Operators interact with HMI devices) and data centers (i.e., "computer rooms" containing servers, data communications and data storage), please count each location separately in the count of Control Center locations. Alternatively, if you have a one-to-one relationship between the operating and data centers, and they are co-located in the same building or location, only count those as a single location.

a. *Please specify the total number of Control Centers you own or operate:* 3

i. *Please specify the number of Control Centers you own or operate that meet the description of a Control Center in Section 1 (High Impact Rating) of Attachment 1 to CIP-002-5.1:* 2

ii. *Please specify the number of Control Centers you own or operate that meet the description of a Control Center in Section 2 (Medium Impact Rating) of Attachment 1 to CIP-002-5.1:* 1

iii. *Please specify the number of Control Centers you own or operate that meet the description of a Control Center in Section 3 (Low Impact Rating) of Attachment 1 to CIP-002-5.1:* 0

b. *Please complete the tables below for each Control Center you own or operate that contain the specified Cyber Assets in the ranges provided. (For example, if you have two Control Centers, one of which has three application servers and meets the description in Section 2.12 of Attachment 1 to CIP-002-5.1 (Medium Impact) and the other with 11 application servers that meets the description in Section 1.3 of Attachment 1 (High Impact), you would complete the two separate tables, one for the Medium Impact Control Center and one for the High Impact Control Center. For the Medium Impact Control Center table you would enter X in the row for application servers under the 1-4 column and indicate it is a Medium Impact Control Center, and in a separate table, mark an X under the 10-19 column and indicate it is a High Impact Control Center.) In addition, many of the Cyber Assets performing the functions described below perform multiple functions. When responding to the survey, only account for each Cyber Asset once, picking the most applicable function performed by the Cyber Asset.*

(For the Transmission Control Center, entity would complete the table as follows.)

For Cyber Assets that Meet the Definition of BES Cyber Asset at Control Centers ***Type of Control Center: __High____ (Select High, Medium, or Low)***							
Type of Cyber Asset	***Number of Cyber Assets at Each Control Center***						
	0	*1-4*	*5-9*	*10-19*	*20-39*	*40-59*	*> 60*
Application Servers		*X*					
Data Servers		*X*					
HMI Workstations			*X*				
Network Printer		*X*					
Data Acquisition		*X*					
Data interchange		*X*					
PDC	*X*						
Computer Networking		*X*					
Communications Processing	*X*						
Diagnostic	*X*						
Fault Recorder	*X*						
Historian		*X*					
Situational Awareness				*X*			
Precision Time Device	*X*						
Training Simulator	*X*						
Development & Testing	*X*						
Infrastructure Support	*X*						
Marketing Systems	*X*						
Physical Access Control System	*X*						
Locally Mounted Physical Security	*X*						
*Other **	*X*						

** Please describe the type and function(s) of the Cyber Asset(s):*

N/A

(For the Backup Transmission Control Center, entity would complete the table as follows.)

For Cyber Assets that Meet the Definition of BES Cyber Asset at Control Centers ***Type of Control Center: __High____ (Select High, Medium, or Low)***							
Type of Cyber Asset	***Number of Cyber Assets at Each Control Center***						
	0	*1-4*	*5-9*	*10-19*	*20-39*	*40-59*	*> 60*
Application Servers		*X*					
Data Servers		*X*					
HMI Workstations		*X*					
Network Printer		*X*					
Data Acquisition		*X*					
Data interchange		*X*					
PDC	*X*						
Computer Networking		*X*					
Communications Processing	*X*						
Diagnostic	*X*						
Fault Recorder	*X*						
Historian		*X*					
Situational Awareness			*X*				
Precision Time Device	*X*						
Training Simulator	*X*						
Development & Testing	*X*						
Infrastructure Support	*X*						
Marketing Systems	*X*						
Physical Access Control System	*X*						
Locally Mounted Physical Security	*X*						
*Other **	*X*						

** Please describe the type and function(s) of the Cyber Asset(s):*

N/A

(For the Generation Control Center, entity would complete the table as follows.)

For Cyber Assets that Meet the Definition of BES Cyber Asset at Control Centers ***Type of Control Center: __Medium____ (Select High, Medium, or Low)***							
Type of Cyber Asset	***Number of Cyber Assets at Each Control Center***						
	0	*1-4*	*5-9*	*10-19*	*20-39*	*40-59*	*> 60*
Application Servers		*X*					
Data Servers		*X*					
HMI Workstations		*X*					
Network Printer		*X*					
Data Acquisition	*X*						
Data interchange		*X*					
PDC	*X*						
Computer Networking		*X*					
Communications Processing	*X*						
Diagnostic	*X*						
Fault Recorder	*X*						
Historian		*X*					
Situational Awareness	*X*						
Precision Time Device	*X*						
Training Simulator	*X*						
Development & Testing	*X*						
Infrastructure Support	*X*						
Marketing Systems	*X*						
Physical Access Control	*X*						

System							
Locally Mounted Physical Security	*X*						
*Other **	*X*						

** Please describe the type and function(s) of the Cyber Asset(s):*

N/A

(Entity would not complete tables for Cyber Assets not meeting definition of BES Cyber Asset because it did not have any out of scope in this example.)

c. *Please describe the functions performed by the Cyber Assets that do not meet the 15-minute impact threshold, and the rationale for not including them.*

1. Study application server – used to analyze potential line switching issues.
2. Long term forecasting server – used to forecast next-season and next-year load patterns.
3. Historian – used for archival and remote display of data to non-operational personnel.
4. Mapboard controller – used to drive mapboard; HMI one-line diagrams used as primary operational tool.

d. *Please describe why Cyber Assets or functions performed by the Cyber Assets are excluded from the definition of BES Cyber Asset for a reason other than the 15-minute impact threshold.*

N/A

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC authorized moving the SAR forward to standard development to implement recommendations of Five-year review of NUC-001-2 - October 17, 2013.
2. SAR posted for informal comment February 12-March 13, 2014.
3. NUC-001-3 for 45 day Comment Period and I~~i~~nitial B~~b~~allot April 8 – May 22, 2014.

Description of Current Draft

~~(Describe~~Draft 1 of NUC-001-3 implements recommendations from the NUC-001-2.1 ~~type of action associated with this posting such as 30-day informal comment period, 30~~F~~f~~ive-Y~~y~~ear R~~r~~eview Team (NUC FYRT)~~of NUC-001-2~~. The FYRT's ~~These~~ recommendations ~~of the FYR team~~ were~~as~~ accepted by the Standards Committee in October 2013. This draft is being posted for a 45-day formal comment period~~, 45 day formal comment period with parallel~~ and initial ballot~~, 30-day formal comment period with parallel successive ballot, recirculation ballot).~~

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	April 8, 2014
Recirculation ballot	June 2014
BOT adoption	August 2014

~~Effective Dates:~~ ~~April 1, 2010~~**Effective Dates:** First day of the first calendar quarter that is twelve months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is twelve~~six~~ months after the date this standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2007	Approved by Board of Trustees	New
2	To be determined	Modifications for Order 716 to Requirement R9.3.5 and footnote 1; modifications to bring compliance elements into conformance with the latest version of the ERO Rules of Procedure.	Revision
2	August 5, 2009	Adopted by Board of Trustees	Revised
2	January 22, 2010	Approved by FERC on January 21, 2010 Added Effective Date	Update
2	February 7, 2013	R9.1, R9.1.1, R9.1.2, R9.1.3, and R9.1.4 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	
2.1	April 11, 2012	Errata approved by the Standards Committee; (Capitalized “Protection System” in accordance with Implementation Plan for Project 2007-17 approval of revised definition of “Protection System”)	Errata associated with Project 2007-17
3	March, 2014	Modifications to implement the recommendations of the five-year review of NUC-001, which was accepted by the Standards Committee on October 17, 2013.	Revision

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

~~**Term:** definition.~~

None

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** **Nuclear Plant Interface Coordination**

2. **Number:** **NUC-001-~~2.1~~3**

3. **Purpose:** This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Nuclear Plant Generator Operator~~s~~.

   4.2. Transmission Entities shall mean all entities that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs). Such entities may include one or more of the following:

   4.2.1 Transmission Operators.

   4.2.2 Transmission Owners.

   4.2.3 Transmission Planners.

   4.2.4 Transmission Service Providers.

   4.2.5 Balancing Authorities.

   4.2.6 Reliability Coordinators.

   4.2.7 Planning Coordinators.

   4.2.8 Distribution Providers.

   4.2.9 Load-serving Entities.

   4.2.10 Generator Owners.

   4.2.11 Generator Operators.

5. Background:

Project 2012-13 Nuclear Power Interface Coordination seeks to implement the changes that were proposed by the NUC FYRT~~-001-2.1 Five Year Review Team~~. ~~-~~The NUC ~~Five Year Review Team (~~FYRT~~)~~ was appointed by the Standards Committee Executive Committee on April 22, 2013. The NUC FYRT reviewed the NUC-001-2.1 standard to identify opportunities for consolidation and additional improvements. The NUC FYRT posted its recommendation to revise NUC-001-2.1 for industry comment on July 27, 2013~~for industry comment its recommendation to revise NUC-001-2.1 on July 27, 2013.~~. The NUC FYRT considered comments and submitted its final recommendation to revise NUC-001-2.1, along with a Standards Authorization Request (SAR) to the Standards Committee on October 17, 2013 ~~its final recommendation to revise NUC-001-2.1, along with a Standards Authorization Request (SAR) on October 17, 2013~~. The Standards Committee accepted the recommendation of the FYRT and appointed the team as the Standard Drafting Team (SDT) to implement the recommendation.

B. Requirements and Measures

R1. The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt. *[Violation Risk Factor: ~~Lower~~Medium] [Time Horizon: -Long-term Planning]*

M1. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide a copy of the transmittal and receipt of transmittal of the proposed NPIRs to the responsible Transmission Entities.

R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements[1] that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. *[Violation Risk Factor: Medium] [Time Horizon: ~~]~~ Long-term Planning]*

M2. The Nuclear Plant Generator Operator and each Transmission Entity shall each have a copy of the Agreement(s) addressing and implementing the ~~elements in Requirement 9~~NPIRs available for inspection upon request of the Compliance Enforcement Authority.

R3. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator.: *[Violation Risk Factor: Medium] [Time Horizon: ~~]~~ Long-term Planning]*

[1]. Agreements may include mutually agreed upon procedures or protocols in effect between entities or between departments of a vertically integrated system.

M3. Each Transmission Entity responsible for planning analyses in accordance with the Agreement shall, upon request of the Compliance Enforcement Authority, provide a copy of the planning analyses results transmitted to the Nuclear Plant Generator Operator, showing incorporation of the NPIRs. The Compliance Enforcement Authority shall refer to the Agreements developed in accordance with this standard for specific requirements.

R4. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall *[Violation Risk Factor: High] [Time Horizon: Operations Planning and Real-time Operations]*

4.1. Incorporate the NPIRs into their operating analyses of the electric system.

4.2. Operate the electric system to meet the NPIRs.

4.3. Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.

M4. Each Transmission Entity responsible for operating the electric system in accordance with the Agreement shall demonstrate or provide evidence of the following, upon request of the Compliance Enforcement Authority:

M4.1 The NPIRs have been incorporated into the current operating analysis of the electric system. (Requirement 4.1)

M4.2 The electric system was operated to meet the NPIRs. (Requirement 4.2)

M4.3 The Transmission Entity informed the Nuclear Plant Generator Operator when it became aware it lost the capability to assess the operation of the electric system affecting the NPIRs

R5. ~~The Nuclear Plant Generator Operator shall operate per~~Per the Agreements developed in accordance with this standard~~.~~, the Nuclear Plant Generator Operator shall operate the nuclear plant to meet the NPIRs. *[Violation Risk Factor: High] [Time Horizon: ~~]~~Operations Planning]*

Rationale for R5: Rationale for R5: The FYRT recommended R5 be revised for consistency with R4 and to clarify that nuclear plants must be operated to meet the Nuclear Plant Interface Requirements.

M5. The Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, demonstrate or provide evidence that the Nuclear Power Plant is being operated consistent with the NPIRs~~. as per the Agreements developed in accordance with this standard.~~

R6. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M6. The Transmission Entities and Nuclear Plant Generator Operator shall, upon request of the Compliance Enforcement Authority, provide evidence of the coordination between the Transmission Entities and the Nuclear Plant Generator Operator regarding outages and maintenance activities which affect the NPIRs.

R7. Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design~~,~~ (e.g., protective relay setpoints), configuration, operations, limits, ~~Protection Systems,~~ or capabilities that may impact the ability of the electric system to meet the NPIRs. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

M7. The Nuclear Plant Generator Operator shall provide evidence that it informed the applicable Transmission Entities of changes to nuclear plant design~~,~~ (e.g., protective relay setpoints), configuration, operations, limits~~, Protection Systems~~, or capabilities that would impact the ability of the Transmission Entities to meet the NPIRs.

Rationale for R7 and R8: The FYRT recommended deleting “Protection Systems” in Requirements R7 and R8 since it is a subset of the "nuclear plant design" and "electric system design" elements currently contained in R7 and R8 respectively; and adding a parenthetical clause (e.g. protective setpoints) to R7 following "nuclear plant design" and parenthetical clause (e.g. relay setpoints) to R8 following "electric system design."

R8. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design~~,~~ (e.g., protective relay setpoints), configuration, operations, limits, ~~Protection Systems~~, or capabilities that may impact the ability of the electric system to meet the NPIRs. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

M8. The Transmission Entities shall each provide evidence that it informed the Nuclear Plant Generator Operator of changes to electric system design~~,~~ (e.g., protective relay setpoints), configuration, operations, limits~~, Protection Systems~~, or capabilities that would impact the ability of the Nuclear Plant Generator Operator to meet the NPIRs.

R9. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include~~, as a minimum,~~ the following elements in aggregate within the ~~a~~Agreement(s) identified in R2.

- Where multiple Agreements with a single Transmission Entity are put into effect, the R9 elements must be addressed in aggregate within the Agreements; however, each Agreement does not have to contain each element. The Nuclear Plant Generator Operator and the Transmission Entity are responsible for ensuring all the R9 elements are addressed in aggregate within the Agreements.
- Where Agreements with multiple Transmission Entities are required, the Nuclear Plant Generator Operator is responsible for ensuring all the R9 elements are addressed in aggregate within the Agreements with the Transmission Entities. The Agreements with each Transmission Entity do not have to contain each element; however, the Agreements with the multiple Transmission Entities, in the aggregate, must address all R9 elements. For each Agreement(s), the Nuclear Plant Generator Operator and the Transmission Entity are responsible to ensure the Agreement(s) contain(s) the elements of R9 applicable to that Transmission Entity. : *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

Rationale for R9: The FYRT recommended that R9 be revised to clarify that all agreements do not have to discuss each of the elements in R9, but that the sum total of the agreements need to address the elements.
In addition, for clarity in Part 9.4.1, the FYRT recommended that "affecting the NPIRs" be inserted following "Provisions for communications" and "applicable unique" be inserted following ""definitions of."

~~8.1.~~ Retired~~Administrative elements:~~

~~8.1.1.~~ ~~Definitions of key terms used in the agreement.~~

~~8.1.2.~~ ~~Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs.~~

~~8.2.~~9.1. ~~A requirement to review the agreement(s) at least every three years. A dispute resolution mechanism.~~. *[Note: Part 9.1 was retired under the Paragraph 81 project~~.~~. The NUC SDT proposes to leave this Part blank to avoid renumbering Requirement parts that would impact existing agreements throughout the industry.]*

~~8.3.~~9.2. Technical requirements and analysis:

~~8.3.1.~~9.2.1. Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the Agreement.

~~8.3.2.~~9.2.2. Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.

~~8.3.3.~~9.2.3. Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.

~~8.4.~~9.3. Operations and maintenance coordination

8.4.1.9.3.1. Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.

8.4.2.9.3.2. Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.

8.4.3.9.3.3. Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.

8.4.4.9.3.4. Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.

8.4.5.9.3.5. Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power.

8.4.6.9.3.6. Coordination of physical and cyber security protection ~~of the Bulk Electric System~~ at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.

8.4.7. Coordination of the NPIRs with transmission system Special Protection Systems and any programs that reduce or shed load based on underfrequency ~~and~~or undervoltage ~~load shedding programs~~.

9.3.7.

8.5.9.4. Communications and training Administrative elements:

8.5.1.9.4.1. Provisions for communications affecting the NPIRs between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of applicable unique terms.

8.5.2.9.4.2. Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.

8.5.3.9.4.3. Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.

8.5.4.9.4.4. Provisions for supplying information necessary to report to government agencies, as related to NPIRs.

8.5.5.9.4.5. Provisions for personnel training, as related to NPIRs.

M9. The Nuclear Plant Generator Operator ~~and each Transmission Entity~~ shall ~~each~~ have a copy of the Agreement(s) addressing the elements in Requirement 9 available for inspection upon request of the Compliance Enforcement Authority. Each Transmission Entity shall have a copy of the Agreement(s) addressing the elements in Requirement 9 for which it is responsible available for inspection upon request of the Compliance Enforcement Authority.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity

1.2. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.3. Data Retention

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

- For Measure 1, the Nuclear Plant Generator Operator shall keep its latest transmittals and receipts.
- For Measure 2, the Nuclear Plant Generator Operator and each Transmission Entity shall have its current, in-force ~~a~~Agreement.
- For Measure 3, the Transmission Entity shall have the latest planning analysis results.
- For Measures 4.3, 6 and 8, the Transmission Entity shall keep evidence for two years plus current.
- For Measures 5, 6 and 7, the Nuclear Plant Generator Operator shall keep evidence for two years plus current.

If a Responsible Entity is found non-compliant it shall keep information related to the noncompliance until found compliant.

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

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1		~~Lower~~**Medium**	The Nuclear Plant Generator Operator provided the NPIR's to the applicable entities but did not verify receipt.	The Nuclear Plant Generator Operator did not provide the proposed NPIR to one of the applicable entities~~.~~ unless there was only one entity.	The Nuclear Plant Generator Operator did not provide the proposed NPIR's to two of the applicable entities~~.~~ unless there was only two entities.	The Nuclear Plant Generator Operator did not provide the proposed NPIR's to more than two of applicable entities. OR For a particular Nuclear Power Plant, if the number of possible applicable transmission entities is equal to the number of applicable transmission entities not provided NPIRs
R2		**Medium**	N/A	N/A	N/A	The Nuclear Plant Generator Operator or the applicable Transmission Entity does not have in effect one or more agreements that include mutually agreed to NPIRs and document the implementation of the NPIRs.
R3		**Medium**	N/A	The responsible entity incorporated the NPIRs into its planning analyses but did not communicate	N/A	The responsible entity did not incorporate the NPIRs into its planning analyses of the electric system.

				the results to the Nuclear Plant Generator Operator.		
R4		**High**	N/A	The responsible entity did not comply with sub-requirement R4.3.	The responsible entity did not comply with R4.1.	The responsible entity did not comply with R4.2.
~~**R4.1**~~		~~**N/A**~~	~~N/A~~	~~The responsible entity did not comply with sub-requirement R4.3.~~	~~The responsible entity did not comply with R4.1.~~	~~The responsible entity did not comply with R4.2.~~
~~**R4.2**~~		~~**N/A**~~	~~N/A~~	~~The responsible entity did not comply with sub-requirement R4.3.~~	~~The responsible entity did not comply with R4.1.~~	~~The responsible entity did not comply with R4.2.~~
~~**R4.3**~~		~~**N/A**~~	~~N/A~~	~~The responsible entity did not comply with sub-requirement R4.3.~~	~~The responsible entity did not comply with R4.1.~~	~~The responsible entity did not comply with R4.2.~~
R5		**High**	N/A	N/A	N/A	The Nuclear Plant Generator Operator failed to operate per the NPIRs~~Agreements~~ developed in accordance with this standard.
R6		**Medium**	~~The Nuclear Operator or Transmission Entity failed to coordinate outages or maintenance activities in accordance with one or more of the administrative elements within the agreements.~~N/A	The Nuclear Plant Generator Operator or Transmission Entity failed to provide outage or maintenance schedules to the appropriate parties as described in the agreement or on a time period consistent with the agreements.	The Nuclear Plant Generator Operator or Transmission Entity failed to coordinate one or more outages or maintenance activities in accordance the requirements of the agreements.	N/A
R7		**High**	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of proposed	~~The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of actual changes to nuclear~~	The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of actual changes to nuclear	~~N/A~~The Nuclear Plant Generator Operator did not inform the applicable Transmission Entities of actual changes to nuclear

			changes to nuclear plant design~~,~~ (e.g. protective relay setpoints), configuration, operations, limits, ~~protection systems,~~ or capabilities that may impact the ability of the electric system to meet the NPIRs.	~~plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.~~N/A	plant design~~,~~ (e.g. protective relay setpoints), configuration, operations, limits, ~~protection systems,~~ or capabilities that ~~directly~~may impact the ability of the electric system to meet the NPIRs.	plant design (e.g., protective relay setpoints), configuration, operations, limits or capabilities that directly impact the ability of the electric system to meet the NPIRs.
R8		**High**	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of proposed changes to transmission system design, configuration~~,~~ (e.g. protective relay setpoints), operations, limits, ~~protection systems,~~ or capabilities that may impact the ability of the electric system to meet the NPIRs.	~~The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of actual changes to transmission system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.~~N/A	The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of actual changes to transmission system design~~,~~ (e.g. protective relay setpoints), configuration, operations, limits, ~~protection systems,~~ or capabilities that ~~directly impacts~~may impact the ability of the electric system to meet the NPIRs.	~~N/A~~The applicable Transmission Entities did not inform the Nuclear Plant Generator Operator of actual changes to transmission system design (e.g. protective relay setpoints), configuration, operations, limits, or capabilities that directly impacts the ability of the electric system to meet the NPIRs.
R9		**Medium**	~~The agreement identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entities is missing one or more sub-components of R9.1.~~	The ~~agreement~~Agreement(s) identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entity~~ies is missing from one~~ failed to ~~five~~include up to 20% of the combined sub-components in ~~R9~~Parts 9.2, ~~R9~~9.3 and ~~R9~~9.4 applicable to that entity.	The ~~agreement~~Agreement(s) identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entity~~ies is missing from six~~ failed to ~~ten~~include greater than 20%, but less than 40% of the combined sub-components in ~~R9~~Parts	The ~~agreement~~Agreement(s) identified in R2. between the Nuclear Plant Generator Operator and the applicable Transmission Entity~~ies is missing eleven~~failed to include 40% or more of the combined sub-components in ~~R9~~Parts 9.2, ~~R9~~9.3 and ~~R9~~9.4 applicable to the entity.

					9.2, R99.3 and R99.4 applicable to the entity.	

D. Regional Variances

The design basis for Canadian (CANDU) Nuclear Power Plants (NPPs) does not result in the same licensing requirements as U.S. NPPs. Nuclear Regulatory Commission (NRC) design criteria specifies that in addition to emergency on-site electrical power, electrical power from the electric network also be provided to permit safe shutdown. ~~This requirement is specified in such NRC Regulations as 10 CFR 50 Appendix A — General Design Criterion 17 and 10 CFR 50.63 Loss of all alternating current power.~~ There are no equivalent Canadian Regulatory requirements for ~~Station Blackout (SBO) or coping times as they do not form part of~~electrical power from the ~~licensing basis for CANDU NPPs.~~electric network to be provided to permit safe shutdown. Therefore the definition of Nuclear Plant Licensing Requirements (NPLR) for Canadian CANDU ~~units~~ NPPs will be as follows:

Canadian Nuclear Plant Licensing Requirements (CNPLR) are requirements included in the design basis of the nuclear plant and are statutorily mandated for the operation of the plant; when used in this standard, NPLR shall mean nuclear power plant licensing requirements for avoiding preventable challenges to nuclear safety as a result of an electric system disturbance, transient, or condition.

E. Interpretations

None.

F. Associated Documents

None.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Benchmark Geomagnetic Disturbance Event Description

Project 2013-03 GMD Mitigation
Standard Drafting Team
Draft: ~~April 21~~June 10, 2014

RELIABILITY | ACCOUNTABILITY

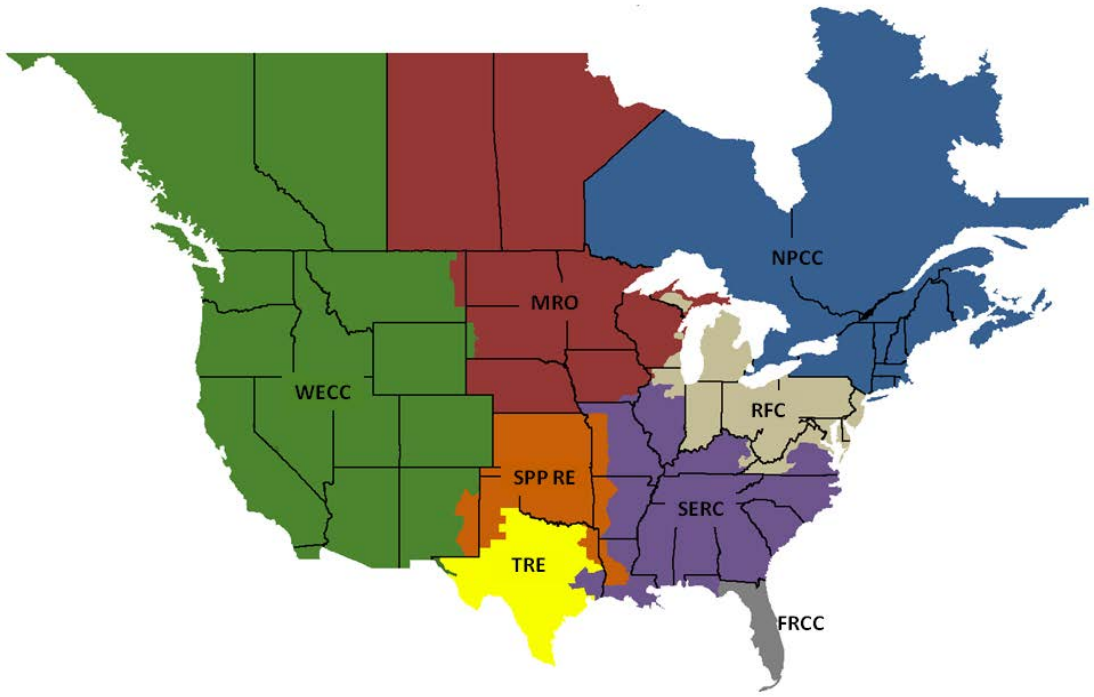
Table of Contents

Preface 3
Introduction 4
Background 4
General Characteristics 4
Benchmark GMD Event Description 6
Reference Geoelectric Field Amplitude 6
Reference Geomagnetic Field Waveshape 6
Appendix I – Technical Considerations 11
Statistical Considerations 11
Impact of Local Geomagnetic Disturbances on GIC 18
Impact of Waveshape on Transformer Hot-spot Heating 18
Appendix II – Scaling the Benchmark GMD Event 21
Scaling the Geomagnetic Field 21
Scaling the Geoelectric Field 22
Example Calculations 27
Example 1 27
Example 2 28
References 29

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the Bulk-Power System (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into several assessment areas within the eight Regional Entity (RE) boundaries, as shown in the map and corresponding table below.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RFC	Reliability*First* Corporation
SERC	SERC Reliability Corporation
SPP-RE	Southwest Power Pool Regional Entity
TRE	Texas Reliability Entity
WECC	Western Electric Coordinating Council

Introduction

Background

The purpose of the benchmark geomagnetic disturbance (GMD) event description is to provide ~~uniform evaluation criteria~~a defined event for assessing system performance during a low probability ~~GMD event. It is to be used in conjunction with Reliability Standards that establish requirements for system modeling, vulnerability assessment, and mitigation planning.~~, high magnitude GMD event as required by proposed standard TPL-007-1 – Transmission System Planned Performance ~~during~~for Geomagnetic Disturbance Events~~s~~. The benchmark GMD event defines the geoelectric field values used to compute geomagnetically-induced current (GIC) flows for a GMD Vulnerability Assessment.

On May 16, 2013, FERC issued Order No. 779, directing NERC to develop Standards that address risks to reliability caused by geomagnetic disturbances in two stages:

- Stage 1 Standard(s) that require applicable entities to develop and implement Operating Procedures. ~~The Stage 1 Standard,~~ EOP-010-1 – Geomagnetic Disturbance Operations is pending at FERC in Docket No. RM14-1-000.
- Stage 2 Standard(s) that require applicable entities to conduct assessments of the potential impact of benchmark GMD events on their systems. If the assessments identify potential impacts, the Standard(s) will require the applicable entity to develop and implement a plan to mitigate the risk.

TPL-007-1 is a new Reliability Standard developed to specifically address the Stage 2 directives in Order No. 779. The benchmark GMD event will define the scope of the Stage 2 Reliability Standard.

General Characteristics

The benchmark GMD event described herein takes into consideration the known characteristics of a severe GMD event and its impact on an interconnected transmission system. These characteristics include:

- Geomagnetic Latitude – The amplitude of the induced geoelectric field for a given GMD event is reduced as the observation point moves away from the earth's magnetic poles.
- Earth Conductivity – The amplitude and phase of the geoelectric field depends on the local or regional earth ground resistivity structure. Higher geoelectric field amplitudes are induced in areas of high resistivity.
- Transformer Electrical Response – Transformers can experience half-cycle saturation when subjected to GIC. Transformers under half-cycle saturation absorb increas~~ing~~ed amounts of reactive power (var) and inject harmonics into the system. However, half-cycle saturation does not occur instantaneously and depends on the electrical characteristics of the transformer and GIC amplitude [1]. Thus, the effects of transformer reactive power absorption and harmonic generation do not occur instantaneously ~~and~~, but instead may take up to several seconds. ~~From a practical point of view, assuming~~It is conservative, therefore, to assume that the effects of GIC on transformer var absorption and harmonic generation are instantaneous ~~is conservative~~.
- Transformer Thermal Effects (e.g. hot spot transformer heating) – Heating of the winding and other structural parts can occur in power transformers during a GMD event. However, the thermal impacts are not instantaneous and are dependent on the thermal time constants of the transformer. Thermal time constants for hot spot heating in power transformers are in the 5-20 minute range.
- Geoelectric Field Waveshape – The geoelectric field waveshape has a strong influence on the hot spot heating of transformer windings and structural parts since thermal time constants of the transformer and time to peak of storm maxima are both on the order of minutes. The frequency content of the magnetic field (dB/dt) is a function of the waveshape, which in turn has a direct effect on the geoelectric field since the earth response to external dB/dt is frequency-dependent.
- Wide Area Geomagnetic Phenomena – The influence of GMD events is typically over a very broad area (e.g. continental scale); however, there can be pockets or very localized regions of enhanced geomagnetic

activity. Since geomagnetic disturbance impacts within areas of influence of approximately 100-200 km do not have a widespread impact on the interconnected transmission system (see Appendix I), statistical methods used to assess the frequency of occurrence of a severe GMD event need to consider broad geographical regions ~~in order~~ to avoid bias caused by spatially localized geomagnetic phenomena.

Benchmark GMD Event Description

Severe geomagnetic disturbance events are high-impact, low-frequency (HILF) events [2]; thus, any benchmark event should consider the probability ~~of occurrence of~~that the event ~~and~~will occur, as well as the impact or consequences of ~~the~~such an event. The benchmark event is composed of the following elements: ~~(~~1) a reference peak geoelectric field amplitude (V/km) derived from statistical analysis of historical magnetometer data; ~~(~~2) scaling factors to account for local geomagnetic latitude; ~~(~~3) scaling factors to account for local earth conductivity; and ~~(~~4) a reference geomagnetic field time series or waveshape to facilitate time-domain analysis of GMD impact on equipment.

Reference Geoelectric Field Amplitude

The reference geoelectric field amplitude was determined through statistical analysis using the plane wave method [3]-[10] geomagnetic field measurements from geomagnetic observatories in northern Europe [11] and the reference (Quebec) earth model shown in **Table 1** [12]. For details of the statistical considerations, see Appendix I. The Quebec earth model is generally resistive and the geological structure is relatively well understood.

Table 1: Reference earth model (Quebec)

Thickness (km)	Resistivity (Ω-m)
15	20,000
10	200
125	1,000
200	100
∞	3

The statistical analysis (see Appendix II) resulted in a conservative peak geoelectric field amplitude of approximately 8 V/km. For steady-state GIC and load flow analysis, the direction of the geoelectric field is assumed to be variable meaning that it can be in any direction (Eastward, Northward, or a vectorial combination thereof).

The frequency of occurrence of this benchmark GMD event is estimated to be approximately 1 in 100 years (see Appendix I). The selected frequency of occurrence is consistent with utility practices where a design basis frequency of 1 in 50 years is currently used as the storm return period for determining wind and ice loading of transmission infrastructure [13], for example.

The regional geoelectric field peak amplitude, E_{peak}, to be used in calculating GIC in the GIC system model can be obtained from the reference value of 8 V/km using the following relationship

$$E_{peak} = 8 \times \alpha \times \beta \text{ (V/km)} \quad (1)$$

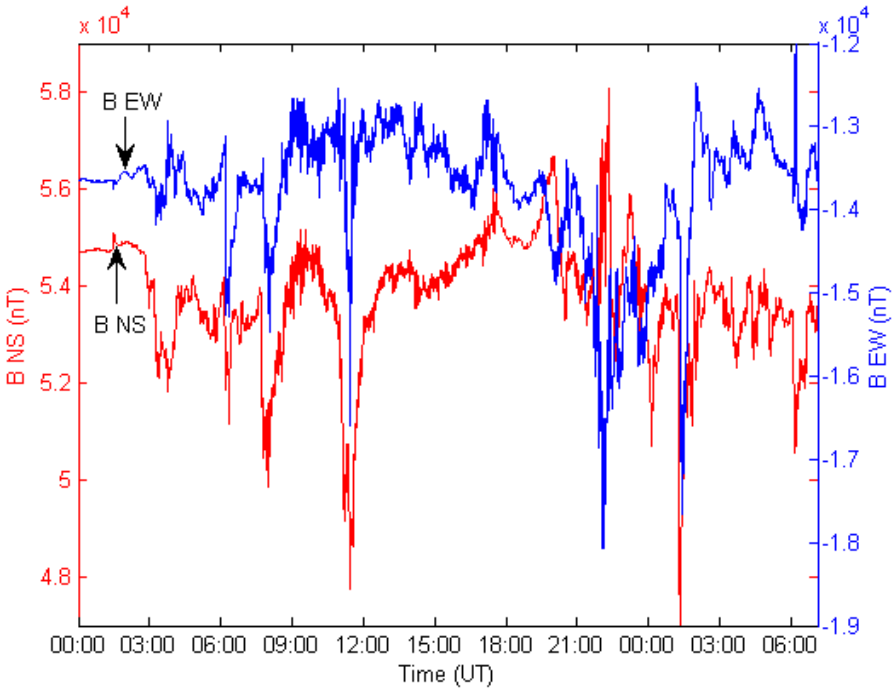
where α is the scaling factor to account for local geomagnetic latitude, and β is a scaling factor to account for the local earth conductivity structure (see Appendix II).

Reference Geomagnetic Field Waveshape

The reference geomagnetic field waveshape was selected after analyzing a number of recorded GMD events, including the reference storm of the NERC interim report of 2012 [14], measurements at the Nurmijarvi (NUR) and Memanbetsu (MMB) geomagnetic observatories for the "Halloween event" of October 29-31, 2003, and the March 1989 GMD event that caused the Hydro Quebec blackout. The geomagnetic field measurement record of

the March 13-14 1989 GMD event, measured at NRCan's Ottawa geomagnetic observatory, was selected as the reference geomagnetic field waveform because it provides generally conservative results when performing thermal analysis of power transformers (see Appendix I). The reference geomagnetic field waveshape is used to calculate the GIC time series, GIC(t), required for transformer thermal impact assessment.

The geomagnetic latitude of the Ottawa geomagnetic observatory is 55°; therefore, the amplitude of the geomagnetic field measurement data were scaled up to the 60° reference geomagnetic latitude (see **Figure 1**) such that the resulting peak geoelectric field amplitude computed using the reference earth model was 8 V/km (see **Figures 2** and **3**). Sampling rate for the geomagnetic field waveshape is 10 seconds.



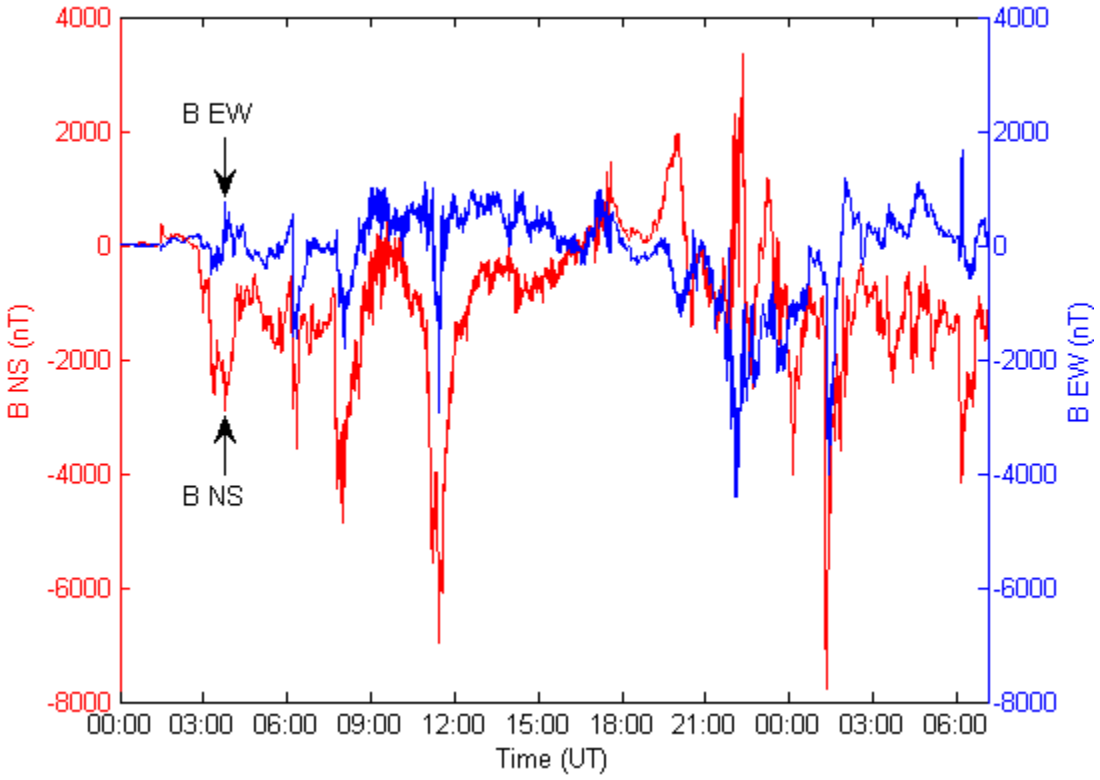
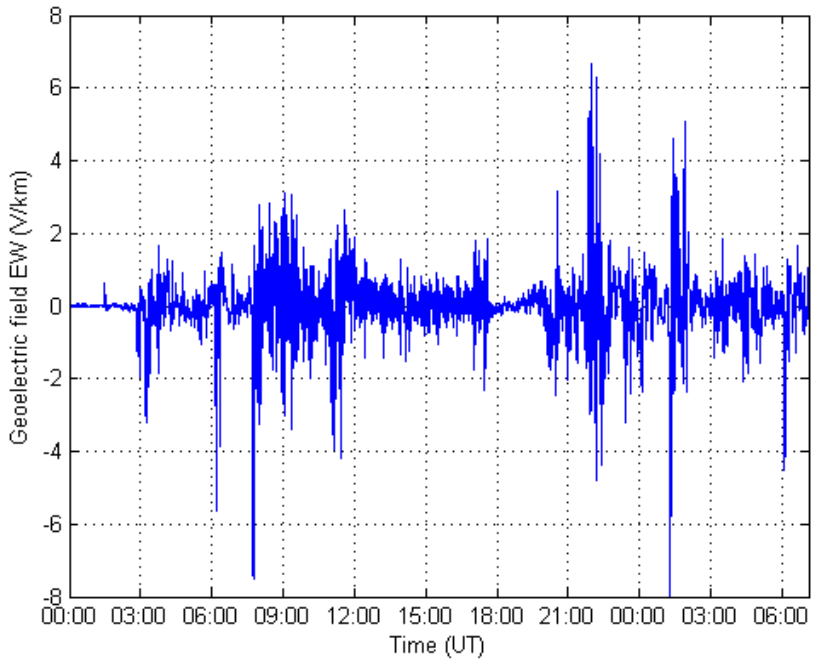


Figure 1: Benchmark Geomagnetic Field Waveshape
Red Bn (Northward), Blue Be (Eastward)



Referenced to pre-event quiet conditions

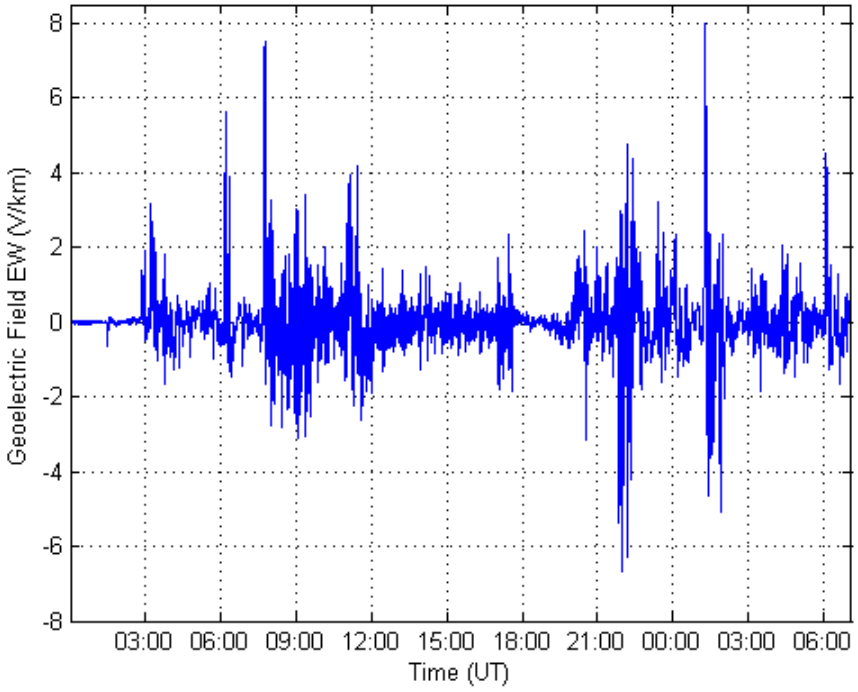
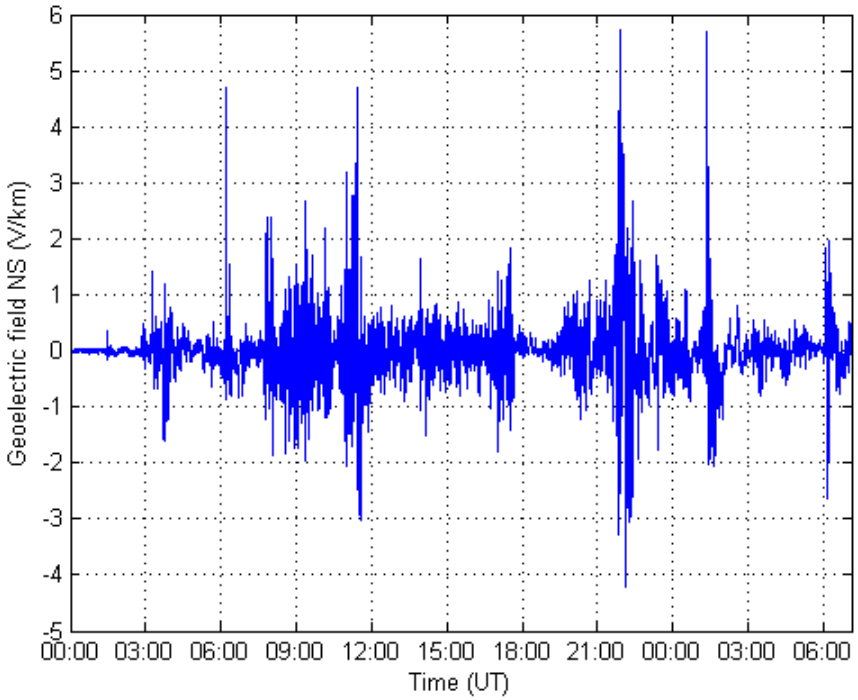


Figure 2: Benchmark Geoelectric Field Waveshape (E_E Eastward)



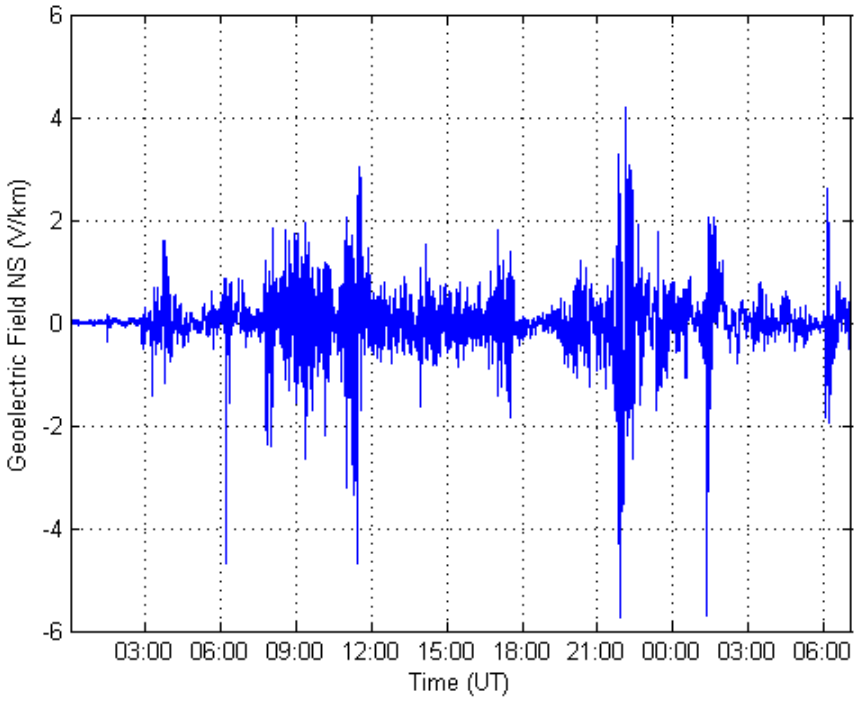


Figure 3: Benchmark Geoelectric Field Waveshape (E_N Northward)

Appendix I – Technical Considerations

The following sections describe the technical justification of the assumptions that were made in the development of the benchmark GMD event.

Statistical Considerations

Due to the lack of long-term accurate geomagnetic field observations, assigning probabilities to the occurrence of historical extreme geomagnetic storms is difficult because of the lack of high fidelity geomagnetic recordings of ~~pre-1980s~~ events prior to the 1980s. This is particularly true for the Carrington event for which data that allow the direct determination of the geoelectric fields experienced during the storm are not available [15].

The storm-time disturbance index Dst has often been used as a measure of storm strength even though it does not provide a direct correspondence with GIC[1]. One of the reasons for using Dst in statistical analysis is that Dst data are available ~~pre~~ for events occurring prior to 1980. Extreme value analysis of GMD events, including the Carrington, September 1859 and March 1989 events, has been carried out using Dst as an indicator of storm strength. In one such study [16], the (one sigma) range of 10-year occurrence probability for another March 1989 event was estimated to be between 9.4-27.8 percent. The range of 10-year occurrence probability for Carrington event in Love's analysis is 1.6-13.7 percent. These translate to occurrence rates of approximately 1 in 30-100 years for the March 1989 event and 1 in 70-600 years for the Carrington event. ~~It should be noted that the~~The error bars in such analysis are significant, ~~but~~however it ~~can be concluded~~is reasonable to conclude that statistically the March 1989 event is~~, statistically speaking,~~ likely more frequent than 1-in-100 years and the Carrington event is likely less frequent than 1-in-100 years.

The benchmark GMD event is based on a 1 in 100 year frequency of occurrence which is a conservative design basis for power systems. Also, the benchmark GMD event is not biased towards local geomagnetic field enhancements since it must address wide-area effects in the interconnected power system. Therefore, the use of Dst-based statistical considerations is not adequate in this context and only relatively modern data have been used.

The benchmark GMD event is derived from modern geomagnetic field data records and corresponding calculated geoelectric field amplitudes. Using such data allows rigorous statistical analysis of the occurrence rates of the physical parameter (i.e. rate of change in geomagnetic field, dB/dt) directly related to the geoelectric field. Geomagnetic field measurements from the IMAGE magnetometer chain for 1993-2013 have been used to study the occurrence rates of the geoelectric field amplitudes.

With the use of modern data it is possible to avoid bias caused by localized geomagnetic field enhancements. The spatial structure of high-latitude geoelectric fields can be very complex during strong geomagnetic storm events [17]-[18]. One reflection of this spatial complexity is localized geomagnetic field enhancements that result in high amplitude geoelectric fields in regions of a few hundred kilometers or less. **Figure I-1**[2] illustrates this spatial complexity of the storm-time geoelectric fields. In areas indicated by the bright red location, the geoelectric field can be a factor of 2-3 larger than at neighboring locations. Localized geomagnetic phenomena should not be confused with local earth structure/conductivity ~~conductivity~~ features that result~~s~~ in consistently high geoelectric fields (e.g., coastal effects). Localized field enhancements can occur at any region exposed to auroral ionospheric electric current fluctuations.

[1] Dst index quantifies the amplitude of the main phase disturbance of a magnetic storm. The index is derived from magnetic field variations recorded at four low-latitude observatories. The data is combined to provide a measure of the average main-phase magnetic storm amplitude around the world.

[2] **Figure I-1** is for illustration purposes only, and is not meant to suggest that any one area is more likely to experience a localized enhanced geoelectric field.

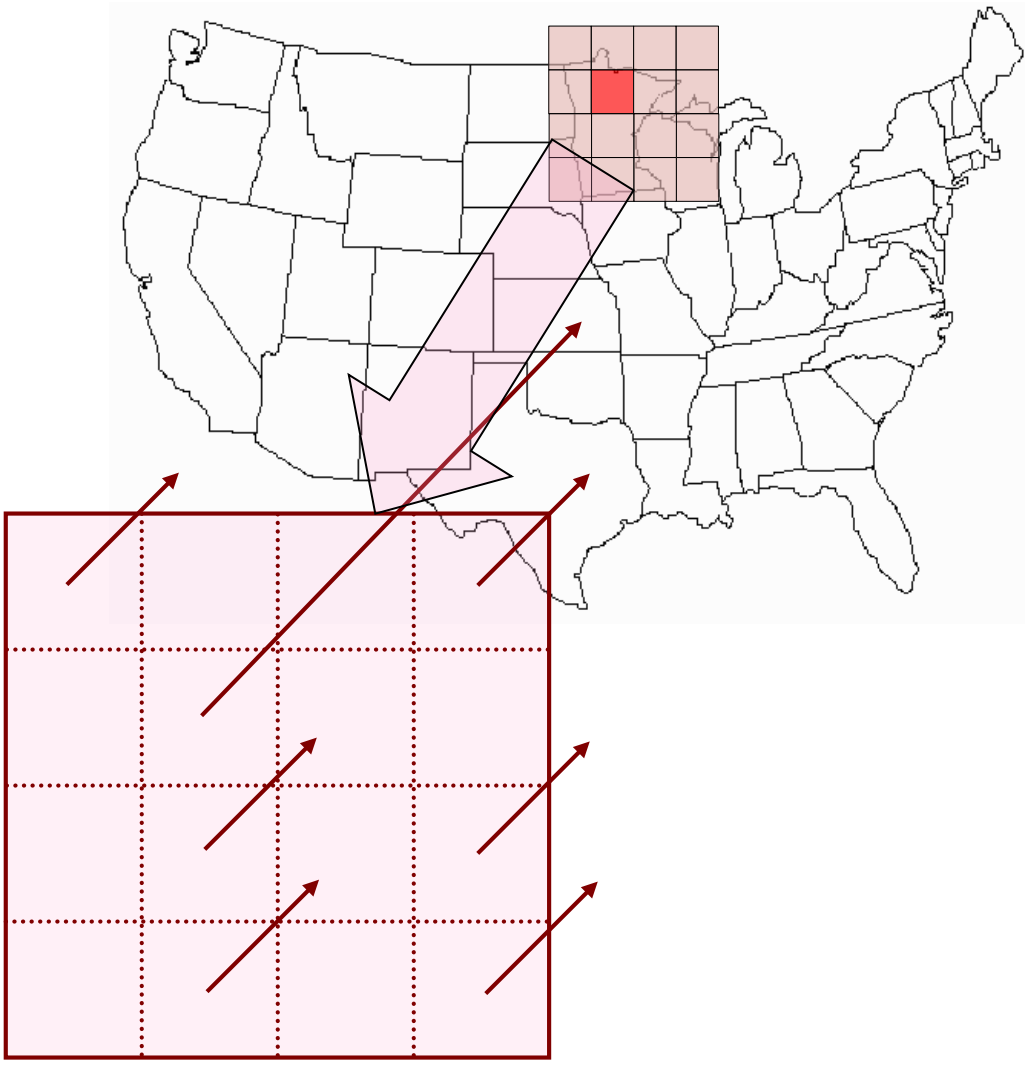


Figure I-1: Illustration of the ~~spatial scale~~Spatial Scale between ~~localized enhancements~~Localized Enhancements and ~~larger spatial scale amplitudes~~Larger Spatial Scale Amplitudes of ~~geoelectric field observed~~Geoelectric Field Observed during a ~~strong geomagnetic storm.~~ Strong Geomagnetic Storm.
In this illustration, the red square illustrates a spatially localized field enhancement.

The benchmark event is designed to address wide-area effects caused by a severe GMD event, such as increased var absorption and voltage depressions. Without ~~characterization of~~characterizing GMD on regional scales, statistical estimates could be weighted by local effects and suggest unduly pessimistic conditions ~~from~~when considering cascading failure and voltage collapse~~ points of view~~. It is important to note that most earlier geoelectric field amplitude statistics and extreme amplitude analyses have been built for individual stations thus reflecting only localized spatial scales [10], [19]-[22]. A modified analysis is required to account for geoelectric field amplitudes at larger spatial scales. Consequently, analysis of spatially averaged geoelectric field amplitudes is presented below.

Figure I-2 shows statistical occurrence of spatially averaged high latitude geoelectric field amplitudes for the period of January 1, 1993 – December 31, 2013. The geoelectric field amplitudes were calculated using 10-s IMAGE magnetometer array observations and the Quebec ground conductivity model, which is used as a reference in the benchmark GMD event. Spatial averaging was carried out over four different station groups spanning a square

area of approximately 500 km in width. For the schematic situation in **Figure I-1** the averaging process ~~would involve~~involves taking the average of the geoelectric field amplitudes over all 16 points or squares.

As can be seen from **Figure I-2**, the computed spatially averaged geoelectric field amplitude statistics indicate the 1-in-100 year amplitude is approximately between 3-8 V/km. Using extreme value analysis as described in the next section, it can be shown that the upper limit of the 95% confidence interval for a 100-year return level is more precisely 5.77 V/km.

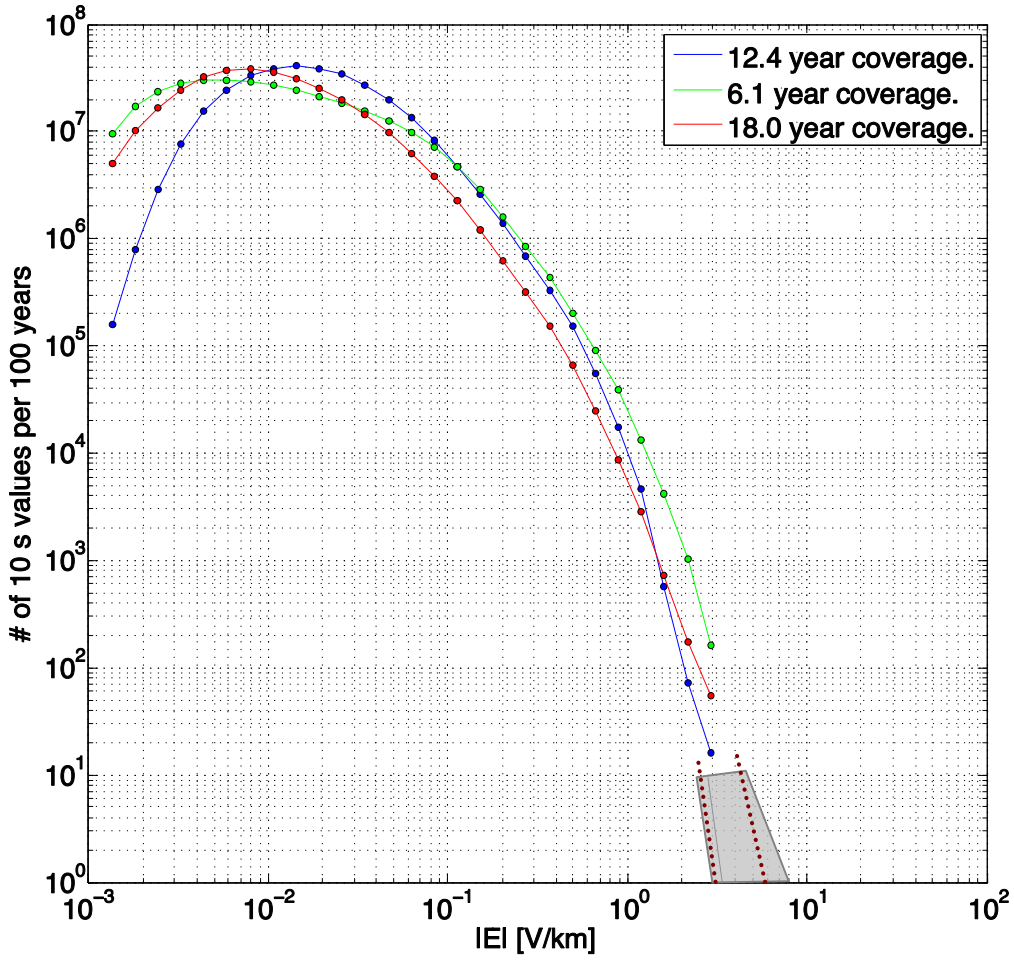


Figure I-2: Statistical ~~o~~Occurrence of ~~spatially averaged geoelectric field amplitudes~~Spatially Averaged Geoelectric Field Amplitudes. Four curves with dots correspond to different station groups and the gray area shows a visual extrapolation to 1-in-100 year amplitudes. Dashed lines represent the values predicted with extreme value analysis. The legend shows the data coverage for each station group used in computing the averaged geoelectric field amplitudes.

Extreme Value Analysis

The objective of extreme value analysis is to describe the behavior of a stochastic process at extreme deviations from the median. In general, the intent is to quantify the probability of an event more extreme than any previously observed. In particular, we are concerned with estimating the 95 percent confidence interval of the maximum geo-electric field amplitude to be expected within a 100-year return period.[3] In the context of this document, extreme value analysis has been used to rigorously support the extrapolation estimates used in the statistical considerations of the previous section.

The data set consists of 21 years of daily maximum geoelectric field amplitudes derived from the IMAGE magnetometer chain, using the Quebec earth model as reference. **Figure I-3** shows a scatter plot of the 10-largest geoelectric field amplitudes per year across the IMAGE stations. The plot indicates that both the amplitude and standard deviation of extreme geoelectric fields are not independent of the solar cycle. The data clearly exhibits heteroskedasticity[4] and an 11-year seasonality in the mean.

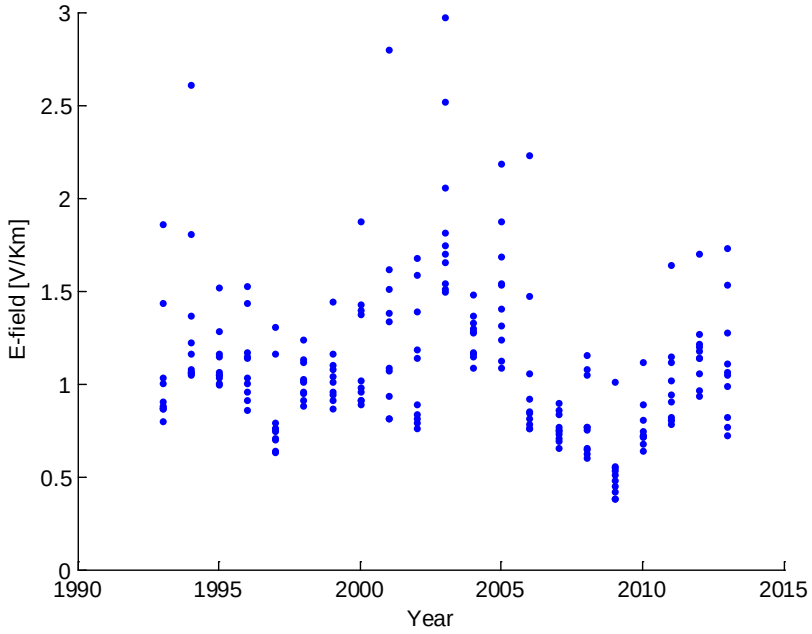


Figure I-3: Scatter Plot of Ten Largest Geoelectric Fields per Year

Data source: IMAGE magnetometer chain from 1993-2013

Several statistical methods can be used to conduct extreme value analysis. The most commonly applied include: Generalized Extreme Value (GEV), Point Over Threshold (POT), R-Largest, and Point Process (PP). In general, all methods assume independent and identically distributed (iid) data [23].

Two of these methods, GEV and POT, have been applied to the geoelectric field data, and their suitability for this application has been examined. **Table I-1** shows a summary of the estimated parameters and return levels obtained from GEV and POT methods. The parameters were estimated using the Maximum Likelihood Estimator (MLE). Since the distribution parameters do not have an intuitive interpretation, the expected geoelectric field amplitude for a 100-year return period is also included in **Table I-1.** The 95 percent confidence interval of the 100-year return level was calculated using the delta method and the profile likelihood. The delta method relies on the

[3] A 95 percent confidence interval means that, if we were to obtain repeated samples, the return level would lie within the confidence interval for 95 percent of the samples.

[4] Heteroskedasticity means that the skedastic function depends on the values of the conditioning variable; i.e., *var(Y|X=x) = f(x)*.

Gaussian approximation to the distribution of the MLE; this approximation can be poor for long return periods. In general, the profile likelihood provides a better description of the return level.

Table I-1: Extreme Value Analysis

Statistical Method	Estimated Parameters	Hypothesis Testing	100 Year Return Level Mean [V/km]	95% CI [V/km]	95% CI P-Likelihood [V/km]
(1) GEV	μ=1.4499 (0.1090) σ=0.4297 (0.0817) ξ=0.0305 (0.2011)	H0: ξ=0 *p* = 0.877	3.57	[1.77 , 5.36]	[2.71, 10.26]
(2) GEV ~~$\mu = \beta_0 + \beta_1 \cdot \sin\left(\frac{t}{T} + \phi\right)$~~ $\mu = \beta_0 + \beta_1 \cdot \sin\left(\frac{t}{T} + \phi\right)$	β_0=1.5047 (0.0753) β_1=0.3722 (0.0740) σ=0.2894 (0.0600) ξ=0.1891 (0.2262)	H0: β_1=0 *p*= 0.0003 H0: ξ=0 *p* = 0.38	4	[2.64, 4.81]	[2.92, 12.33]
(3) POT, threshold=1V/km	σ=0.3163 (0.0382) ξ=0.0430 (0.0893)		3.4	[2.28, 4.52]	[2.72,5.64]
(4) POT, threshold=1V/km ~~$\sigma = \alpha_0 + \alpha_1 \cdot \sin\left(\frac{t}{T} + \phi\right)$~~ $\sigma = \alpha_0 + \alpha_1 \cdot \sin\left(\frac{t}{T} + \phi\right)$	α_0=0.2920 (0.0339) α_1=0.1660 (0.0368) ξ=-0.0308 (0.0826)	H0: α_1=0 *p*= 3.7e-5	3.724	[2.64, 4.81]	[3.02, 5.77]

Statistical model (1) in **Table I-1** is the traditional GEV estimation using blocks of 1 year maxima; i.e., only 21 data points are used in the estimation. The mean expected amplitude of the geolectric field for a 100-year return level is 3.57 V/km. Since GEV works with blocks of maxima, it is typically regarded as a wasteful approach. This is reflected in the comparatively large confidence intervals: [1.77, 5.36] V/km for the delta method and [2.71, 10.26] V/km for the profile likelihood.

As discussed previously, GEV assumes that the data is iid. Based on the scatter plot shown in **Figure 1-3**, the iid statistical assumption is not warranted by the data. Statistical model (2) in **Table I-1** is a re-parameterization of the GEV distribution contemplating the 11-year seasonality in the mean,

~~$\mu = \beta_0 + \beta_1 \cdot \sin\left(\frac{t}{T} + \phi\right)$~~ $\mu = \beta_0 + \beta_1 \cdot \sin\left(\frac{t}{T} + \phi\right)$

where β_0 represents the offset in the mean, β_1 describes the 11-year seasonality, *T* is the period (11 years), and ϕ is a constant phase shift.

A likelihood ratio test is used to test the hypothesis that β_1 is zero. The null hypothesis, H0: β_1=0, is rejected with a p-value of 0.0003; as expected, the 11-year seasonality has explanatory power. The blocks of maxima during the

solar minimum are better represented in the re-parameterized GEV. The ~~upshot~~benefit is an increase in the mean return level to 4 V/km and a wider confidence interval: [2.63, 4.81] V/km for the delta method and [2.92, 12.33] V/km for the profile likelihood (calculated at solar maximum).

Statistical model (3) in **Table I-1** is the traditional POT estimation using a threshold *u* of 1 V/km; the data was de-clustered using a 1-day run. The data set consists of normalized excesses over a threshold, and therefore, the sample size for POT is increased if more than one extreme observation per year is available (in the GEV approach, only the maximum observation over the year was taken; in the POT method, a single year can have multiple observations over the threshold). The selection of the threshold *u* is a compromise between bias and variance. The asymptotic basis of the model relies on a high threshold; a threshold that is too low ~~a threshold~~ will likely lead to bias. On the other hand, ~~too high~~ a threshold that is too high will reduce the sample size and result in high variance. The stability of parameter estimates can guide the selection of an appropriate threshold. **Figure I-4** shows the estimated parameters (modified scale $\sigma^*=\sigma_u-\xi\cdot u$, and shape ξ) for a range of thresholds. The objective is to select the lowest threshold for which the estimates remain near constant; 1V/km appears to be a good choice.

The mean return level for statistical model (3), 3.4 V/km, is similar to the GEV estimates. However, due to the larger sample size the POT method is more efficient, and consequently, the confidence intervals are significantly reduced: [2.28, 4.52] V/km for the delta method, and [2.72, 5.64] V/km for the profile likelihood method.

In order to cope with the heteroskedasticity exhibited by the data, a re-parameterization of POT is used in statistical model (4) in **Table I-1**,

~~$\sigma = \alpha_0 + \alpha_1 \cdot \sin\left(\frac{t}{T} + \phi\right)$~~ $\sigma = \alpha_0 + \alpha_1 \cdot \sin\left(\frac{t}{T} + \phi\right)$

where α_0 represents the offset in the standard deviation, α_1 describes the 11-year seasonality, *T* is the period (365.25 · 11), and ϕ is a constant phase shift.

The parameter α_1 is statistical significant; the null hypothesis, H0: $\alpha_1=0$, is rejected with a p-value of 3.7e-5. The mean return level has slightly increased to 3.72 V/km. The upper limit of the confidence interval, calculated at solar maximum, also increases: [2.63, 4.81] V/km for the delta method and [3.02, 5.77] V/km for the profile likelihood method. As a final remark, it is emphasized that the confidence interval obtained using the profile likelihood is preferred over the delta method. **Figure I-5** shows the profile likelihood of the 100-year return level of statistical model (4). Note that the profile likelihood is highly asymmetric with a positive skew, rendering a larger upper limit for the confidence interval. Recall that the delta method assumes a normal distribution for the MLEs, and therefore, the confidence interval is symmetric around the mean.

To conclude, traditional GEV (1) and POT (3) models are misspecified; the statistical assumptions (iid) are not warranted by the data. The models were re-parameterized to cope with heteroskedasticity and the 11-year seasonality in the mean. Statistical model (4) better utilizes the available extreme measurements and it is therefore preferred over statistical model (2). The upper limit of the 95 percent confidence interval for a 100-year return level is 5.77 V/km. This analysis shows that the geoelectric field amplitude of 8 V/km for the benchmark is conservative for a 100-year return level and it includes an implicit 25 percent ~~safety~~engineering margin.

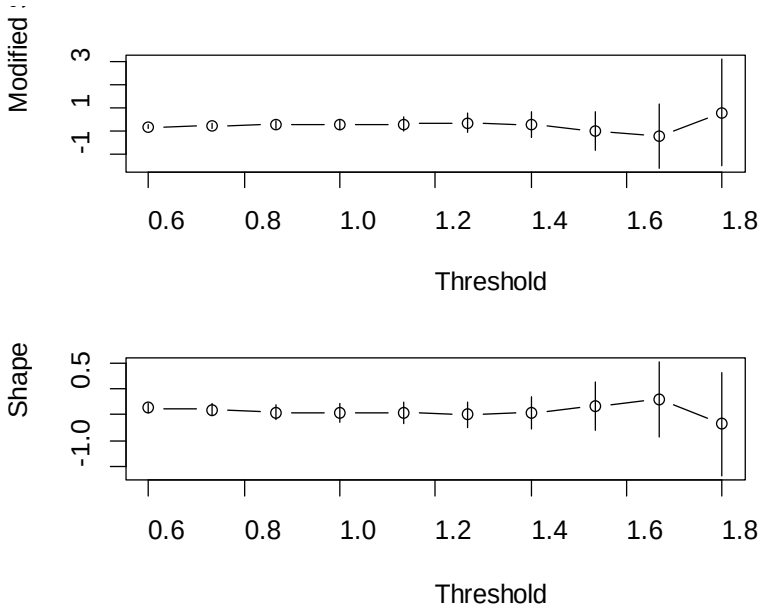


Figure I-4: Parameter Estimates Against Threshold for Statistical Model (3)

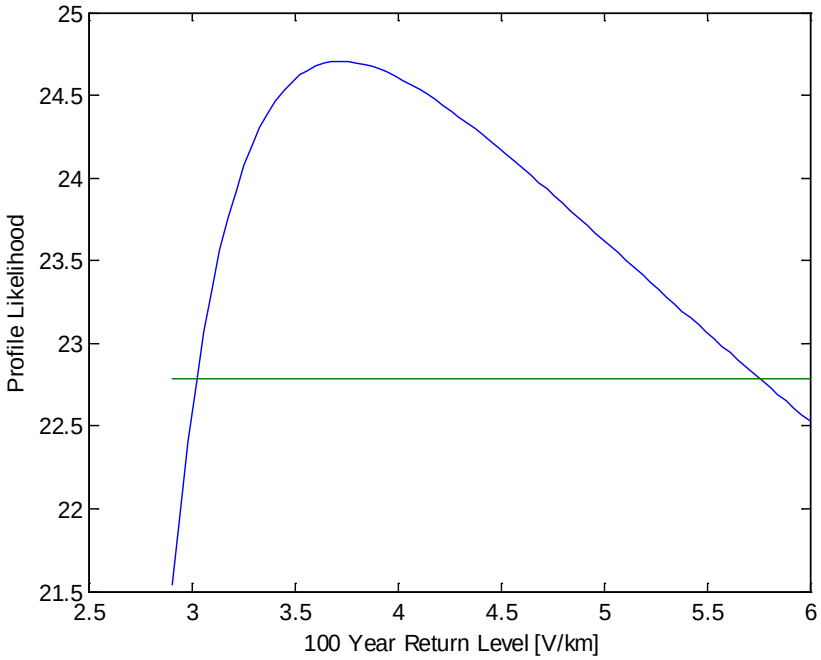


Figure I-5: Profile Likelihood for 100-year Return Level for Statistical Model (4)

Impact of Local Geomagnetic Disturbances on GIC

The impact of local disturbances on a power network is illustrated with the following example. A 500 km by 500 km section of a North American transmission network ~~was~~is subdivided into 100 km by 100 km sections. The geoelectric field is assumed to be uniform within each section. The analysis is performed by scaling the geoelectric field in each section individually by an intensification factor of 2.5 and computing the corresponding GIC flows in the network, resulting in a total of 25 GIC distribution simulations.[5] In these simulations the peak geomagnetic field amplitude has been scaled according to geomagnetic latitude of the network under study.

Figure I-6 shows the number of transformers that experience a GIC increase greater than 10 Amps (in red), those that experienced a reduction in GIC of more than 10 Amps (in blue), and those that remain essentially the same (in green). It can be observed that there is a small set of transformers that are affected by the local amplification of the geo-electric field but that the impact on the GIC distribution of the entire network due to a local intensification of the geoelectric field in a "local peak" is minor. Therefore, it can be concluded that the effect of local disturbances on the larger transmission system is relatively minor and do~~es~~ not warrant further consideration in network analysis.

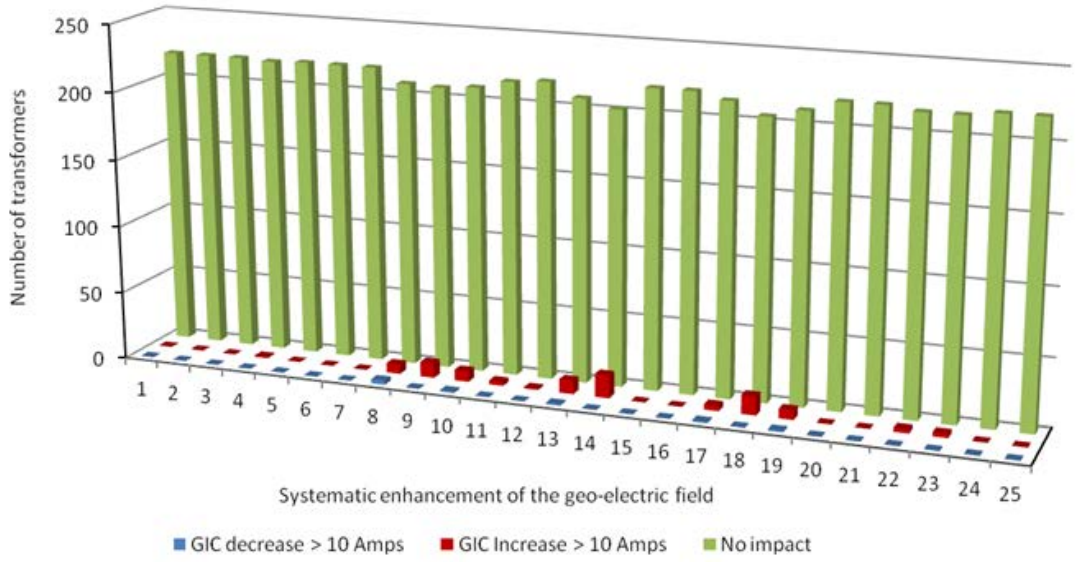


Figure I-6: Number of Transformers ~~That See~~that see a 10 A/phase Change in GIC ~~Due To~~due to Local Geoelectric Field Intensification

Impact of Waveshape on Transformer Hot-spot Heating

Thermal effects (e.g. hot spot transformer heating) in power transformers are not instantaneous. Thermal time constants associated with hot spot heating in power transformers are in the 5-20 minute range; therefore, the waveshape of the geomagnetic and geoelectric field has a strong impact on transformer hot spot heating of windings and metallic parts since thermal time constants are of the same order of magnitude as the time-to-peak of storm maxima. The waveshape of the March 13-14 1989 GMD event measured at the Ottawa geomagnetic observatory was found to be a conservative choice when compared with other events of the last 20 years, such

[5] An intensification factor of 2.5 would make a general 8 V/km peak geoelectric field in the entire network show a 20 V/km intensified geoelectric field in one of the twenty five 100 km by 100 km sections.

as the reference storm of the NERC interim report of 2012 [14], measurements at the Nurmijarvi (NUR) and Memanbetsu (MMB) geomagnetic observatories for the "Halloween event" of October 29-31, 2003.

To illustrate, the results of a thermal analysis performed on a relatively large test network with a diverse mix of circuit lengths and orientations is provided in **Figures I-7** and **I-8**. These results illustrate the relative effect of different waveshapes in a broad system setting and should not be interpreted as a vulnerability assessment of any particular network.

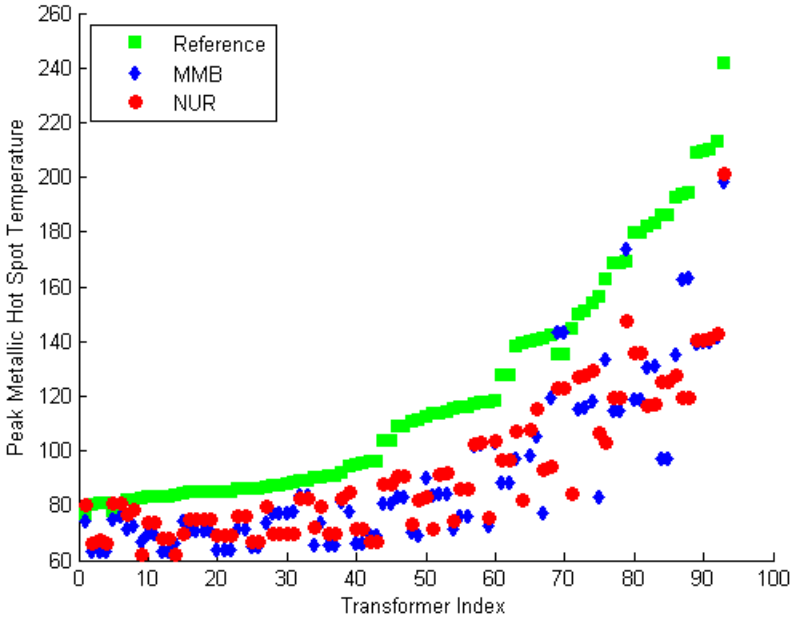


Figure I-7: Calculated ~~peak metallic hot spot temperature~~Peak Metallic Hot Spot Temperature for ~~all transformers~~All Transformers in a ~~test system~~Test System with a ~~temperature increase~~Temperature Increase of ~~more than~~More Than 20°C for ~~d~~Different GMD ~~events scaled~~Events Scaled to the ~~same peak geoelectric field~~Same Peak Geoelectric Field

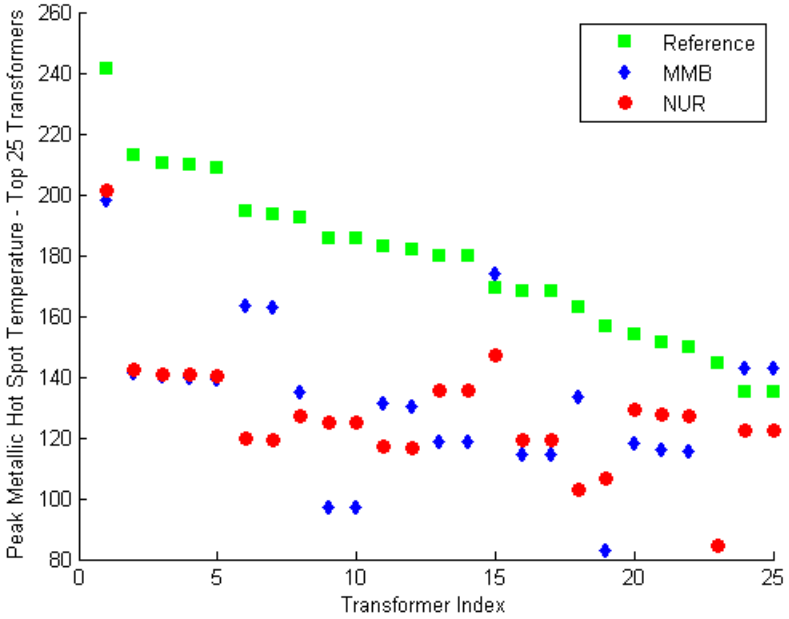


Figure I-8: Calculated ~~peak metallic hot spot temperature~~Peak Metallic Hot Spot Temperature for the ~~t~~Top 25 ~~t~~Transformers in a ~~test system~~Test System for ~~d~~Different GMD ~~events scaled~~Events Scaled to the ~~same peak geoelectric field~~Same Peak Geoelectric Field

Appendix II – Scaling the Benchmark GMD Event

The intensity of a GMD event depends on geographical considerations such as geomagnetic latitude[6] and local earth conductivity[7] [3]**.** Scaling factors for geomagnetic latitude take in consideration that the intensity of a GMD event varies according to latitude-based geographical location. Scaling factors for earth conductivity take into account that the induced geoelectric field depends on earth conductivity, and that different parts of the continent have different earth conductivity and deep earth structure.

Scaling the Geomagnetic Field

The benchmark GMD event is defined for geomagnetic latitude of 60° and it must be scaled to account for regional differences based on geomagnetic latitude. To allow usage of the reference geomagnetic field waveshape in other locations, **Table II-1** ~~provides a~~summarizes the scaling factor α correlating peak geoelectric field to geomagnetic latitude as described in **Figure II-1** [3]. This scaling factor α has been obtained from a large number of global geomagnetic field observations of all major geomagnetic storms since the late 1980s [15], [24]-[25], and can be approximated with the empirical expression in (II.1)

$$\alpha = 0.001 \cdot e^{(0.115 \cdot L)} \quad \text{(II.1)}$$

where L is the geomagnetic latitude in degrees and $0.1 \leq \alpha \leq 1.0$.

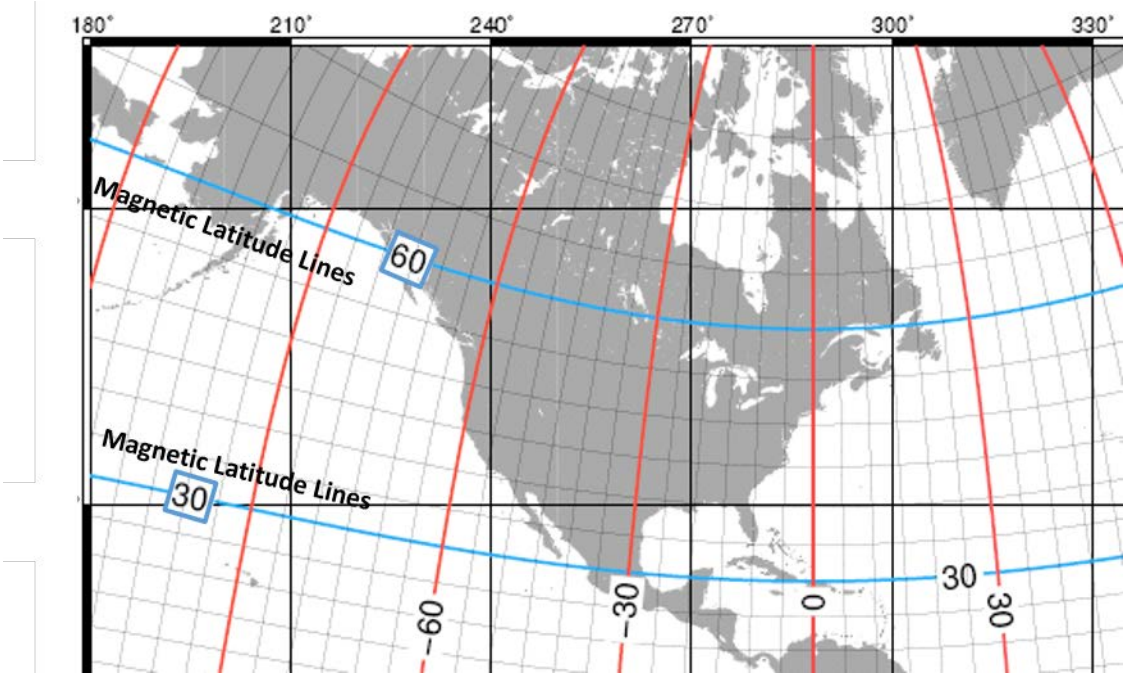


Figure II-1: Geomagnetic Latitude Lines in North America

[6] Geomagnetic latitude is analogous to geographic latitude, except that bearing is ~~with respect~~in relation to the magnetic poles, as opposed to the geographic poles. Geomagnetic phenomena are often best organized as a function of geomagnetic coordinates.

[7] Local earth conductivity refers to the electrical characteristics to depths of hundreds of km down to the earth's mantle. In general terms, lower ground conductivity results in higher geoelectric field amplitudes.

Table II-1: Geomagnetic Field Scaling Factors	
Geomagnetic Latitude (Degrees)	Scaling Factor1 (α)
≤ 40	0.10
45	0.2
50	0.3
~~55~~54	0.~~6~~5
56	0.6
57	0.7
58	0.8
59	0.9
≥ 60	1.0

Scaling the Geoelectric Field

The benchmark GMD event is defined for the reference Quebec earth model provided in **Table 1**. This earth model has been used in many peer-reviewed technical articles [12, 15]. The peak geoelectric field depends on the geomagnetic field waveshape and the local earth conductivity. Ideally, the peak geoelectric field, E_{peak}, is obtained by calculating the geoelectric field from the scaled geomagnetic waveshape using the plane wave method and taking the maximum value of the resulting waveforms

$$E_N = (z(t)/\mu_o) * B_E(t)$$
$$E_E = -(z(t)/\mu_o) * B_N(t) \quad \text{(II.2)}$$
$$E_{peak} = \max\left\{\left|E_E(t), E_N(t)\right|\right\}$$

where,

* denotes convolution in the time domain,

z(t) is the impulse response for the earth surface impedance calculated from the laterally uniform or 1D earth model,

$B_E(t)$, $B_N(t)$ are the scaled Eastward and Northward geomagnetic field waveshapes,

$E_E(t)$, $E_N(t)|$ are the magnitudes of the calculated Eastward and Northward geoelectric field $E_E(t)$ and $E_N(t)$.

As noted previously, the response of the earth to B(t) (and dB/dt) is frequency dependent. **Figure II-2** shows the magnitude of Z(ω) for the reference earth model.

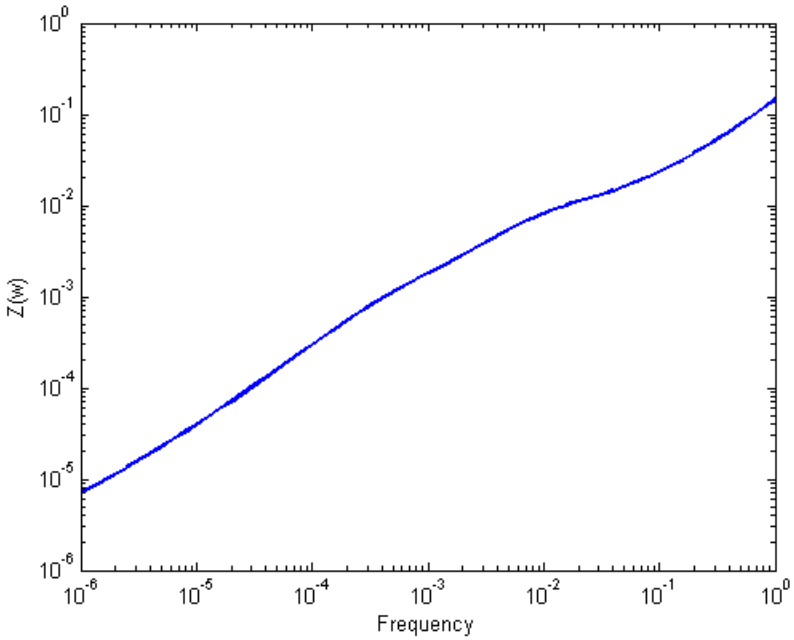


Figure II-2: Magnitude of the Earth Surface Impedance for the Reference Earth Model

If a utility does not have the capability of calculating the waveshape or time series for the geoelectric field, an earth conductivity scaling factor β can be obtained from **Table II-2**. Using α and β, the peak geoelectric field E_{peak} for a specific service territory shown in **Figure II-3** can be obtained using (II.3)

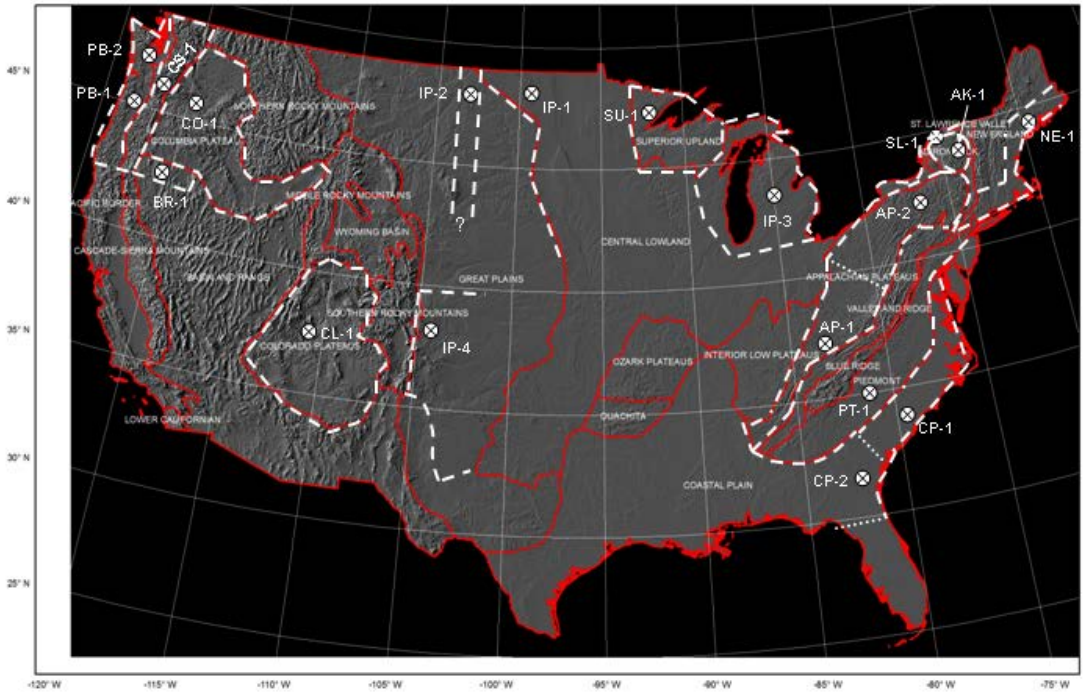
$$E_{peak} = 8 \times \alpha \times \beta \text{ (V/km)} \quad \text{(II.3)}$$

It should be noted that (II.3) is an approximation based on the following assumptions:

- The earth models used to calculate Table II-2 for the United States ~~is~~are from magnetotelluric data and ~~is~~are available from the USGS website.
- The models used to calculate Table II-2 for Canada were obtained from NRCan and reflect the average structure for large regions. When models are developed for sub-regions these will all be different (to a greater or lesser degree) from the average model. For instance, detailed models for Ontario have been developed by NRCan and ~~comprise~~consist of seven major sub-regions.
- The conductivity scaling factor β is calculated as the quotient of the local geoelectric field peak amplitude in a physiographic region with respect to the reference peak amplitude value of 8 V/km. Both geoelectric field peaks amplitudes are calculated using the reference geomagnetic field time series. If a different geomagnetic field time series were used, the calculated scaling factors β would be different than the values in Table II-2 because the frequency content of storm maxima is, in principle, different for every storm. However, the reference time series produces generally more conservative values of β when compared to the time series of reference storm of the NERC interim report of 2012 [14], measurements at the Nurmijarvi (NUR) and Memanbetsu (MMB) geomagnetic observatories for the "Halloween event" of October 29-31, 2003, and other recordings of the March 1989 event at high latitudes (Meanook observatory, Canada). The average variation between minimum and maximum β is approximately 12 percent. **Figure II-4** illustrates the values of β calculated using the 10-second ~~geomagnetic field~~ recordings for these geomagnetic field time series.

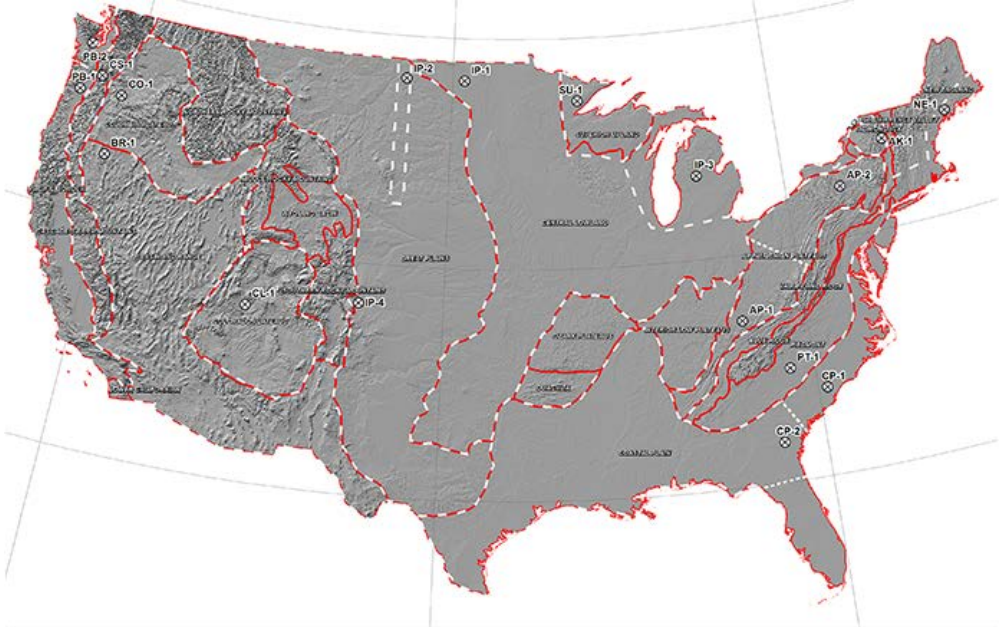
- If a utility has technically-sound earth models for its service territory ~~of~~and sub-regions thereof, then the use of such earth models is preferable to estimate E_{peak}.

Location of 1D Earth Resistivity Models with respect to Physiographic Regions of the USA



- When a ground conductivity model is not available the planning entity should use a β factor of 1 or other technically-justified value.

Physiographic Regions of the Continental United States



Physiographic Regions of Canada

Figure II-3: Physiographic Regions of North America

Table II-2 Geoelectric Field Scaling Factors	
USGS Earth model	Scaling Factor (β)
AK1A	0.56
AK1B	.0.56
AP1	0.33
AP2	0.82
BR1	0.22
CL1	0.76
CO1	0.27
CP1	0.81
CP2	0.95
CS1	0.41
IP1	0.94
IP2	0.28
IP3	0.93
IP4	0.41
NE1	0.81
PB1	0.62

PB2	0.46
PT1	1.17
SL1	0.53
SU1	0.93
BOU	0.28
FBK	0.56
PRU	0.21
BC	0.67
PRAIRIES	0.96
SHIELD	1.0
ATLANTIC	0.79

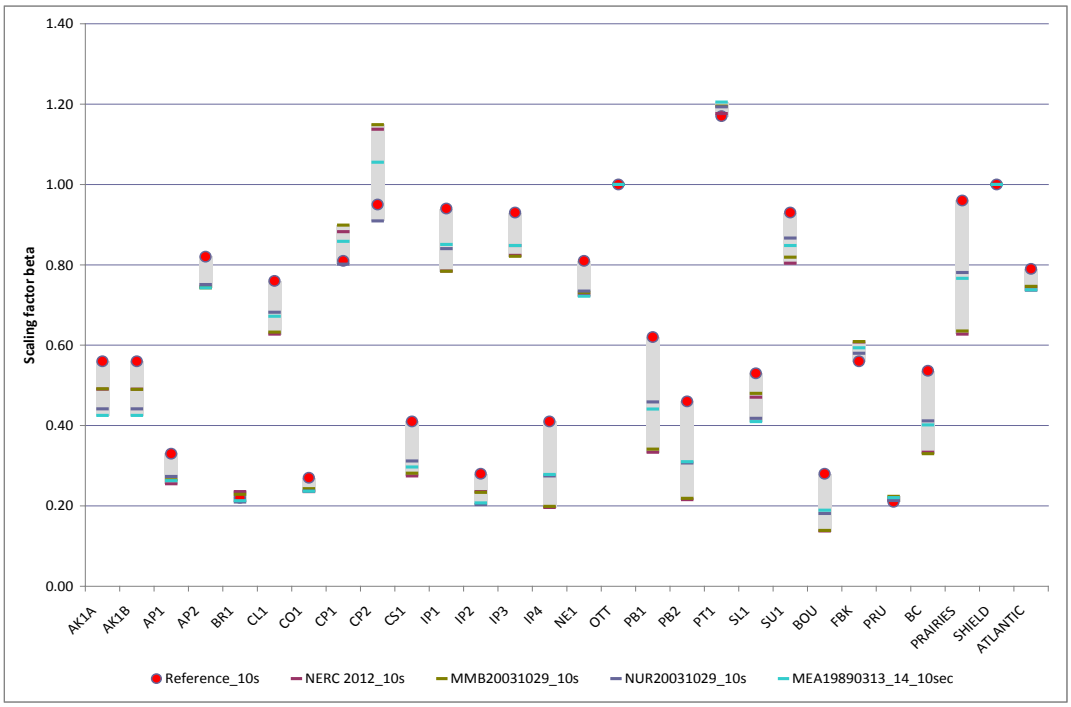


Figure II-4: Beta factors Calculated for Different GMD Events
Red circles corresponds to the values in Table II-2

Example Calculations

Example 1

Consider a transmission service territory that lies in a geographical latitude of 45.5°, which translates to a geomagnetic latitude of 55°. The scaling factor α ~~from **Table**~~calculated using II-1 is 0.56~~2~~; therefore, the benchmark waveshape and the peak geoelectric field will be scaled accordingly. If the service territory has the same earth conductivity as the benchmark then β=1, and the peak geoelectric field will be

$$\alpha = 0.56$$
$$\beta = 1.0$$
$$E_{peak} = 8 \times 0.56 \times 1 = 4.5 V/km$$
$$\alpha = 0.562$$
$$\beta = 1$$
$$Epeak = 8 \times 0.562 \times 1 = 4.5 \text{ V/km}$$

If the service territory spans more than one physiographic region (i.e. several locations within the service territory have a different earth model) then the largest α can be used across the entire service territory for conservative results. Alternatively, the network can be split into multiple subnetworks, and the corresponding geoelectric field amplitude can be applied to each subnetwork.

Example 2

Consider a service territory that lies in a geographical latitude of 45.5° which translates to a geomagnetic latitude of 55°. The scaling factor α ~~from **Table**~~calculated using II-.1 is 0.56~~2~~; therefore, the benchmark waveshape and the peak geoelectric field will be scaled accordingly.

The service territory has lower conductivity that the reference benchmark conductivity, and according to the conductivity factor β from Table II-2. Then:

Conductivity factor β=1.17

$$\alpha = 0.56$$

$$E_{peak} = 8 \times 0.56 \times 1.17 = 5.2V / km$$

$$\alpha = 0.562$$

$$\beta = 1.17$$

$$Epeak = 8 \times 0.562 \times 1.17 = 5.3\ \mathrm{V/km}$$

References

[1] L. Bolduc, A. Gaudreau, A. Dutil, "Saturation Time of Transformers Under dc Excitation", Electric Power Systems Research, 56 (2000), pp. 95-102

[2] *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*, A Jointly-Commissioned Summary Report of the North American Reliability Corporation and the U.S. Department of Energy's November 2009 Workshop.

[3] Application Guide: Computing Geomagnetically-Induced Current in the Bulk-Power System, NERC. NERC. http://www.nerc.com/comm/PC/Geomagnetic%20Disturbance%20Task%20Force%20GMDTF%202013/GIC%20Application%20Guide%202013_approved.pdf

[4] Kuan Zheng, Risto Pirjola, David Boteler, Lian-guang Liu, "Geoelectric Fields Due to Small-Scale and Large-Scale Source Currents", *IEEE Transactions on Power Delivery*, Vol. 28, No. 1, January 2013, pp. 442-449.

[5] Boteler, D. H. "Geomagnetically Induced Currents: Present Knowledge and Future Research", *IEEE Transactions on Power Delivery*, Vol. 9, No. 1, January 1994, pp. 50-58.

[6] Boteler, D. H. "Modeling Geomagnetically Induced Currents Produced by Realistic and Uniform Electric Fields", *IEEE Transactions on Power Delivery*, Vol. 13, No. 4, January 1998, pp. 1303-1308.

[7] J. L. Gilbert, W. A. Radasky, E. B. Savage, "A Technique for Calculating the Currents Induced by Geomagnetic Storms on Large High Voltage Power Grids", Electromagnetic Compatibility (EMC), 2012 IEEE International Symposium on.

[8] *How to Calculate Electric Fields to Determine Geomagnetically-Induced Currents.* EPRI, Palo Alto, CA: 2013. 3002002149.

[9] Pulkkinen, A., R. Pirjola, and A. Viljanen, Statistics of extreme geomagnetically induced current events, Space Weather, 6, S07001, doi:10.1029/2008SW000388, 2008.

[10] Boteler, D. H., Assessment of geomagnetic hazard to power systems in Canada, Nat. Hazards, 23, 101–120, 2001.

[11] Finnish Meteorological Institute's IMAGE magnetometer chain data available at: http://image.gsfc.nasa.gov/

[12] Boteler, D. H., and R. J. Pirjola, The complex-image method for calculating the magnetic and electric fields produced at the surface of the Earth by the auroral electrojet, Geophys. J. Int., 132(1), 31—40, 1998

[13] ANSI Standard C2, *National Electric Safety Code*, 2012, ISBN 978-0-7381-6588-2

[14] 2012 Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System. NERC. February 2012. http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2012GMD.pdf

[15] Pulkkinen, A., E. Bernabeu, J. Eichner, C. Beggan and A. Thomson, Generation of 100-year geomagnetically induced current scenarios, *Space Weather*, Vol. 10, S04003, doi:10.1029/2011SW000750, 2012.

[16] Love, J., Credible occurrence probabilities for extreme geophysical events: Earthquakes, volcanic eruptions, magnetic storms, Geophysical Research Letters, Vol. 39, L10301, doi:10.1029/2012GL051431, 2012.

[17] Pulkkinen, A., A. Thomson, E. Clarke, and A. Mckay, April 2000 geomagnetic storm: ionospheric drivers of large geomagnetically induced currents, Annales Geophysicae, 21, 709-717, 2003.

[18] Pulkkinen, A., S. Lindahl, A. Viljanen, and R. Pirjola, Geomagnetic storm of 29–31 October 2003: Geomagnetically induced currents and their relation to problems in the Swedish high-voltage power transmission system, Space Weather, 3, S08C03, doi:10.1029/2004SW000123, 2005.

[19] Pulkkinen, A., R. Pirjola, and A. Viljanen, Statistics of extreme geomagnetically induced current events, Space Weather, 6, S07001, doi:10.1029/2008SW000388, 2008.

[20] Langlois, P., L. Bolduc, and M. C. Chouteau, Probability of occurrence of geomagnetic storms based on a study of the distribution of the electric field amplitudes measured in Abitibi, Québec, in 1993–1994, J. Geomagn. Geoelectr., 48, 1033–1041, 1996.

[21] Pulkkinen, A., R. Pirjola, and A. Viljanen, Statistics of extreme geomagnetically induced current events, Space Weather, 6, S07001, doi:10.1029/2008SW000388, 2008.

[22] Campbell, W. C., Observation of electric currents in the Alaska oil pipeline resulting from auroral electrojet current sources, Geophys. J. R. Astron. Soc., 61, 437–449, 1980.

[23] Coles, Stuart (2001). An Introduction to Statistical Modelling of Extreme Values. Springer.

[24] Ngwira, C., A. Pulkkinen, F. Wilder, and G. Crowley, Extended study of extreme geoelectric field event scenarios for geomagnetically induced current applications, Space Weather, Vol. 11, 121–131, doi:10.1002/swe.20021, 2013.

[25] Thomson, A., S. Reay, and E. Dawson. Quantifying extreme behavior in geomagnetic activity, Space Weather, 9, S10001, doi:10.1029/2011SW000696, 2011.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Transformer Thermal Impact Assessment White Paper (Draft)

Project 2013-03 (Geomagnetic Disturbance Mitigation)

TPL-007-1 Transmission System Planned Performance ~~during~~for Geomagnetic ~~Disturbances~~Disturbance Events

Background

On May 16, 2013, FERC issued Order No. 779, directing NERC to develop Standards that address risks to reliability caused by geomagnetic disturbances (GMDs) in two stages:

- Stage 1 Standard(s) that require applicable entities to develop and implement Operating Procedures. ~~The Stage 1 Standard,~~ EOP-010-1 – Geomagnetic Disturbance Operations is pending at FERC in Docket No. RM14-1-000.
- Stage 2 Standard(s) that require applicable entities to conduct assessments of the potential impact of benchmark GMD events on their systems. If the assessments identify potential impacts, the Standard(s) will require the applicable entity to develop and implement a plan to mitigate the risk.

TPL-007-1 is a new Reliability Standard to specifically address the Stage 2 directives in Order No. 779.

Large power transformers connected to the EHV transmission system can experience both winding and structural hot spot heating as a result of GMD events. TPL-007-1 will require owners of such transformers to conduct thermal analyses of their transformers to determine if the transformers will be able to withstand the thermal transient effects associated with the Benchmark GMD event. This paper discusses methods that can be employed to conduct such analyses, including example calculations.

The primary impact of GMDs on large power transformers is a result of the quasi-dc current that flows through wye-grounded transformer windings. This geomagnetically-induced current (GIC~~),~~) results in an offset of the ac sinusoidal flux resulting in asymmetric or half-cycle saturation (see **Figure 1**).

Half-cycle saturation results in a number of known effects:

- Hot spot heating of transformer windings due to harmonics and stray flux;
- Hot spot heating of non-current carrying transformer metallic members due to stray flux;
- Harmonics;
- Increase in reactive power absorption; and
- Increase in vibration and noise level.

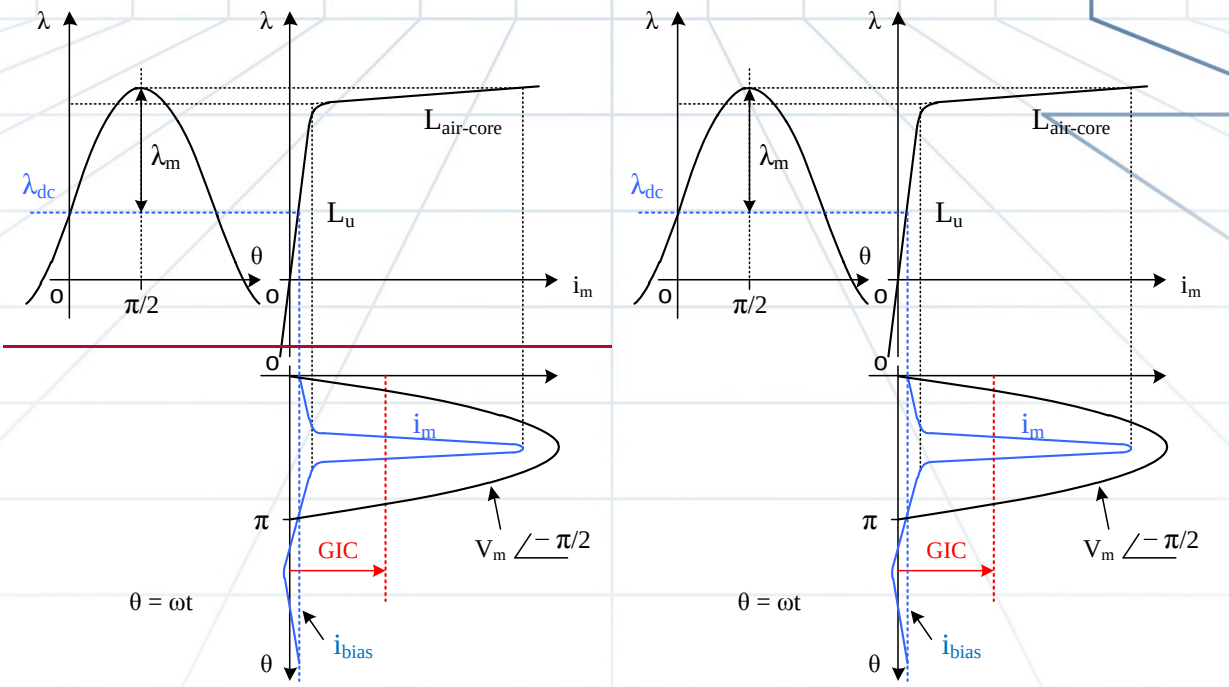


Figure 1: Mapping Magnetization Current to Flux through Core Excitation Characteristics

This paper focuses on hot spot heating of transformer windings and non current-carrying metallic parts. Effects such as the generation of harmonics, increase in reactive power absorption, vibration and noise are not within the scope of this document.

Technical Considerations

The effects of half-cycle saturation on HV and EHV transformers, namely localized "hot spot" heating, are relatively well understood, but are difficult to quantify. A transformer GMD impact assessment must consider GIC amplitude, duration, and transformer physical characteristics such as design and condition (e.g., age, gas content, and moisture in the oil). A single threshold value of GIC cannot be justified as a "pass or fail" screening criterion where "fail" means that the transformer will suffer damage. A single threshold value of GIC only makes sense in the context where "fail" means that a more detailed study is required and that "pass" means that GIC in a particular transformer is so low that a detailed study is unnecessary. Such a threshold would have to be technically justifiable and sufficiently low to be considered a conservative value within the scope of the benchmark.

The following considerations should be taken into account when assessing the thermal susceptibility of a transformer to half-cycle saturation:

- In the absence of manufacturer specific information, use the temperature limits for safe transformer operation such as those suggested in the IEEE Std. C57.91-2011 standard [1] for hot spot heating during short-term emergency operation. This standard does not suggest that exceeding these limits will result in transformer failure, but rather that it will result in additional aging of cellulose in the paper-oil insulation, and the potential for the generation of gas bubbles in the bulk oil. Thus, from the point of view of evaluating possible transformer damage due to increased hot spot heating, these thresholds can be considered conservative for a transformer in good operational condition.
- The worst case temperature rise for winding and metallic part (e.g., tie plate) heating should be estimated taking into consideration the construction characteristics of the transformer as they pertain to dc flux offset in the core (e.g., single-phase, shell, 5 and 3-leg three-phase construction).
- Bulk oil temperature due to ambient temperature and transformer loading must be added to the incremental temperature rise caused by hot spot heating. For planning purposes, maximum ambient and loading temperature should be used unless there is a technically justified reason to do otherwise.
- The time series or "waveshape" of the reference GMD event in terms of peak amplitude, duration and frequency of the geoelectric field has an important effect on hot spot heating. Winding and metallic part hot spot heating have different thermal time constants and their temperature rise will be different if the GIC currents are sustained for 2, 10, or 30 minutes for a given GIC peak amplitude.
- The "effective" GIC in autotransformers (reflecting the different GIC ampere-turns in the common and the series windings) must be used in the assessment. The effective current $I_{dc,eq}$ in an autotransformer is defined by [2]

~~$I_{dc,eq} = I_H + (I_N/3 - I_H)V_X/V_H$~~ $I_{dc,eq} = I_H + (I_N/3 - I_H)V_X/V_H$

(1)

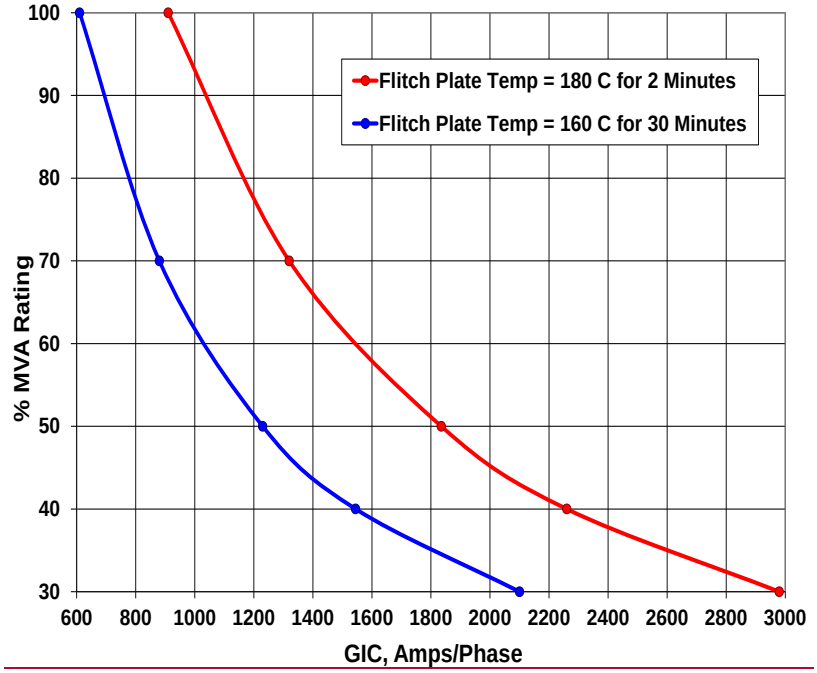
where,

I_H is the dc current in the high voltage winding;
I_N is the neutral dc current;
V_H is the rms rated voltage at HV terminals;
V_X is the rms rated voltage at the LV terminals.

Transformer Thermal Impact Assessment Process

There are two different ways to carry out a detailed thermal impact screening:

1. Transformer manufacturer GIC capability curves. These curves relate permissible peak GIC (obtained by the user from a steady-state GIC calculation) and loading for a specific transformer. An example of manufacturer capability curves is provided in **Figure 2**. Presentation details vary between manufacturers and limited information is available regarding the assumptions used to generate these curves, in particular the assumed waveshape or duration of the effective GIC. Some manufacturers assume that the waveshape of the GIC in the transformer windings is a square pulse of 2, 10, or 30 minutes in duration. In the case of the transformer capability curve shown in **Figure 2** [3], a square pulse of 900 A/phase with a duration of 2 minutes would cause the Flitch plate hot spot to reach a temperature of 180 °C at full load. While GIC capability curves are relatively simple to use, a fair amount of engineering judgment is necessary to ascertain what portion of a GIC waveshape is equivalent to, for instance, a 2 minute pulse. Also, manufacturers generally maintain that in the absence of transformer standards defining thermal duty due to GIC, such capability curves have to be developed for every transformer design and vintage.



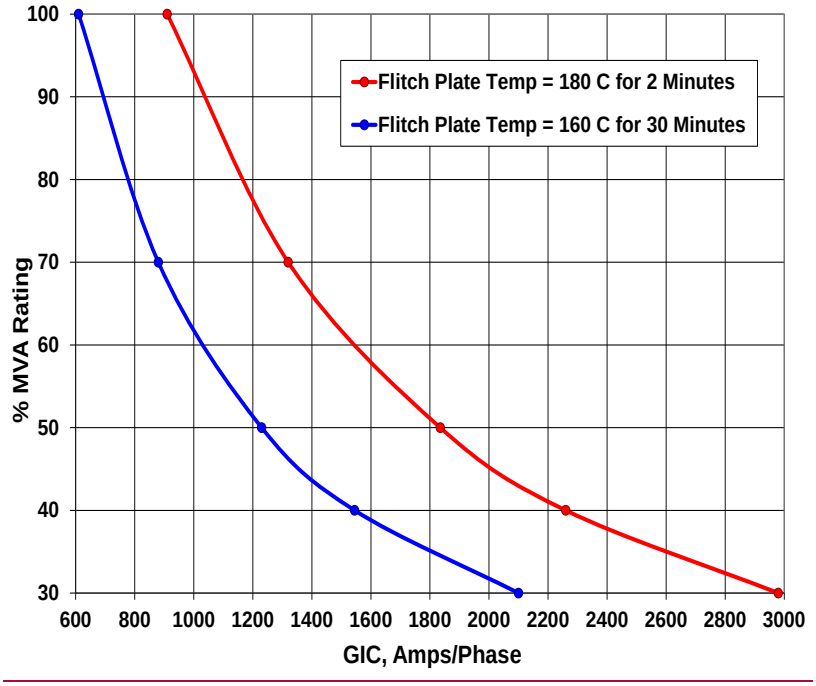


Figure 2: Sample GIC ~~manufacturer capability curve~~Manufacturer Capability Curve of a ~~large single-phase transformer design~~Large Single-Phase Transformer Design using the Flitch ~~plate temperature criteria~~Plate Temperature Criteria [3]

2. Thermal response simulation[1]. The input to this type of simulation is the time series or waveshape of effective GIC flowing through a transformer (taking into account the actual configuration of the system) and the result of the simulation is the hot spot temperature (winding or metallic part) time sequence for a given transformer. An example of GIC input and hotspot temperature time series values from [4] are shown in **Figure 3**. The hot spot thermal transfer functions can be obtained from measurements or calculations provided by transformer manufacturers. ~~Default~~Conservative default values can be used (e.g. those provided in [4]) when specific data are not available. Hot spot temperature thresholds shown in **Figure 3** are consistent with IEEE Std. C57.91 emergency loading hot spot limits. Emergency loading time limit is usually 30 minutes.

[1] Technical details of this methodology can be found in [4].

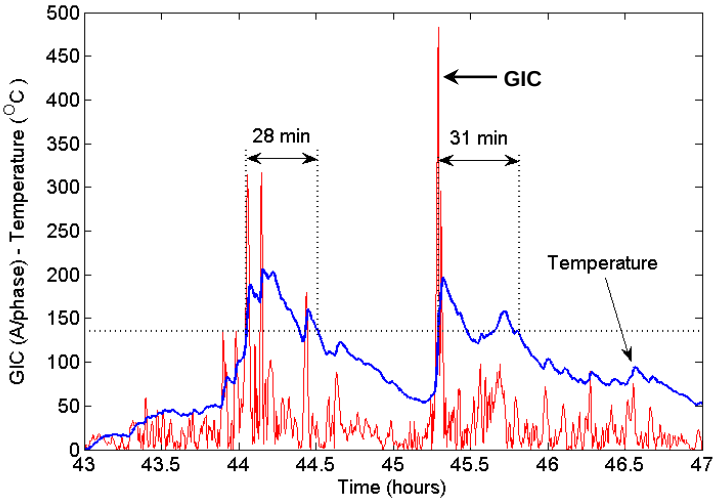


Figure 3: Sample Tie Plate Temperature Calculation

Blue trace is incremental temperature and red trace is the magnitude of the GIC/phase [4]

It is important to reiterate that the characteristics of the time sequence or "waveshape" are very important in the assessment of the thermal impact of GIC on transformers. Transformer hot spot heating is not instantaneous. The thermal time constants of transformer windings and metallic parts are typically on the order of minutes to tens of minutes; therefore, hot spot temperatures are heavily dependent on GIC history and rise time, amplitude and duration of GIC in the transformer windings, bulk oil temperature due to loading, ambient temperature and cooling mode.

Calculation of the GIC ~~w~~Waveshape for a ~~t~~Transformer

The following procedure can be used to generate time series GIC data, i.e. GIC(t), using a software program capable of computing GIC in the steady-state. The steps are as follows:

1. Calculate contribution of GIC due to eastward and northward geoelectric fields for the transformer under consideration;
2. Scale the GIC contribution according to the reference geoelectric field time series to produce the GIC time series for the transformer under consideration.

Most available GIC–capable software packages can calculate GIC in steady-state in a transformer assuming a uniform ~~E~~eastward geoelectric field of 1 V/km (GIC_E) while the ~~N~~northward geoelectric field is zero. Similarly, GIC_N can be obtained ~~when~~for a uniform ~~N~~northward geoelectric field of 1 V/km while the ~~E~~eastward geoelectric field is zero. GIC_E and GIC_N are the normalized GIC contributions for the transformer under consideration.

If the earth conductivity is assumed to be uniform (or laterally uniform) in the transmission system of interest, then the transformer GIC (in A/phase/V/km) for any value of E_E (t) and E_N(t) can be calculated using (2) [2].

~~$$GIC(t) = |E(t)| \cdot \{GIC_E \sin(\varphi(t)) + GIC_N \cos(\varphi(t))\}$$~~

$$GIC(t) = |E(t)| \cdot \{GIC_E \sin(\varphi(t)) + GIC_N \cos(\varphi(t))\} \quad (2)$$

where

~~$$|E(t)| = \sqrt{E_N^2(t) + E_E^2(t)}$$~~ $$|E(t)| = \sqrt{E_N^2(t) + E_E^2(t)} \quad (3)$$

~~$$\varphi(t) = \tan^{-1}\left(\frac{E_E(t)}{E_N(t)}\right)$$~~ $$\varphi(t) = \tan^{-1}\left(\frac{E_E(t)}{E_N(t)}\right) \quad (4)$$

$$GIC(t) = E_E(t) \cdot GIC_E + E_N(t) \cdot GIC_N \quad (5)$$

GIC_N is the effective GIC due to a ~~N~~northward geoelectric field of 1 V/km and GIC_E is the effective GIC due to an ~~E~~eastward geoelectric field of 1 V/km.

The geoelectric field time series $E_N(t)$ and $E_E(t)$ is obtained, for instance, from the reference geomagnetic field time series [5] after the appropriate geomagnetic latitude ~~factor α is applied[2]. Applying (2~~scaling factor α is applied[3]. The reference geoelectric field time series is calculated using the reference earth model. When using this geoelectric field time series where a different earth model is applicable, it should be scaled with the conductivity scaling factor β[4]. Alternatively the geoelectric field can be calculated from the reference geomagnetic field time series after the appropriate geomagnetic latitude scaling factor α is applied and the appropriate earth model is used. In such case, the conductivity scaling factor β is not applied because it is already taken into account by the use of the appropriate earth model.

~~[2] The geomagnetic factor α is described in [2] and is used to scale the geomagnetic field according to geomagnetic latitude. The lower the geomagnetic latitude (closer to the equator) the lower the amplitude of the geomagnetic field.~~

[3] The geomagnetic factor α is described in [2] and is used to scale the geomagnetic field according to geomagnetic latitude. The lower the geomagnetic latitude (closer to the equator) the lower the amplitude of the geomagnetic field.

[4] The conductivity scaling factor β is described in [2] and is used to scale the geoelectric field according to the conductivity of different physiographic regions. Lower conductivity results in higher β scaling factors.

Applying (5) to each point in $E_N(t)$ and $E_E(t)$ results in GIC(t).

GIC(t) Calculation Example

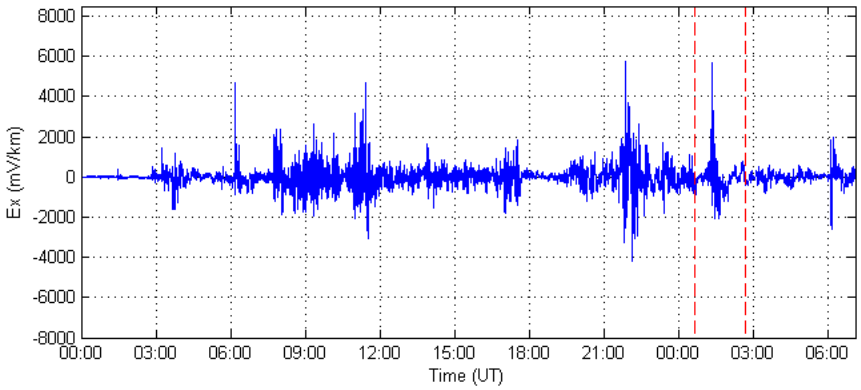
Let us assume that from the steady-state solution, the effective GIC in this transformer is GIC_E = -~~6A~~20 A/phase if E_N=0, E_E=1 V/km and GIC_N = ~~9.6A~~26 A/phase if E_N=1 V/km, E_E=0. Let us also assume the geomagnetic field time series corresponds to a geomagnetic latitude where α = 1 and that the earth conductivity corresponds to the reference earth model in [5]. The resulting geoelectric field time series is shown in **Figure 4**. Therefore,

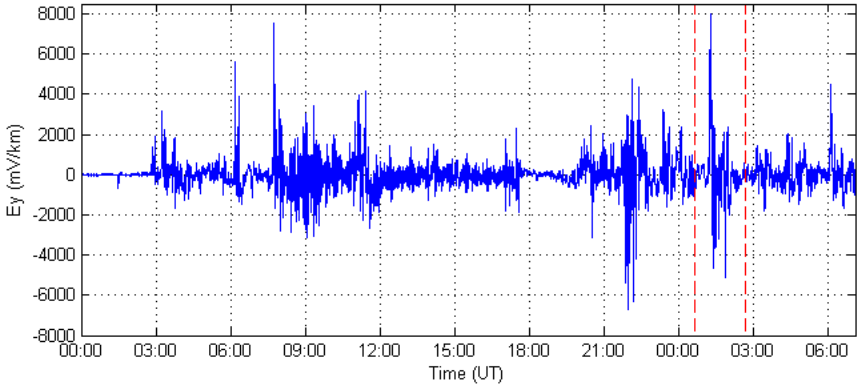
$$GIC(t) = E_E(t) \cdot GIC_E + E_N(t) \cdot GIC_N \text{ (A/phase)}$$

$$GIC(t) = -E_E(t) \cdot 20 + \cdot E_N(t) \cdot 26 \text{ (A/phase)}$$

The resulting GIC waveshape GIC(t) is shown in **Figures 5 and 6** and can subsequently be used for thermal analysis.

It should be emphasized that even for the same reference event, the GIC(t) waveshape in every transformer will be different, depending on the location within the system and the number and orientation of the circuits connecting to the transformer station. Assuming a single generic GIC(t) waveshape to test all transformers is incorrect.


8000
6000
4000
2000
0
-2000
-4000
-6000
-8000
Ex (mV/km)
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
00:00
03:00
06:00
Time (UT)


8000
6000
4000
2000
0
-2000
-4000
-6000
-8000
Ey (mV/km)
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
00:00
03:00
06:00
Time (UT)

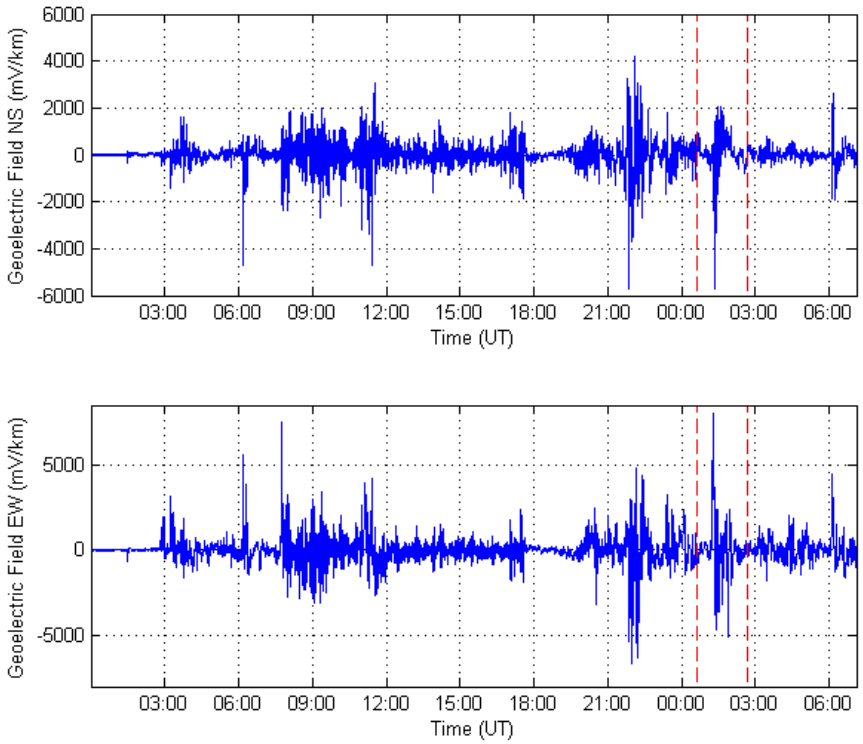


Figure 4: Calculated ~~geoelectric field~~Geoelectric Field $E_N(t)$ and $E_E(t)$ ~~a~~Assuming $\alpha=1$ and $\beta=1$ (Reference Earth Model~~)~~). Zoom area for subsequent graphs is highlighted. Dashed lines approximately show the close-up area for subsequent Figures.

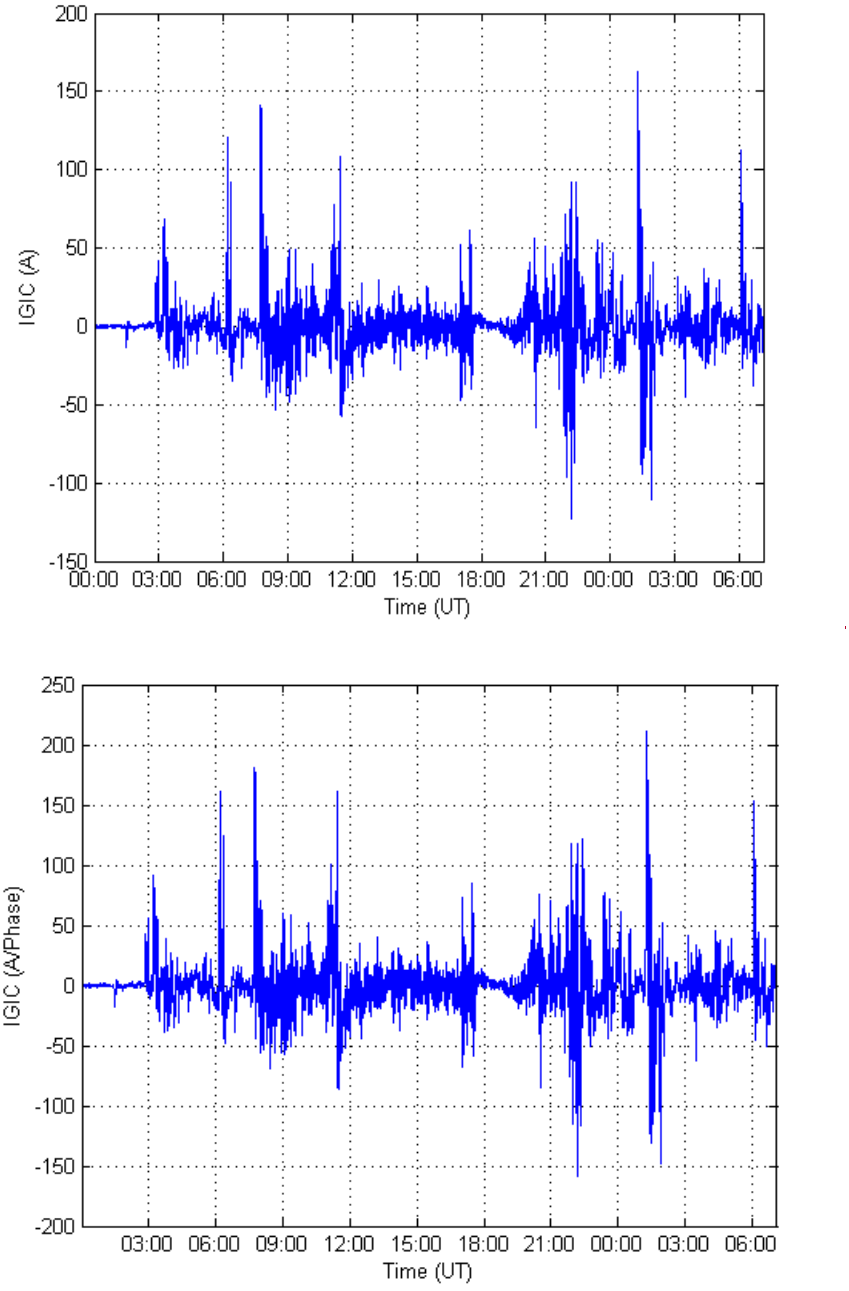


Figure 5: Calculated GIC(t) Assuming $\alpha=1$ and $\beta=1$ (Reference Earth Model)

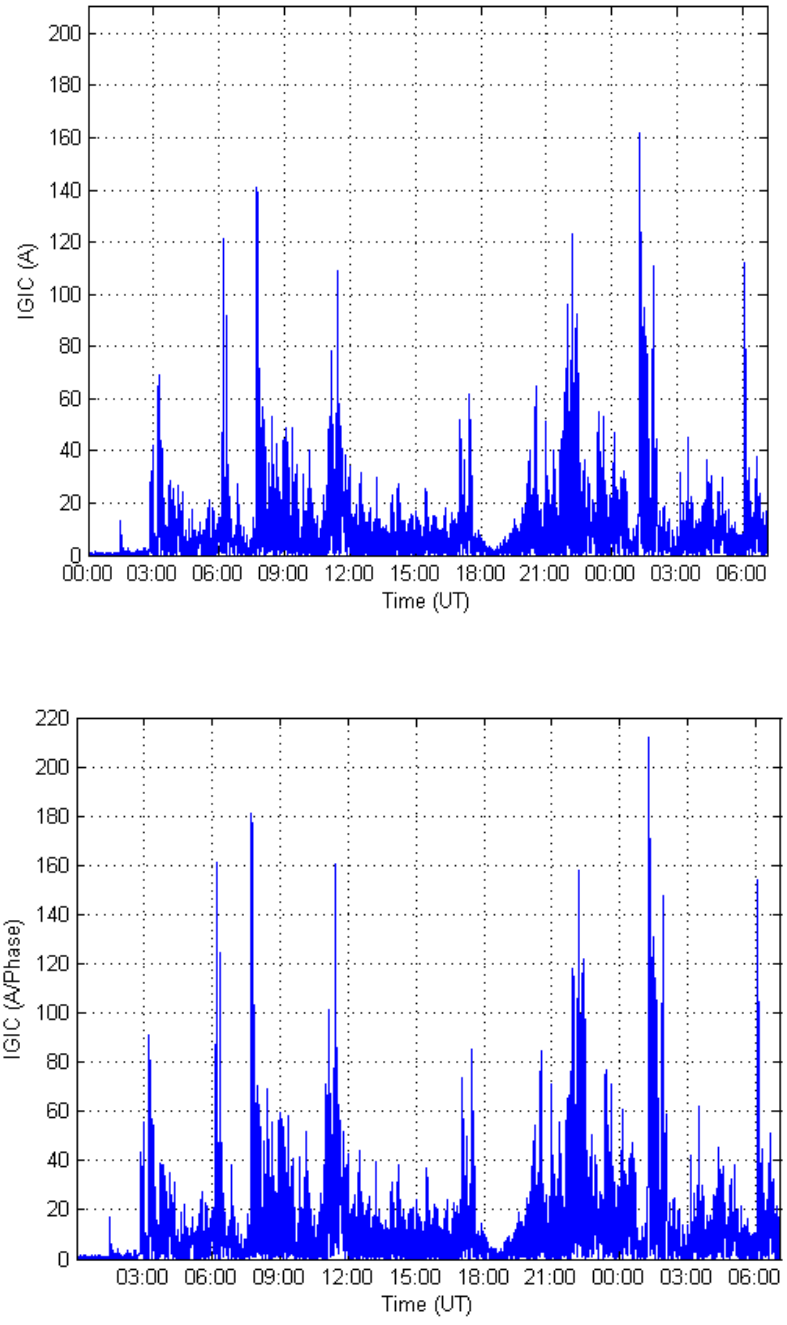


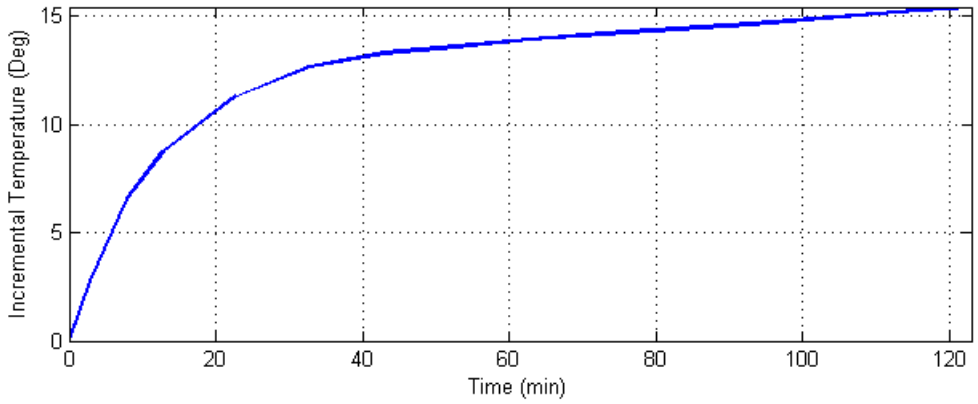
Figure 6: Calculated Magnitude of GIC(t) Assuming α=1 and β=1 (Reference Earth Model)

Transformer Thermal Assessment Examples

There are two basic ways to carry out a transformer thermal analysis once the GIC time series GIC(t) is known for a given transformer: 1) ~~using manufacturer's capability curves, and 2)~~ calculating the thermal response as a function of time; and 2) using manufacturer's capability curves.

Example 1: ~~Using~~Calculating the thermal response as a function of time using a thermal response tool

The thermal step response of the transformer can be obtained for both winding and metallic part hot spots from: ~~(a~~1) measurements; ~~(b~~2) manufacturer's calculations; or ~~(c~~3) generic published values. **Figure 7** shows the measured metallic hot spot thermal response to a dc step of 16.67 A/phase of the top yoke clamp from [~~4~~6] that will be used in this example. **Figure 8** shows the ~~estimated~~measured incremental temperature rise (asymptotic response) of the same hot spot to long duration GIC steps.[5] ~~The asymptotic response in **Figure 8** is extrapolated linearly from relatively low magnitude dc measurements. This is a conservative approximation for illustration purposes. In the Fingrid transformer tests reported in 2002 [6], the measured maximum value of the asymptotic response of the inside of the yoke clamp (highest hot spot temperature) is 15% lower than the value obtained using linear extrapolation. The linear extrapolation results in a calculated temperature peak 9% higher than the measured asymptotic behavior when the GIC(t) time series in **Figure 6** is used.~~



[5] The heating of the bulk oil due to the hot spot temperature increase is not included in the asymptotic response because the time constant of bulk oil heating is at least an order of magnitude larger than the time constants of hot spot heating.

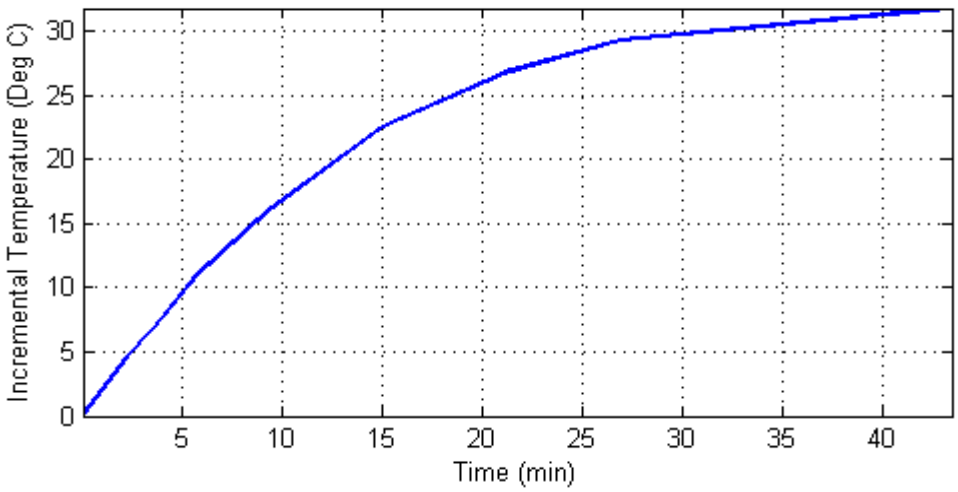
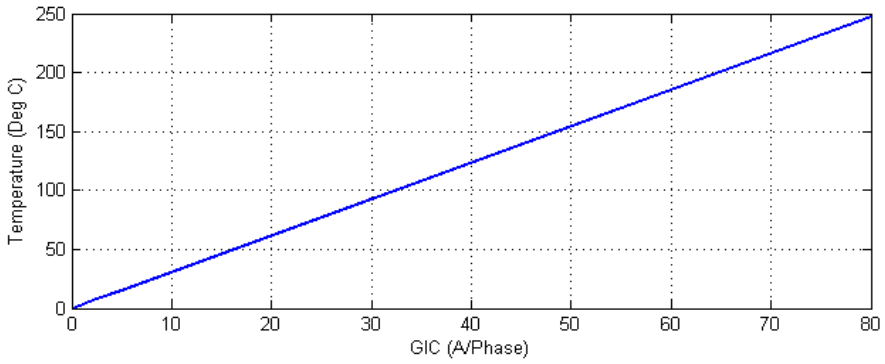


Figure 7: Thermal Step Response to a ~~5 A/phase~~ 16.67 Amperes per Phase dc Step ~~[3]~~

Metallic hot spot heating.



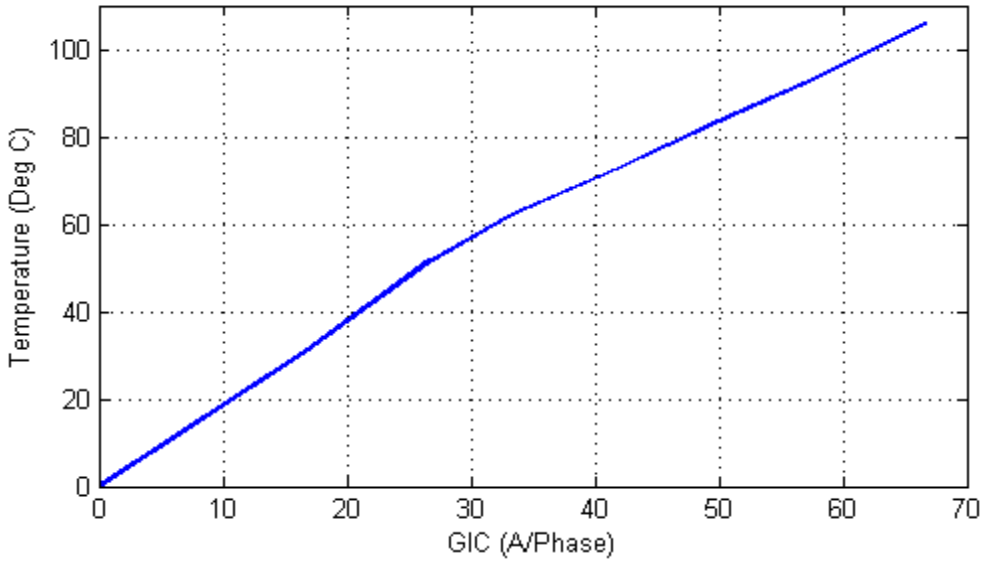


Figure 8: Asymptotic Thermal Step Response ~~[4]~~
Metallic hot spot heating.

In order to obtain the thermal response of the transformer to a GIC waveshape such as the one in **Figure 6**, a thermal response model is required. To create a thermal response model, the measured or manufacturer-calculated transformer thermal step responses (winding and metallic part) for various GIC levels are required. The GIC(t) time series or waveshape is then applied to the thermal model to obtain the incremental temperature rise as a function of time $\theta(t)$ for the GIC(t) waveshape. The total temperature is calculated by adding the oil temperature, for example, at full load.

Figure 9 shows the calculated GIC(t) and the corresponding hot spot temperature time series $\theta(t)$. **Figure 10** shows a close-up of the peak transformer temperatures calculated in this example.

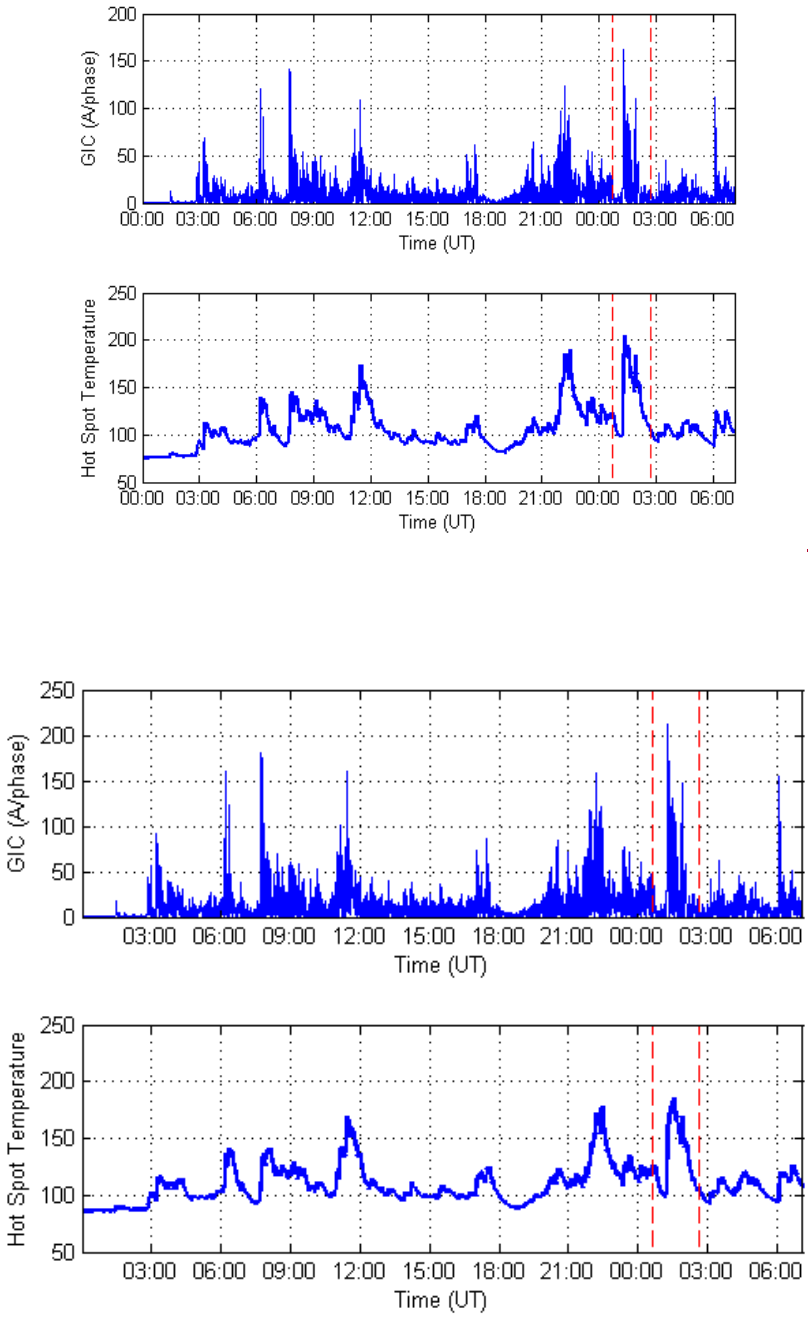


Figure 9: Magnitude of GIC(t) and ~~metallic hot spot temperature~~Metallic Hot Spot Temperature θ(t) ~~assuming full load oil temperature~~Assuming Full Load Oil Temperature of ~~75~~85.3°C (~~30~~40°C ambient~~)~~). Dashed lines approximately show the close-up area for subsequent Figures.

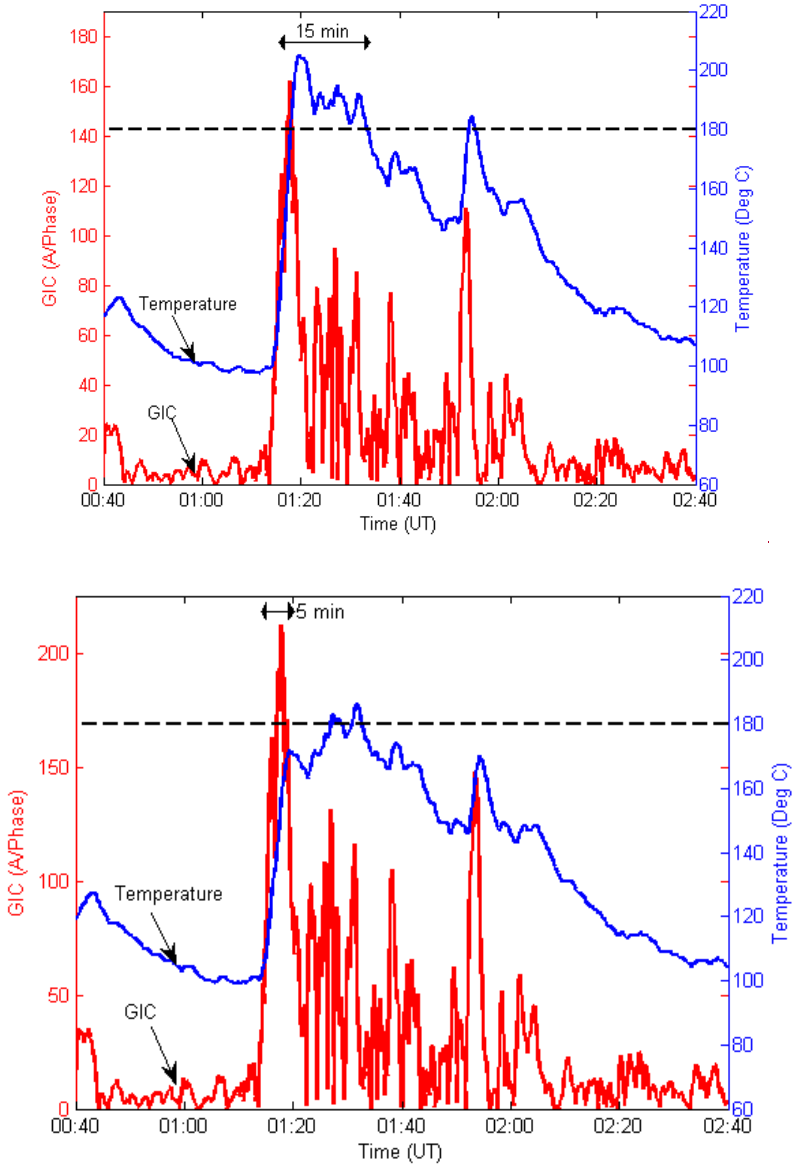


Figure 10: Close-up of Metallic ~~hot spot temperature~~ Hot Spot Temperature Assuming a Full Load

(Blue trace is θ(t~~) assuming a full load (blue trace)~~). Red trace is GIC(t~~)~~))

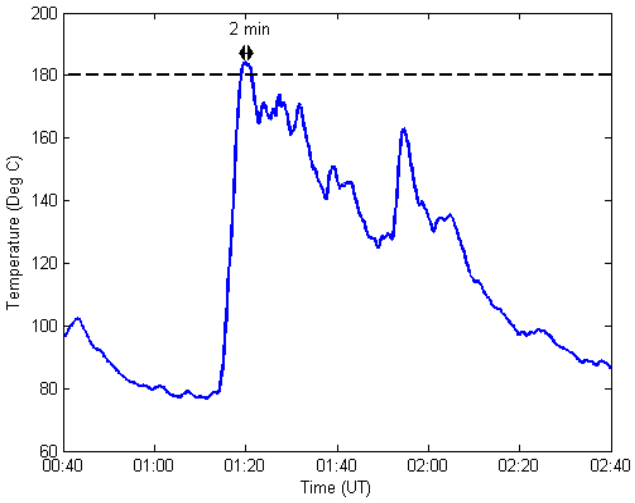
In this example the IEEE Std. C57.91 emergency loading hot spot threshold of 200°C for metallic hot spot heating is not exceeded ~~for 3 minutes (as opposed to 30 minutes for emergency overloading).~~ . Peak

temperature is ~~204~~186°C. The IEEE standard is silent as to whether the temperature can be higher than 200°C for less than 30 minutes. Manufacturers can provide guidance on individual transformer capability.

It is not unusual to use a lower temperature threshold of 180°C to account for calculation and data margins as well as transformer age and condition. **Figure 10** shows that 180°C will be exceeded for ~~15~~5 minutes.

At ~~70~~75% loading, the initial temperature is ~~54.5~~64.6 °C rather than ~~75~~85.3 °C and the hot spot temperature peak is ~~183~~165°C~~. In this case~~, well below the 180°C threshold ~~is~~(see **Figure 11**).

If a conservative threshold of 160°C were to be used to take into account the age and condition of the transformer, then the full load limits would exceeded for ~~2~~approximately 22 minutes~~ (see **Figure 11**).~~.



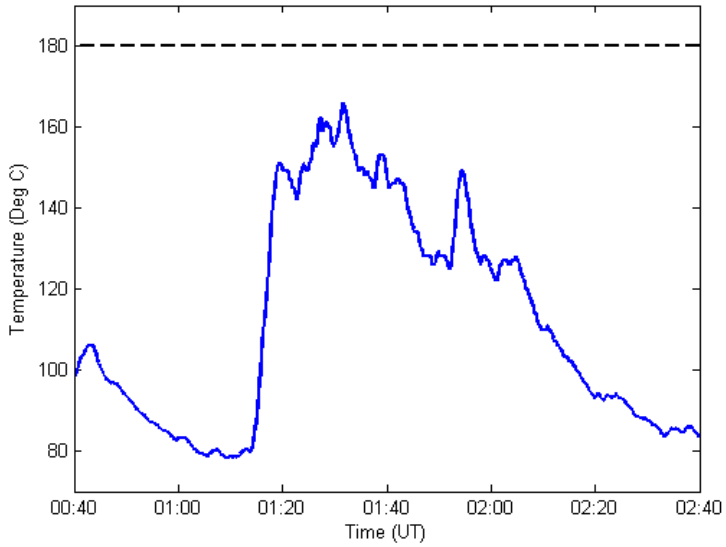


Figure 11: Close-up of Metallic ~~hot spot temperature assuming a 70% load~~ Hot Spot Temperature Assuming a 75% Load
(Oil temperature of ~~54~~64.5°C)

Example 2: Using a ~~manufacturer's capability curves~~Manufacturer's Capability Curves

The capability curves used in this example are shown in **Figure 12**. To be consistent with the previous example, these particular capability curves have been reconstructed from the thermal step response shown in **Figures 8** and **9**, and the simplified loading curve shown in **Figure 14** (calculated using formulas from IEEE Std. C57.91).

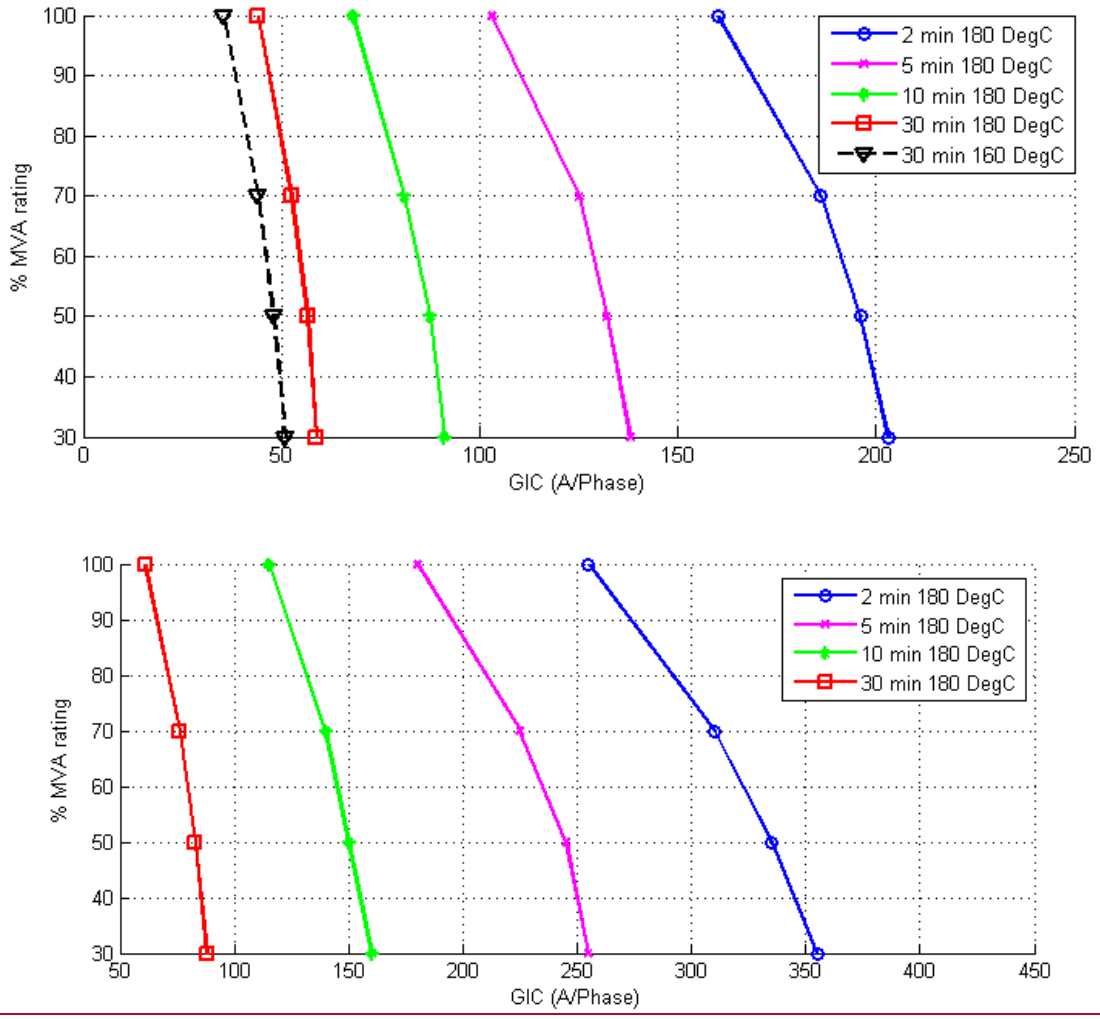
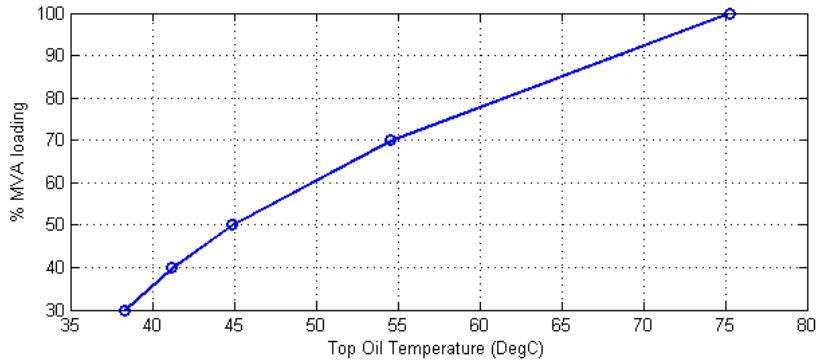


Figure 12: Capability ~~c~~Curve of a ~~transformer based~~Transformer Based on the ~~thermal response shown~~Thermal Response Shown in Figures 8 and 9~~.~~.



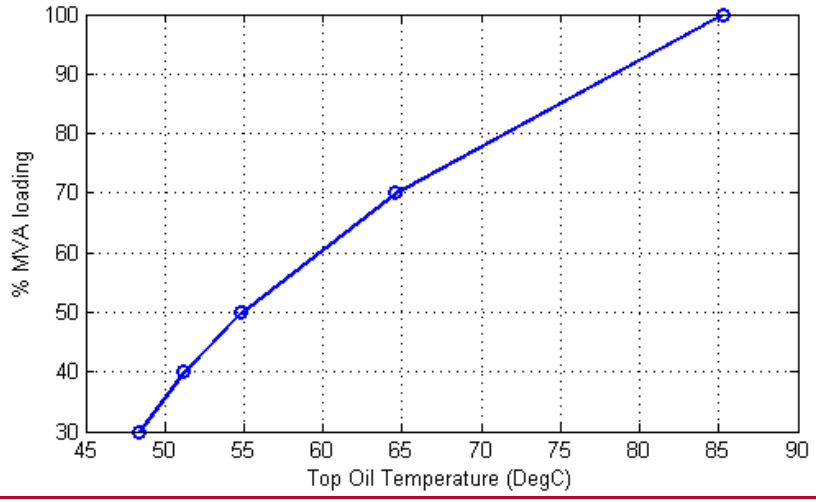
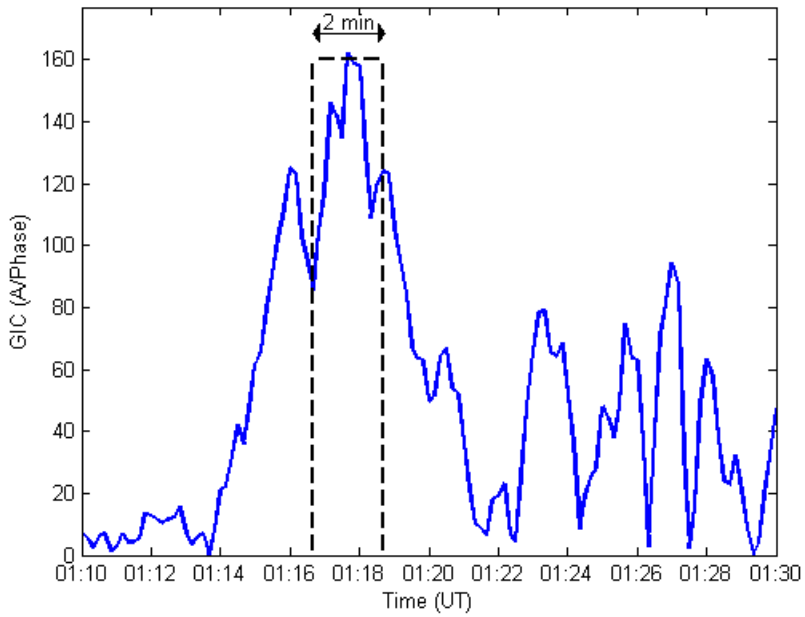


Figure 13: Simplified ~~loading curve assuming 30~~Loading Curve Assuming 40°C ~~ambient temperature~~Ambient Temperature.

The basic notion behind the use of capability curves is to compare the calculated GIC in a transformer with the limits at different GIC pulse widths. A narrow GIC pulse has a higher limit than a longer duration or wider one. If the calculated GIC and assumed pulse width falls below the appropriate pulse width curve then the transformer is within its capability.

To use these curves it is necessary to estimate an equivalent square pulse that matches the waveshape of GIC(t), generally at a GIC(t) peak. **Figure 14** shows a close-up of the GIC near its highest peak superimposed to a ~~160 A/~~255 Amperes per phase, 2 minute pulse at 100% loading from **Figure 12**. Since a narrow 2-minute pulse is not representative of GIC(t) in this case, a 5 minute pulse with an amplitude of 1803 A/phase at 100% loading has been superimposed on **Figure 15**. It should be noted that a ~~160~~255 A/phase, 2 minute pulse is equivalent to a ~~103A~~180 A/phase 5 minute pulse from the point of view of transformer capability. Deciding what GIC pulse is equivalent to the portion of GIC(t) under consideration is a matter of engineering judgment.



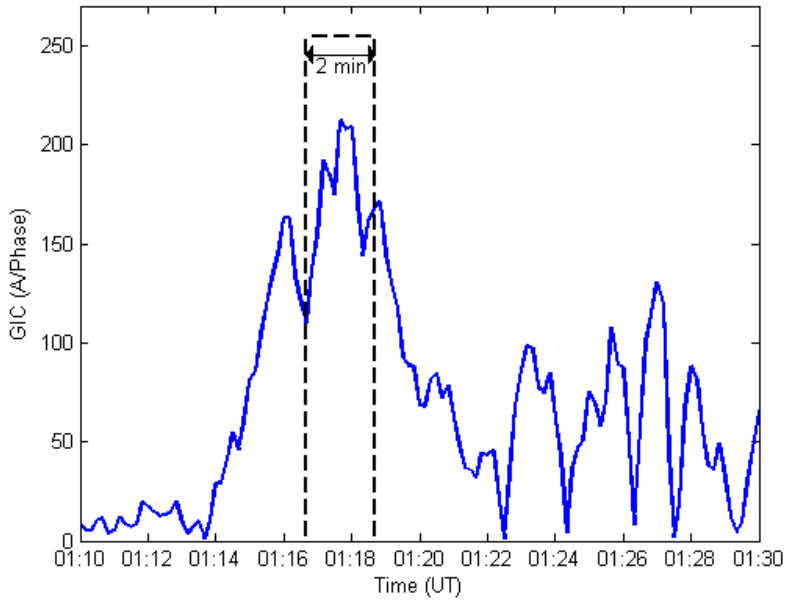


Figure 14: Close-up of GIC(t) and a 2 minute 255 A/phase GIC pulse at full load

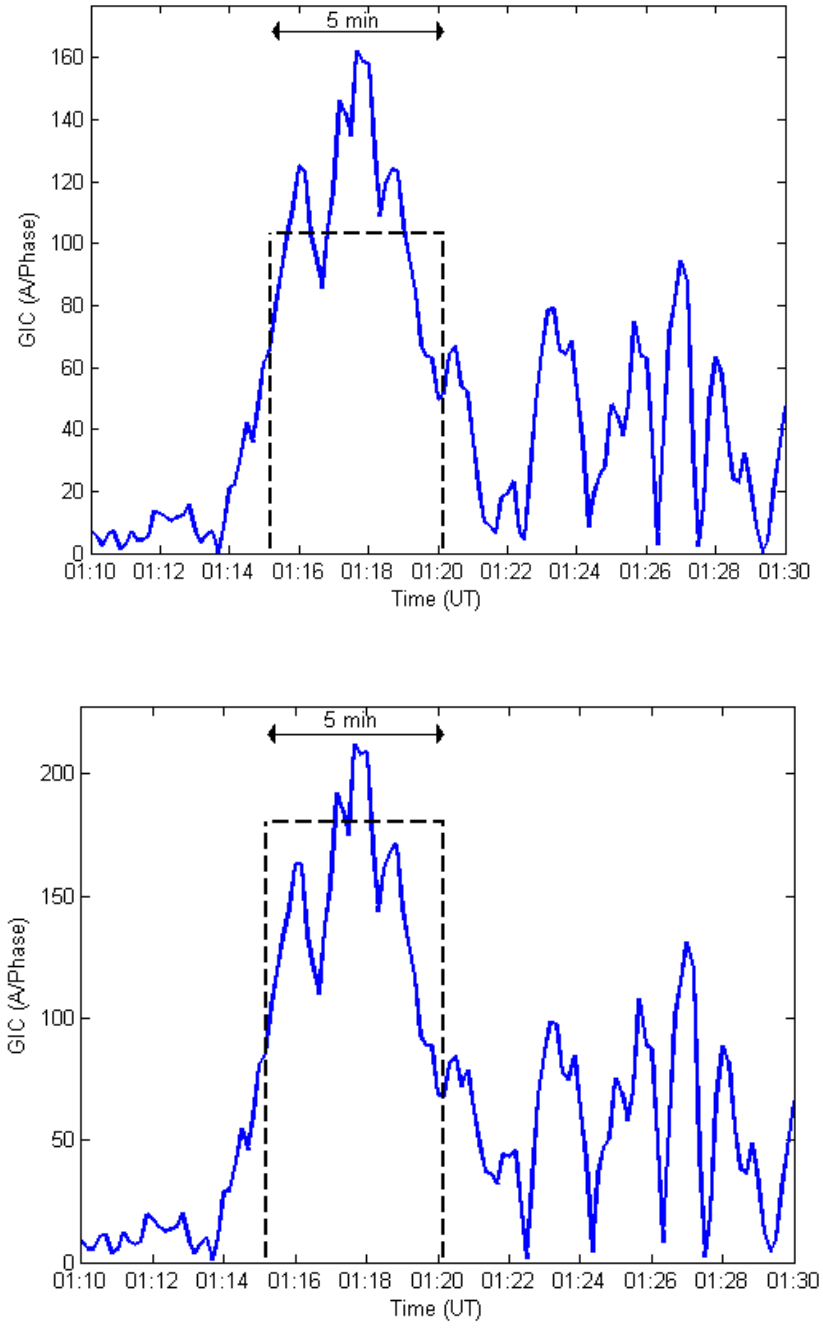
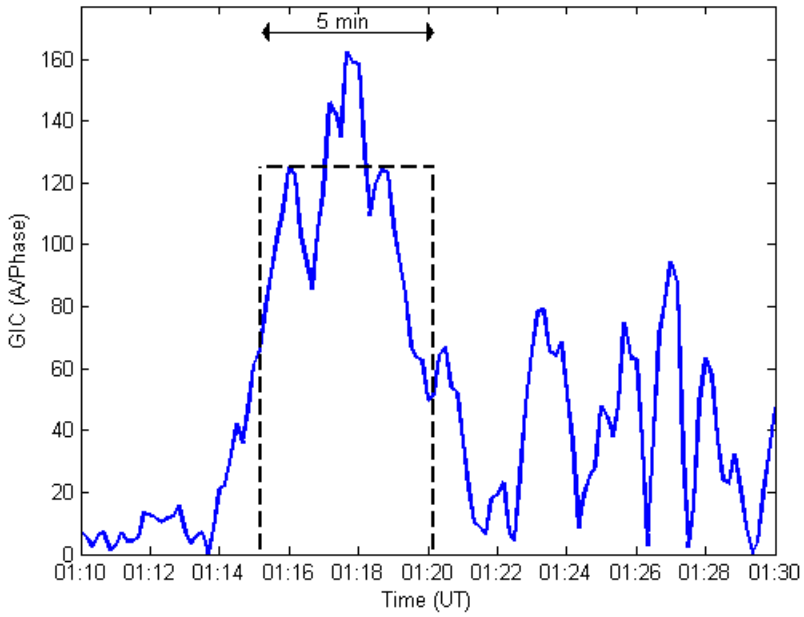


Figure 15: Close-up of GIC(t) and a ~~5 minute~~Five Minute 180 A/phase GIC ~~p~~Pulse at ~~full load~~Full Load

When using a capability curve it should be understood that the curve is derived assuming that there is no hot spot heating due to prior GIC at the time the GIC pulse occurs (only an initial temperature due to loading). Therefore, in addition to estimating the equivalent pulse that matches GIC(t), allowances have to

be made in terms of prior hot spot heating. From these considerations it is ~~apparent that~~unclear whether the capability curves would be exceeded at full load with a 180 °C threshold in this example.

At 70% loading, the two and five minute pulses from **Figure 12** would have amplitudes of ~~186~~310 and ~~1~~225 A/phase, respectively. The 5 minute pulse is illustrated in **Figure 16**. In this case, ~~it~~judgment is ~~not easy~~also required to assess if the GIC(t) is within the capability curve for 70% loading. In general, capability curves are easier to use when GIC(t) is substantially above or clearly below the GIC thresholds for a given pulse duration.



If a conservative threshold of 160°C were to be used to take into account the age and condition of the transformer, then a new set of capability curves would be required.

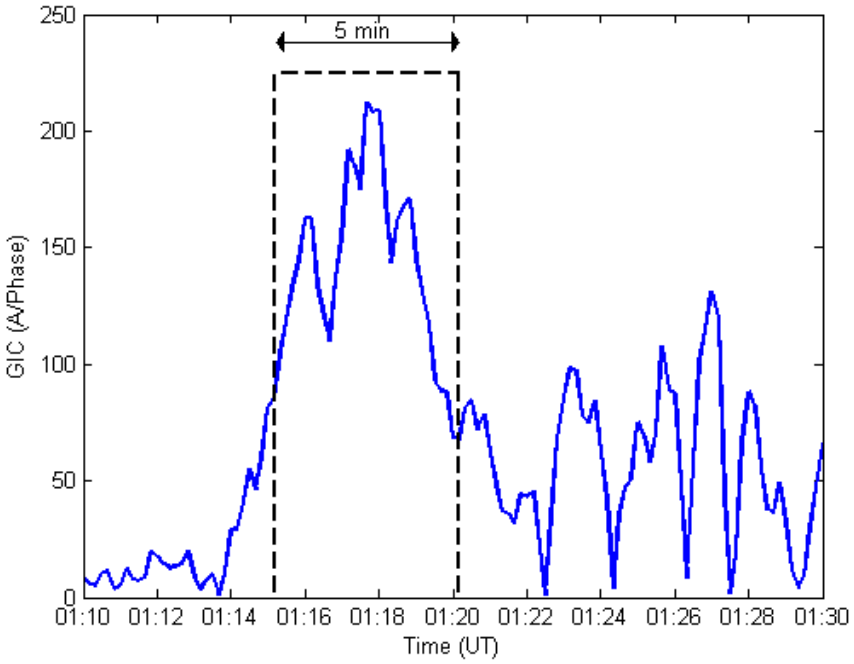


Figure 16: Close-up of GIC(t) and a 5 ~~minute~~Minute 225 A/phase GIC ~~pulse assuming 70% load~~Pulse Assuming 75% Load

References

[1] "IEEE Guide for loading mineral-oil-immersed transformers and step-voltage regulators." IEEE Std C57.91-2011 (Revision of IEEE Std C57.91-1995).

[2] Application Guide: Computing Geomagnetically-Induced Current in the Bulk-Power System, NERC. Available at: http://www.nerc.com/comm/PC/Geomagnetic%20Disturbance%20Task%20Force%20GMDTF%202013/GIC%20Application%20Guide%202013_approved.pdf

[3] Girgis, R.; Vedante, K. "Methodology for evaluating the impact of GIC and GIC capability of power transformer designs." IEEE PES 2013 General Meeting Proceedings. Vancouver, Canada.

[4] Marti, L., Rezaei-Zare, A., Narang, A. "Simulation of Transformer Hotspot Heating due to Geomagnetically Induced Currents." IEEE Transactions on Power Delivery, vol.28, no.1. pp 320-327. January 2013.

[5] Benchmark Geomagnetic Disturbance Event Description white paper. Developed by the Project 2013-03 (Geomagnetic Disturbance) standard drafting team. Available at:

http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx

[6] Lahtinen, Matti. Jarmo Elovaara. "GIC occurrences and GIC test for 400 kV system transformer". IEEE Transactions on Power Delivery, Vol. 17, No. 2. April 2002.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

State of Reliability 2014

May 2014

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

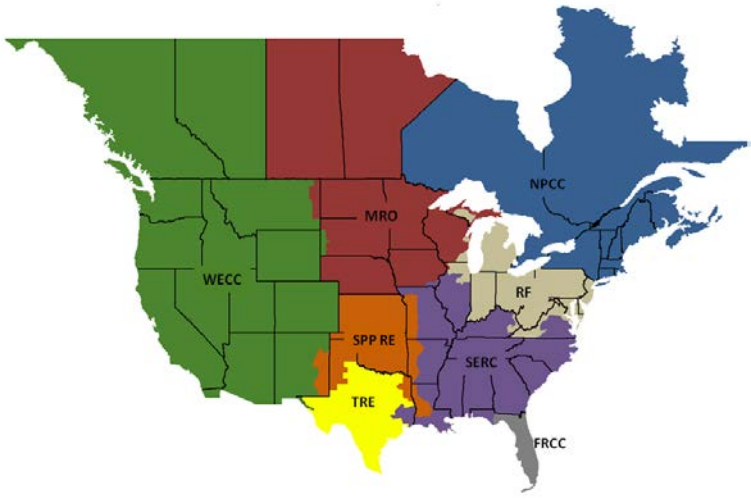
Preface 3
Executive Summary 5
Chapter 1 – Key Findings and Conclusions 10
Chapter 2 – Daily Performance Severity Risk Assessment 23
Chapter 3 – Risk Issue Identification and Transmission Severity Analysis 29
Chapter 4 – Reliability Indicator Trends 41
Chapter 5 – Event Analysis 60
Chapter 6 – Spare Equipment Database Initiative (2014) 71
Appendix A – Statistical Analysis for Chapter 3 73
Appendix B – Statistical Analysis for ALR1-12 Metric 91
Appendix C – Statistical Summary of SRI_{bps} Assessment 101
Appendix D – Abbreviations Used in This Report 104
Contributions 105

Preface

The North American Electric Reliability Corporation (NERC) prepared this assessment in accordance with the Energy Policy Act of 2005, in which the United States Congress directed NERC to conduct periodic assessments of the reliability and adequacy of the bulk power system (BPS) of North America.[1, 2]

NERC is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the BPS[3] in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into several assessment areas within the eight Regional Entity (RE) boundaries, as shown in the map and corresponding table below.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP-RE	Southwest Power Pool Regional Entity
TRE	Texas Reliability Entity
WECC	Western Electric Coordinating Council

[1] H.R. 6 as approved by the One Hundred Ninth Congress of the United States, the Energy Policy Act of 2005: http://www.gpo.gov/fdsys/pkg/BILLS-109hr6enr/pdf/BILLS-109hr6enr.pdf.

[2] The NERC Rules of Procedure, Section 800, further detail the objectives, scope, data and information requirements, and reliability assessment process requiring annual, seasonal, and long-term reliability assessments.

[3] http://www.nerc.com/files/glossary_of_terms.pdf, BPS definition, page 21.

Notice

This report presents metrics and trends derived from the data available at the time of publication and may be modified pending further review and analysis.

Executive Summary

The *State of Reliability 2014* report represents NERC's independent view of ongoing BPS trends to objectively provide an integrated view of reliability performance. The key findings and recommendations serve as technical input to NERC's risk assessment, Reliability Standards project prioritization, compliance process improvement, event analysis, reliability assessment, and critical infrastructure protection. The analysis of BPS performance developed as part of this report provides an industry reference of historical reliability, offers analytical insights regarding industry action, and enables the identification and prioritization of specific steps that can be taken to manage risks to reliability.

Sustained High Performance for Bulk Power System Reliability

The daily severity risk index (SRI_{bps})[4] value, which measures risk impact or "stress" from events resulting in the loss of transmission, generation, and load, has been stable to improving from 2008 to 2013. Including weather-initiated events, 2013 had no high-stress days (i.e., there were no days with an SRI_{bps} greater than 5.0). On average, the SRI_{bps} was approximately as good as the performance achieved during 2008, which is the best year on record. From 2008 through 2013, the majority of high-stress days (days with high SRI_{bps} scores) were weather-initiated or weather-exacerbated; only a small number of days were associated with initiating events internal to the BPS.

The availability of the bulk transmission system remained high from 2008 to 2013. The ac transmission circuit availability remained above 97 percent, and transmission transformer availability was above 98 percent for the 2010 to 2013 period (unavailability includes both forced and planned outages). High transmission availability demonstrates that the BPS is able to perform reliably over a variety of operating conditions.

NERC continues activity on several projects to maintain the availability and resiliency of the BPS. For example, several standards projects were completed in 2013 that support sustained high performance of BPS reliability by providing the data necessary for bulk transmission system analysis: 1) the Modeling Data standards[5] provide a foundational framework for consistent data requirements and reporting procedures needed to develop planning horizon simulation models that are critical supporting the analysis of the reliability of the interconnected BPS; 2) the Demand Data standard[6] provides authority for applicable entities to collect demand, energy, and related data to support reliability studies and assessments, measuring whether there is an adequate amount of resources available to serve peak demand while also maintaining a sufficient margin to address operating events; and 3) the ATC standard[7] requires the determination of available transmission system capability and specifies that the methods and data underlying those determinations must be disclosed to those registered entities that need the information for reliability purposes.

Frequency Response Remains Stable

From 2009 to 2013, the Eastern Interconnection, ERCOT Interconnection, Québec Interconnection[8] and the Western Interconnection have shown steady frequency response performance, trending above the recommended interconnection frequency response obligation (IFRO) at all times during the study period. The Eastern Interconnection data showed a slightly downward trend in frequency response; however, this trend is not statistically significant. It is important to continue to monitor these trends to determine whether they approach or drop below the IRFO for any interconnection. The study methods and statistical results of the frequency response evaluation are summarized in Chapter 4 (ALR1-12) and detailed in Appendix B.

[4] SRI Enhancement Whitepaper, April 9, 2014, http://www.nerc.com/comm/PC/Performance Analysis Subcommittee PAS 2013/SRI Enhancement Whitepaper.pdf
[5] Modeling Data (MOD B), http://www.nerc.com/pa/Stand/Pages/Project2010-03ModelingData(MOD-B).aspx
[6] MOD-031-1, Demand Data (MOD C), http://www.nerc.com/pa/Stand/Pages/Project2010-04DemandData(MOD-C).aspx
[7] ATC Revisions (MOD A), http://www.nerc.com/pa/Stand/Pages/Project201205MODAAvailableTransferCapability.aspx
[8] Only Québec Interconnection 2011 and 2013 frequency response data is available.

Several projects are ongoing at NERC to monitor and maintain frequency response. For example, NERC completed the development of BAL-003-1 in 2013, and FERC approved the standard on January 16, 2014. BAL-003-1 establishes a minimum frequency response obligation for each Balancing Authority (BA), provides a uniform calculation of frequency response and frequency bias settings that transition to values closer to natural frequency response, and encourages coordinated Automatic Generation Control operation. This standard, in partnership with BAL-001-2, maintains interconnection steady-state frequency within defined limits by balancing real power demand and supply in real time, ensuring that BAs take actions to maintain interconnection frequency and that they each contribute their fair share to frequency control. NERC also completed development of BAL-001-2 in 2013, which is pending regulatory approval.

RECOMMENDATION:
EXAMINE INCIDENTS IN 2013 WHERE FREQUENCY RESPONSE WAS LESS THAN IFRO. DETERMINE ACTIONS TO MAINTAIN AND IMPROVE FREQUENCY RESPONSE PERFORMANCE.

Protection System Misoperations Cause Transmission Events

Similar to the key finding in the *State of Reliability 2013* report, protection system misoperations continued to be a significant contributor to automatic transmission outage severity in 2013, as shown in Chapter 3. On average, transmission system events with protection system misoperations were more impactful than other transmission events. They were also, in aggregate, a significant contributor to transmission outage severity, indicating that a reduction in protection system misoperations would lead to an improvement in system reliability.

Protection system misoperations continues to be an area of NERC concentration. The Reliability Issues Steering Committee (RISC) has identified system protection reliability, uncoordinated protection systems, and protection system misoperations as top-priority risks to reliability. NERC has focused its Reliability Standards efforts in these areas, with the completion of the relay loadability standards[9] and continued work on relay misoperations[10] and coordination.[11] In addition, NERC staff is coordinating with the North American Transmission Forum to find ways to reduce protection system misoperations and develop ways to minimize their impact. NERC's Event Analysis activities continue to examine system events to identify actions needed to address protection system trends and common causes of misoperations.

RECOMMENDATION:
COMPLETE DEVELOPMENT OF PRC-004-3. DEVELOP ACTIONS TO ADDRESS THE THREE MOST COMMON CAUSES OF PROTECTION SYSTEM MISOPERATIONS.

Substation Equipment Failures Impact Transmission Event Severity

AC substation equipment failures can exacerbate the severity of transmission outages, as observed in the *State of Reliability 2013* report.

As recommended in the *State of Reliability 2013* report, NERC (through joint action of the Planning Committee and Operating Committee) formed the AC Substation Equipment Task Force (ACSETF) in 2013 to address ac substation equipment failures. The ACSETF has gathered ac substation equipment failure data from multiple sources, including but not limited to the Event Analysis Program, the Transmission Availability Data System (TADS), a supplemental TADS survey conducted by the ACSETF, and the WECC trouble report dataset. The data is being analyzed, and a report will be completed by the end of 2014.

[9] Generator Relay Loadability and Transmission Relay Loadability, http://www.nerc.com/pa/Stand/Pages/Project-2010-13-2-Phase-2-Relay-Loadability-Generation.aspx

[10] Protection System (Misoperations), http://www.nerc.com/pa/Stand/Pages/Project2010-05_Protection_System_Misoperations.aspx

[11] Protection System Coordination, http://www.nerc.com/pa/Stand/Pages/Project-2007-06-System-Protection-Coordination.aspx

In addition, NERC is focusing on increasing awareness of this risk to reliability. For example, NERC developed the adequate level of reliability metric, ALR6-13 AC Transmission Outages Initiated by Failed AC Substation Equipment, to measure performance changes in failed ac substation equipment. The metric shows that outages per element demonstrate year-over-year improvement from 2011 to 2013; this is posted on NERC's website.[12]

NERC's analysis of substation equipment, specifically circuit breakers, identified a failure trend for a specific type of circuit breaker in many of the reported events. A case history was established for a specific type of 345 kV SF_6 puffer-type circuit breaker failure. The average time between reported failures of these breakers was 4.2 months for the six failures discovered in the NERC Event Analysis program. NERC further uncovered a maintenance advisory published for this equipment that indicated the need for equipment modification. These analyses resulted in NERC issuing a Level 1 Advisory Alert regarding identification of a trend in 345 kV SF_6 puffer-type circuit breaker failures and the potential risk it posed to reliability. The purpose of the alert was to ensure industry was aware of the recent failures and previously published maintenance advisories, so appropriate action could be taken by entities that have this particular equipment. Since the alert was published, there have been no reported events caused by this failure mechanism.

RECOMMENDATION:
ASSESS THE EFFECTIVENESS OF NERC ADVISORY ADDRESSING 345 KV SF_6 BREAKER FAILURES. DEVELOP A PLAN TO ADDRESS THE CAUSES OF SUBSTATION EQUIPMENT FAILURES.

Use of Energy Emergency Alert Level 3 Declines

In 2013 there were seven Energy Emergency Alert (EEA) Level 3[13] events declared, which is significantly less than the number that occurred in prior years. EEA trends provide a relative indication of performance measured at a BA or interconnection level. By definition, when an EEA Level 3 Alert is issued, firm-load interruptions are imminent or in progress. An EEA Level 3 Alert indicates an issue with the real-time adequacy of the electric supply system. It may be due to a lack of fuel or dependence on transmission for imports into a constrained area, not simply a lack of available generation resources. In 2013, NERC began to collect and analyze more information surrounding EEA Level 3 events, including load shed, if any. Only one of the seven EEA 3 events in 2013 required firm load to be shed to preserve reliability of the BPS. This further demonstrates the ability of the BPS to perform well under stressed conditions.

There were eight instances of load shedding to mitigate actual and post-contingency transmission system conditions in 2013. The total amount of load shed did not exceed 300 MW in any of these events, and all but one lasted less than four hours.

RECOMMENDATION:
ANALYZE SYSTEM EVENTS THAT RESULTED IN FIRM LOAD SHEDDING TO DETERMINE ANY COMMON CAUSES OR TRENDS

NERC Continues to Focus on Risks to Reliability

The goal of the *State of Reliability 2014* report is to quantify risk and performance, highlight areas for improvement, and reinforce and measure success in controlling these risks. A number of activities are in place to further these objectives.

The RISC was formed in 2011 and continues to identify top-priority risks to reliability. The ongoing work in NERC's Performance Analysis area provides a foundation for their risk assessments. These highest-priority risks are being packaged into specific project work aimed at addressing components of reliability risk. NERC is actively addressing many of these risks, as called for in its corporate goals*: Review the BES[14] risk profile each year to determine actual and potential risks. The target is to identify, select, and mitigate the high-priority risks.*

[12] Reliability Indicators: Automatic Outages Initiated by Failed AC Substation Equipment / Automatic Outages Initiated by Failed AC Circuit Equipment, http://www.nerc.com/pa/RAPA/ri/Pages/Automatic-OutagesInitiatedbyFailedACSubstationACCirc.aspx

[13] http://www.nerc.com/pa/rrm/ea/Documents/EOP-002-2.pdf, EEA3 definition, page 9

[14] http://www.nerc.com/files/glossary_of_terms.pdf, BES Definition, page 20

For example, in 2014, the following projects are now ongoing:

- Changing Resource Mix
- Extreme Physical Events
- Protection System Misoperations
- Cold Weather Preparedness
- Right-of-Way Clearances
- 345 kV Breaker Failures

The NERC Standards department continues to review standards to improve the performance of the BPS.[15] This work focuses on improving the quality and content of standards while addressing key system risks identified by analyzing existing trends.

NERC continues to develop solutions to evolving threats to reliability. The BPS is a highly interconnected system with some remaining challenges, including weather (e.g., droughts, floods, severe winter) and the potential for major cyber and physical attacks. Under the direction of the Critical Infrastructure Protection Committee (CIPC), the Performance Analysis Subcommittee[16] (PAS) is collaborating with the Bulk Electric System Security Metrics Working Group to develop security performance metrics.

Development of Reliability Standards is also ongoing. On November 22, 2013, FERC approved the CIP Version 5 standards, which offer several improvements over previous versions, including increased flexibility in implementing risk mitigation to individual entity operations, elimination of unnecessary documentation requirements, and transitions from the "in or out" classification of critical assets to a "Low-Medium-High" impact-based classification at the system level. The set of CIP Version 5 standards are currently being revised to address FERC directives issued in the order approving the standards.[17]

A physical security standard is being developed in response to a FERC order issued on March 7, 2014, which stated "…the Commission directs the ERO to develop and file for approval proposed Reliability Standards that address threats and vulnerabilities to the physical security of critical facilities on the Bulk-Power System. Such Reliability Standards will enhance the Commission's ability to assure the public that critical facilities are reasonably protected against physical attacks." The FERC order directed NERC to develop the standard in 90 days. The proposed Reliability Standard would require owners or operators of the BPS, as appropriate, to identify facilities on the BPS that are critical to the reliable operation of the BPS and then develop, validate, and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities.

NERC continues to examine impacts on the BPS related to the changing resource mix. Reliably integrating high levels of variable resources (wind, solar, and some forms of hydro) into the BPS will require significant changes to traditional methods used for system planning and operation. The amount of variable generation is expected to grow considerably as policy and regulations on greenhouse gas emissions are being developed and implemented by federal authorities and individual states and provinces throughout North America. Power system planners must consider the impacts of variable generation in power system planning and design and develop the necessary practices and methods to maintain long-term BPS reliability. Operators will require new tools and practices, including potential enhancements to NERC Reliability Standards or guidelines to maintain BPS reliability. NERC is defining essential reliability services and possible sources for those services and expects to form a task force to continue related work.

[15] NERC Reliability Standards Development Plan, http://www.nerc.com/pa/Stand/Pages/ReliabilityStandardsDevelopmentPlan.aspx
[16] Performance Analysis Subcommittee (PAS) http://www.nerc.com/comm/PC/Pages/Performance-Analysis-Subcommittee-(PAS)-2013.aspx
[17] http://www.nerc.com/pa/Stand/Pages/Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions.aspx

Report Organization

Chapter 1 outlines key findings and conclusions, and Chapter 2 details the SRI_{bps} trend analysis. Chapter 3 presents a framework and statistical analysis studies that identify the top risks to the BPS using transmission outage data. Chapter 4 provides an assessment for a set of adequate level of reliability metrics. Chapter 5 outlines NERC Event Analysis efforts and findings. Chapter 6 highlights the NERC Spare Equipment Database program, an emerging NERC program that provides an important tool for industry participants to use when sharing information on the availability of spare equipment.

This report was prepared by NERC staff and the NERC PAS under the direction of the Operating Committee and Planning Committees, in collaboration with many stakeholder groups,[18] including:

- Operating Committee (OC):
  - Resources Subcommittee (RS)
  - Frequency Working Group (FWG)
  - Event Analysis Subcommittee (EAS)
  - Operating Reliability Subcommittee (ORS)
- Planning Committee (PC)
  - Reliability Assessment Subcommittee (RAS)
  - System Protection and Control Subcommittee (SPCS)
  - Protection System Misoperations Task Force (PSMTF)
  - Transmission Availability Data System Working Group (TADSWG)
  - Generating Availability Data System Working Group (GADSWG)
  - Demand Response Availability Data System Working Group (DADSWG)
  - Spare Equipment Database Working Group (SEDWG)
- Compliance and Certification Committee (CCC)

Since the initial 2010 annual reliability metrics report,[19] the PAS (formerly the Reliability Metrics Working Group)[20] has enhanced data collection and trend analysis for 16 reliability indicators[21] through NERC's voluntary or mandatory data requests.

[18] NERC Committees, http://www.nerc.com/comm/Pages/default.aspx
[19] 2010 Annual Report on Bulk Power System Reliability Metrics, June 2010, http://www.nerc.com/docs/pc/rmwg/RMWG_AnnualReport6.1.pdf
[20] Reliability Metrics Working Group (RMWG), http://www.nerc.com/comm/PC/Pages/Performance Analysis Subcommittee (PAS)/Reliability-Metrics-Working-Group-RMWG-Archives.aspx
[21] Reliability Performance Metric, http://www.nerc.com/pa/RAPA/Pages/ReliabilityIndicators.aspx

Chapter 1 – Key Findings and Conclusions

2014 State of Reliability

The BPS remains reliable and performance is high, as reflected in metrics analysis provided in Chapter 4. The revised SRI_{bps}[22] and 16 metrics that measure system characteristics and performance indicate that the BPS maintained acceptable reliability performance during observed system conditions in 2013. The system is defined as having an adequate level of reliability when the following performance objectives are maintained or achieved:[23]

1. The BES does not experience instability, uncontrolled separation, cascading, or voltage collapse under normal operating conditions and when subject to predefined disturbances.
2. BES frequency is maintained within defined parameters under normal operating conditions and when subject to predefined disturbances.
3. BES voltage is maintained within defined parameters under normal operating conditions and when subject to predefined disturbances.
4. Adverse reliability impacts on the BES following low-probability disturbances (e.g., multiple contingences, unplanned and uncontrolled equipment outages, cybersecurity events, and malicious acts) are managed.
5. Restoration of the BES after major system disturbances that result in blackouts and widespread outages is performed in a coordinated and controlled manner.
6. BES transmission capability is assessed to determine the availability to meet anticipated BES demands during normal operating conditions and when subject to predefined disturbances.
7. Resource capability is assessed to determine the BES's availability to meet anticipated BES demands during normal operating conditions and when subject to predefined disturbances.

2013 Overall Reliability Performance

An adequate level of reliability was preserved in 2013 as performance remained high, as evidenced by no significant upward or downward trends in the metrics for the 2008 to 2013 period. The SRI_{bps} and 16 metrics that measure the characteristics of an adequate level of reliability indicate the BPS is within the defined acceptable ALR performance objectives. Based on the data and analysis in the latter chapters of this report, the following key findings were identified:

- Sustained high performance for BPS reliability
- Frequency response remains stable
- Protection system misoperations cause transmission events
- Substation equipment failures impact transmission event severity
- Use of Energy Emergency Alert Level 3 declined

[22] SRI_{bps} is a "stress" index, measuring risk impact from events resulting in transmission loss, generation loss, and load loss.

[23] Definition of "Adequate Level of Reliability," http://www.nerc.com/comm/Other/Adequate Level of Reliability Task Force ALRTF DL/Final Documents Posted for Stakeholders and Board of Trustee Review/10_04_12_ALR_Definition_clean.pdf

Key Finding 1: Sustained High Performance for Bulk Power System Reliability

Daily Performance Severity Risk Assessment

Based on the SRI_{bps} and 16 metrics that measure the characteristics of an ALR, BPS reliability is adequate and within the defined acceptable ALR performance objectives. Seven out of the top-10 most severe events in 2013 were initiated or exacerbated by weather. There were no high-stress days (i.e., there were no days with an SRI_{bps} greater than 5.0) in 2013, compared to three days in 2012.

Figure 1.1 captures the daily SRI_{bps} value from 2008 to 2013, including the historic significant events. The SRI_{bps} is a daily, blended metric where transmission loss, generation loss, and load loss events are aggregated into a single value that represents the performance of the system. Accumulated over one year, these daily performance measurements are sorted in descending order to evaluate the year-on-year performance of the system. Since there is a significant difference between best days, normal days, and high-stress days in terms of SRI values, the curve is depicted using a logarithmic scale.

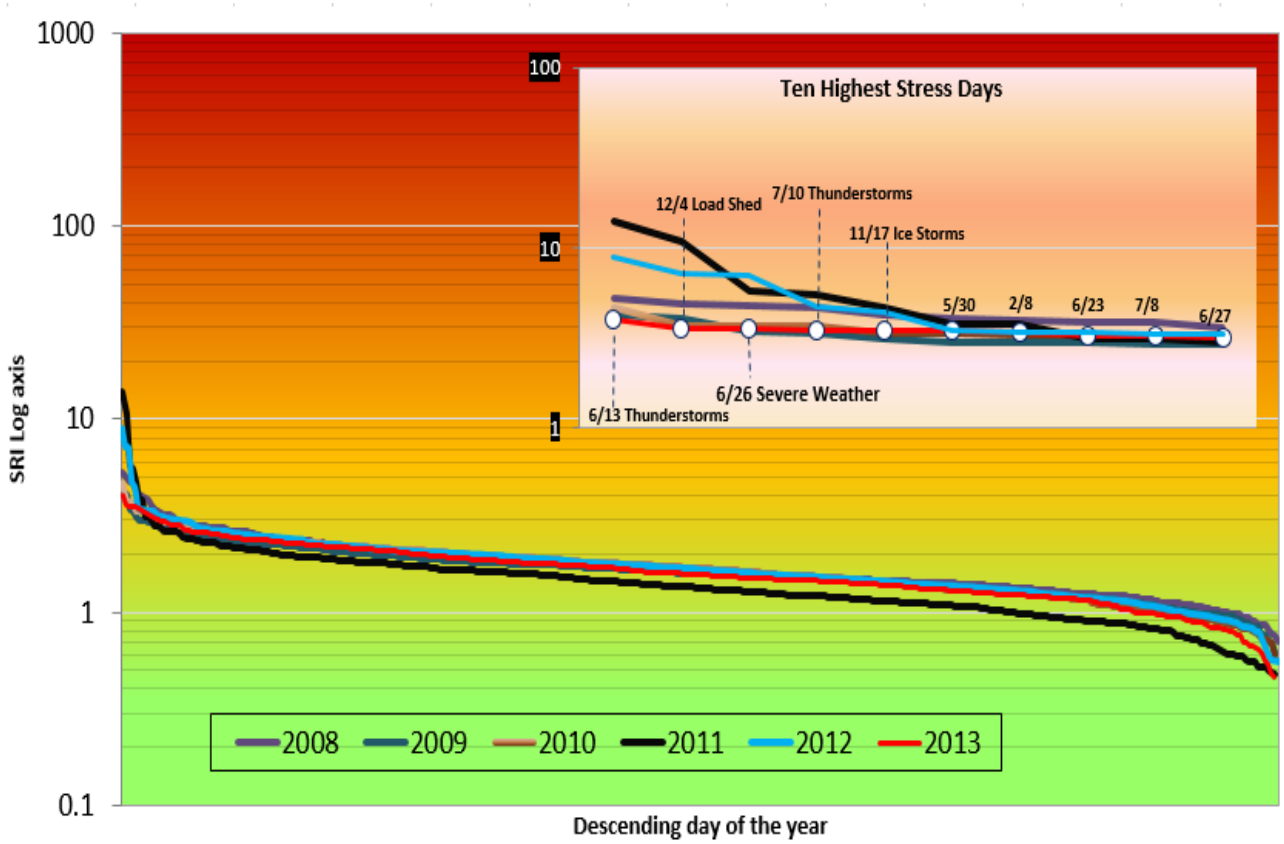


Figure 1.1: NERC Daily Severity Risk Index Sorted Descending by Year

Table 1.1: 2013 Top-Ten SRI Days							
Date	NERC SRI and Components				Weather Influenced (Y/N)	Cause Description	Interconnection
		Components and Weighting					
	SRI_{bps}	Generation (10%)	Transmission (30%)	Load Loss (60%)			
6/13/2013	4.1	14.5	4.4	2.1	Y	Severe Thunderstorms	Eastern
12/4/2013	3.6	11.1	1.7	3.3	Y	Cold/Load Shed	Western
6/26/2013	3.6	16.8	4.9	0.7	Y	Severe Weather	Eastern and Western
7/10/2013	3.5	18.9	3.0	1.2	Y	Severe Thunderstorms	Eastern
11/17/2013	3.5	7.9	3.5	2.8	Y	Severe Ice & Snow Storm	Eastern
5/30/2013	3.5	18.9	4.7	0.3	N	Power System Condition, Fire	Western and Eastern
2/8/2013	3.4	9.9	0.2	3.9	N	Equipment Failure	Eastern
6/23/2013	3.3	8.9	3.5	2.2	Y	Weather	Western
7/8/2013	3.2	14.8	5.5	0.2	Y	Rainfall Leading to Flooding	Eastern
6/27/2013	3.2	13.2	3.8	1.2	N	Fault and Equipment Failure	Western and Eastern

Steady Transmission System Availability and Metrics

Availability of the transmission system remains high with no statistically significant change in performance from 2008 to 2013. Operated at 200 kV and above, ac circuit availability is greater than 97 percent, and transformer availability is greater than 98 percent for the period of 2010–2013, the only years that planned outage data (an integral component in total availability) is available.

This availability includes both planned and unplanned outages. Planned outages for maintenance and construction have a long-term positive impact on transmission system reliability. AC circuit and transformer unavailability was well below 3 percent, as shown in Figures 1.2 and 1.3. The unavailability due to automatic sustained outages was 0.30 percent for ac circuits, and 0.10 percent for transformers. These relative percentages provide an indication of the overall availability of the transmission system operated at 200 kV and above.

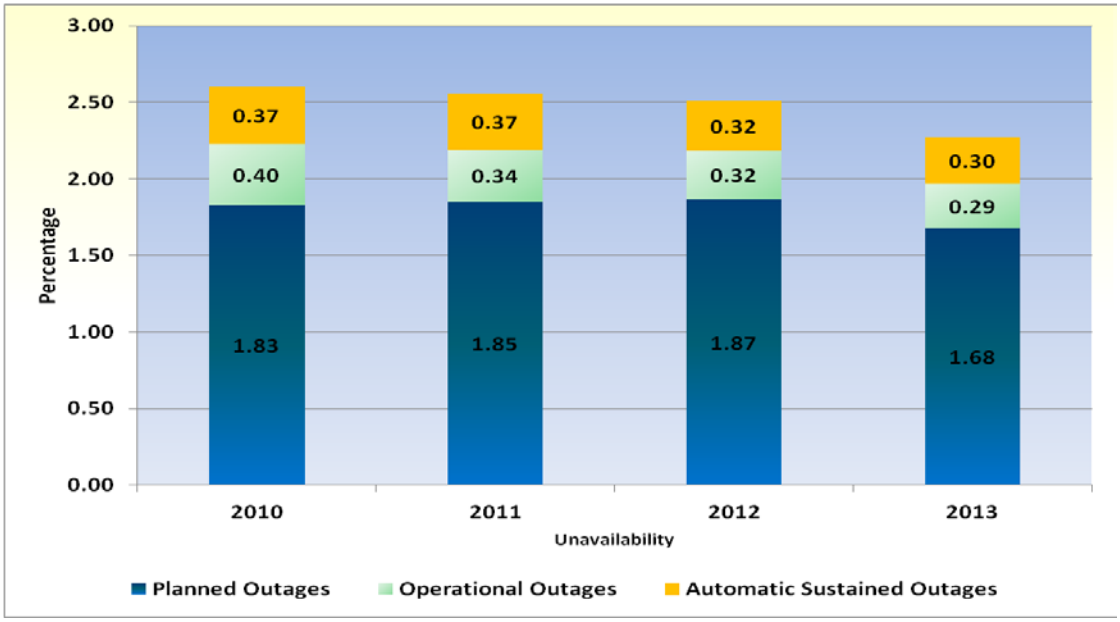


Figure 1.2: NERC Transmission AC Circuits Unavailability by Outage Type (2010–2013)

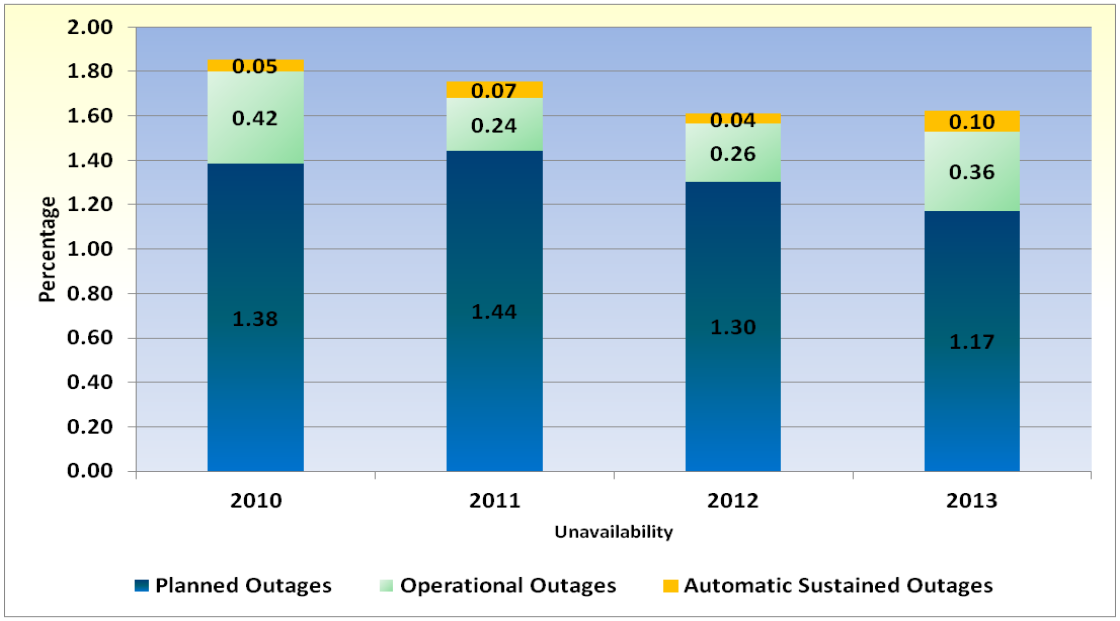
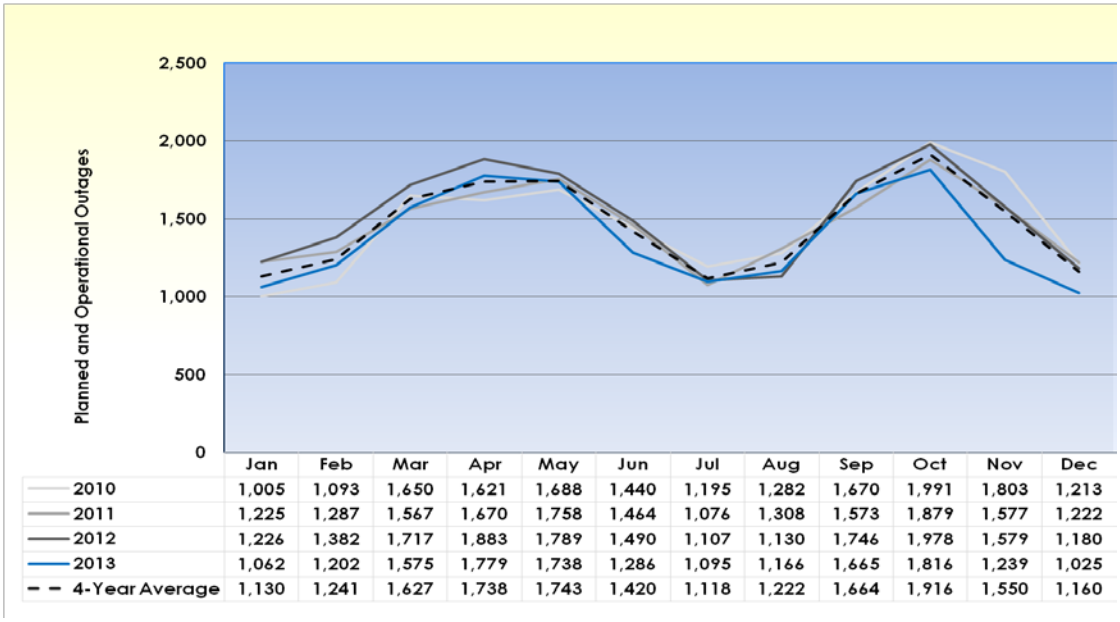


Figure 1.3: NERC Transmission Transformers Unavailability by Outage Type (2010–2013)

Figure 1.4 illustrates that during winter (December, January, and February) and summer (June, July, and August) months, the number of transmission planned and operational outages are lower compared to other months of the year, when most construction and maintenance work occurs.



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2010	1,005	1,093	1,650	1,621	1,688	1,440	1,195	1,282	1,670	1,991	1,803	1,213
2011	1,225	1,287	1,567	1,670	1,758	1,464	1,076	1,308	1,573	1,879	1,577	1,222
2012	1,226	1,382	1,717	1,883	1,789	1,490	1,107	1,130	1,746	1,978	1,579	1,180
2013	1,062	1,202	1,575	1,779	1,738	1,286	1,095	1,166	1,665	1,816	1,239	1,025
4-Year Average	1,130	1,241	1,627	1,738	1,743	1,420	1,118	1,222	1,664	1,916	1,550	1,160

Figure 1.4: NERC Transmission Planning and Operational Outages by Month (2010–2013)

Overview of NERC Actions Supporting Sustained High Performance

NERC's Reliability Risk Management (RRM) group performs assessments (including real-time or near-real-time assessments) of the reliability and adequacy of the BPS and identifies potential issues of concern relating to system, equipment, entity, and human performance. RRM focuses on awareness of BPS conditions and events. The group analyzes events and addresses the most significant risks to BPS reliability, ensuring that industry is well informed of system events, emerging trends, risk analysis, lessons learned, and expected actions. The observations from RRM's focused situation awareness and event analysis activities are consistent with the broader conclusions above and provided context and depth to all 10 of the top SRI days as shown in Table 1.1.

In 2013, several standards projects were completed that support sustained high performance of BPS reliability by providing the data necessary for bulk transmission system analysis. The Modeling Data standards[24] provide a foundational framework for consistent data requirements and reporting procedures needed to develop planning horizon simulation models critical to support the analysis of the interconnected BPS's reliability. The standards establish clear expectations of who provides what data to whom to support each interconnection model construction and introduces Planning Coordinator-level data validation within each planning area. The Demand Data standard[25] provides authority for applicable entities to collect demand, energy, and related data to support reliability studies and assessments measuring whether there is an adequate amount of resources available to serve peak demand while also maintaining a sufficient margin to address operating events. This Reliability Standard enumerates the responsibilities and obligations of requestors and respondents of the data. The ATC standard[26] requires available transmission system capability to be determined to support the reliable operation

[24] MOD-032-1 and MOD-033-1, Modeling Data (MOD B), http://www.nerc.com/pa/Stand/Pages/Project2010-03ModelingData(MOD-B).aspx
[25] MOD-031-1, Demand Data (MOD C), http://www.nerc.com/pa/Stand/Pages/Project2010-04DemandData(MOD-C).aspx
[26] MOD-001-2, ATC Revisions (MOD A), http://www.nerc.com/pa/Stand/Pages/Project201205MODAAvailableTransferCapability.aspx

of the BPS, and that the methods and data underlying those determinations must be disclosed to those registered entities that need such information for reliability purposes.

In early 2014, NERC completed work on modifications to a standard on operator communications protocols, COM-002-4.[27] The purpose of the standard is to improve communications for the issuance of operating instructions with predefined communications protocols to reduce the possibility of miscommunication that could lead to action or inaction harmful to the reliability of the BES. The standard addresses communications protocols for operating personnel in emergency and non-emergency conditions.

Key Finding 2: Frequency Response Remains Stable

NERC annually applies statistical tests to interconnection frequency response datasets,[28] including additional analyses on time of year, load levels, and other attributes. From 2009 to 2013, the Eastern Interconnection, ERCOT Interconnection, Québec Interconnection,[29] and Western Interconnection have shown steady frequency response performance, trending above the recommended IFRO at all times during the study period. The Eastern Interconnection data showed a slightly downward trend in frequency response; however, this trend is not statistically significant. It is important to continue to monitor these trends to determine whether any numbers approach or drop below the IRFO for any interconnection. The study methods and statistical results are summarized in Chapter 4 (ALR1-12) and detailed in Appendix B.

Overview of NERC Actions Supporting Sustained Frequency Response

FERC approved BAL-003-1 on January 16, 2014. This standard establishes a minimum frequency response obligation for each BA, provides a uniform calculation of frequency response and frequency bias settings that transition to values closer to natural frequency response, and encourages coordinated Automatic Generation Control operation. This standard, in partnership with BAL-001-2, maintains interconnection steady-state frequency within defined limits by balancing real power demand and supply in real time. BAL-003-1 will ensure that BAs take actions to maintain interconnection frequency, with each BA contributing its fair share to frequency control. BAL-001-2 is pending regulatory approval.

NERC is continuing development work in 2014 on the Reliability Standards that relate to frequency response. The Balancing Authority Reliability-Based Controls: Reserves project[30] is modifying BAL-002 to measure the ability of an entity to recover from a reportable event with the deployment of its reserves. The reliable operation of the interconnected BPS requires that adequate generating capacity be available at all times to maintain scheduled frequency and avoid loss of firm load following loss of transmission or generation contingencies. This generating capacity is necessary to replace generating capacity and energy lost due to forced outages of generation or transmission equipment. The Disturbance Monitoring project[31] is modifying PRC-002 to establish requirements for recording and reporting sequence-of-events (SOE) data, fault-recording (FR) data, and dynamic-disturbance-recording (DDR) data to facilitate analyses of disturbances. The proposed modifications to the standard will not specify what equipment must be used to capture this data but will focus on ensuring that the requisite data is captured. This will improve system reliability by providing personnel with necessary data to enable more effective analysis of events that affect the BES.

There were no reported Event Analysis Program[32] qualified events in 2013 where frequency response performance was cited as a causal factor for initiating or sustaining an event. NERC will examine incidents in 2013

[27] Operating Personnel Communications Protocols, http://www.nerc.com/pa/Stand/Pages/Op_Comm_Protocol_Project_2007-02.aspx
[28] Datasets described in the Frequency Response Initiative Report, October 2012 http://www.nerc.com/docs/pc/FRI_Report_10-30-12_Master_w-appendices.pdf
[29] Only Québec Interconnection 2011 and 2012 frequency response data is available.
[30] Phase 1 of Balancing Authority Reliability-based Controls: Reserves, http://www.nerc.com/pa/Stand/Pages/Project2010-14-1-Phase-1-of-Balancing-Authority-RBC.aspx
[31] Disturbance Monitoring, http://www.nerc.com/pa/Stand/Pages/Project_2007-11_Disturbance_Monitoring.aspx
[32] http://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx

where frequency response was below the IFRO to determine any actions that should be taken in response to the frequency response performance.

Recommendation
NERC will examine and develop root causes for incidents in 2013 where frequency response was less than the IFRO. NERC will determine additional actions, beyond those currently being worked on in NERC Standards, that should be taken to maintain and improve frequency response performance.

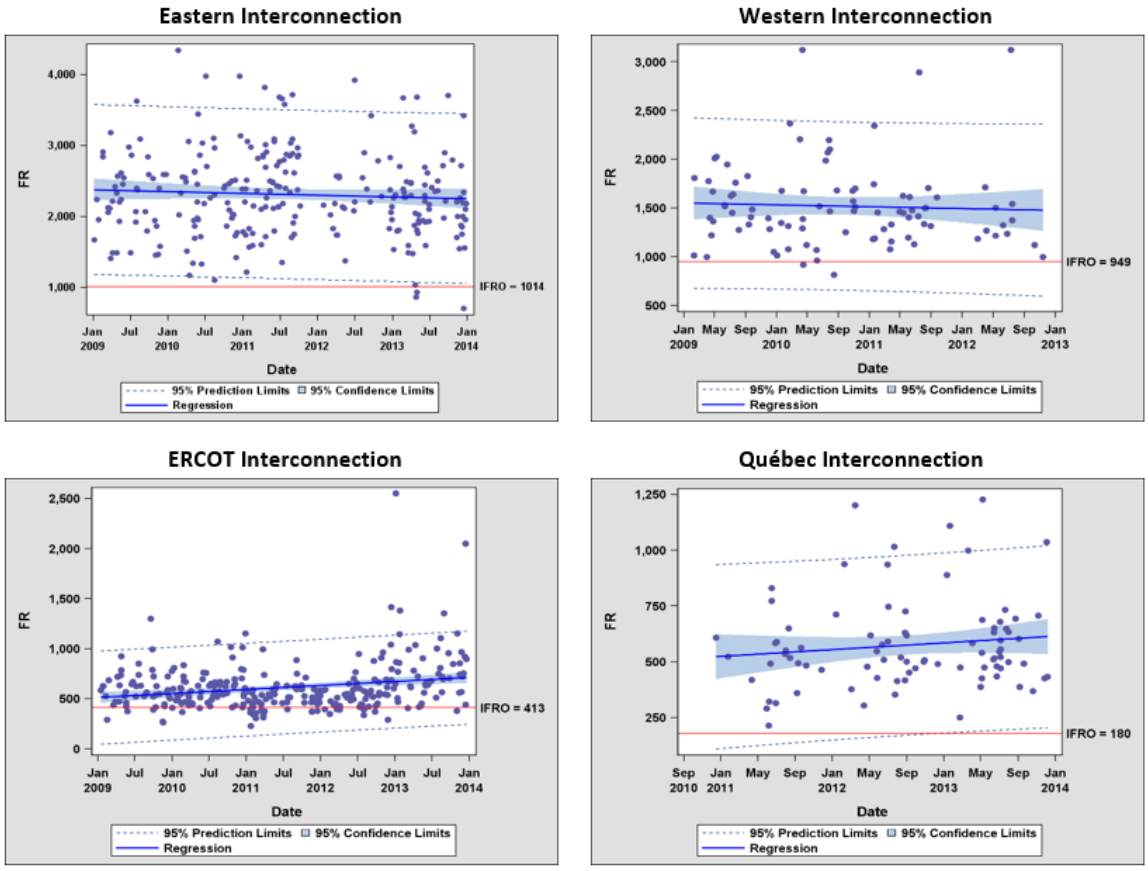


Figure 1.5: Interconnection Frequency Response Trend (2009–2013)

Key Finding 3: Protection System Misoperations Cause Transmission Events

Protection System Misoperation was identified in previous years as a cause code that has significant probability of occurrence and is positively correlated with transmission severity when outages do occur. Below are additional findings from analyses of misoperations from 2011 through 2013:

- Misoperation occurrences have been consistent over the past three years, with approximately 2,000 misoperations per year.
- The rate of misoperations, as a percentage of total operations, has remained consistent during this period at approximately 10 percent (i.e., roughly one in 10 operations is a misoperation).
- The three most common causes of misoperations remain the same (approximately 65 percent of misoperations are caused by settings/logic/design errors, communication failures, and relay failures).

Three datasets are available to better understand the impact of misoperations on reliability. One dataset is a database of all misoperations that occur on the BES (100 kV and above) that is collected on a quarterly basis by the Regions and NERC. This database provides a comprehensive set of data for all transmission and generation misoperations. It is submitted by the system protection owners and includes detailed information about the misoperation, including a description of the misoperation, its category, its causes, and the proposed mitigation and completion date.

A second dataset that is used to assess risk associated with misoperations is the event reports that are submitted to the Regions and NERC through the event analysis program document that was established by the Events Analysis Subcommittee (EAS). When misoperations are associated with reported system disturbances, NERC can then assess their actual impact on the BES and also identify whether they were causal or contributory to the event through cause coding.

A third source of misoperations reporting occurs through the TADS data collection. Misoperations that were identified as being caused by human error or relay failure are identified in TADS reporting. This occurs for transmission facilities operated at 200 kV and above.

Focusing the statistical analysis of the 2012–2013 TADS data on the transmission severity and initiating causes of TADS events yields the following results and observations:

- Excluding Weather-related and Unknown Initiating Cause Codes (ICC),[33] Misoperations is one of the two largest contributors to the transmission severity risk.
- TADS events initiated by Misoperations and Failed AC Substation Equipment ICCs have a greater expected severity than all other TADS ICC events.

In 2013, there were 71 transmission-related system disturbances that resulted in a NERC Event Analysis reported event. Of those 71 events, 47 (about 66 percent) had associated misoperations. Of these 47 events, 38 (about 81 percent) experienced misoperations that were contributory to or exacerbated the severity of the event. In several cases, multiple misoperations occurred during a single disturbance. Cause coding has not yet been completed for all 2013 events, but it is estimated that there were 60–75 misoperations associated with these 38 reportable events. Therefore, out of approximately 2,000 total misoperations in 2013, approximately 3.0 to 3.5 percent were causal to or exacerbated by the severity of reportable system disturbances.

Two complementary views of misoperations data have been provided in this report. Based upon the total number of misoperations experienced by the industry, the relationship between the Misoperations ICC and transmission risk, and the positive correlation between misoperations and transmission severity, understanding and reducing misoperations should remain a focus of NERC and industry participants.

Overview of NERC Actions Addressing System Protection Misoperations

NERC is continuing activity on several projects to address protection system misoperations. The Reliability Issues Steering Committee (RISC) has identified system protection reliability, uncoordinated protection systems, and protection system misoperations as top-priority risks to reliability. NERC has focused its Reliability Standards efforts in this area with the completion of the relay loadability standards[34] and continues work on relay misoperations[35] and coordination.[36] In addition, NERC staff is coordinating with the North American Transmission

[33] ICC - The Automatic Outage Cause Code that describes the initiating cause of the outage, page 16, Appendix 7, http://www.nerc.com/docs/pc/tadswg/Appendix%207%2020101202a%20clean.pdf

[34] Generator Relay Loadability and Transmission Relay Loadability, http://www.nerc.com/pa/Stand/Pages/Project-2010-13-2-Phase-2-Relay-Loadability-Generation.aspx

[35] Protection System (Misoperations), http://www.nerc.com/pa/Stand/Pages/Project2010-05_Protection_System_Misoperations.aspx

[36] Protection System Coordination, http://www.nerc.com/pa/Stand/Pages/Project-2007-06-System-Protection-Coordination.aspx

Forum to find ways to reduce protection system misoperations and develop methods to minimize their impact. NERC Event Analysis continues to examine system events to identify those that are impacted by protection system misoperations to determine if action is needed to address trends and common modes of misoperations.

Recommendation
NERC will complete development of Reliability Standard PRC-004-3 — Protection System Misoperation Identification and Correction. NERC will develop a plan and catalyze industry action to address the three most common causes of protection system misoperations (settings/logic/design errors, communication failures, and relay failures).

Key Finding 4: Substation Equipment Failures Impact Transmission Event Severity

As mentioned in Chapter 3, AC Substation Equipment Failures had the largest positive correlation with automatic transmission outage severity in 2013. The correlation is statistically significant: a pattern and underlying dependency exists between ac substation equipment failures and transmission outage severity. A similar observation was made in Key Finding #5 of the *State of Reliability 2013* report. NERC recommended that a small subject matter expert technical group be formed to further validate the findings and root causes to understand the contributing factors of ac substation equipment failures and provide solutions to improve performance. The AC Substation Equipment Task Force (ACSETF) was created to address high-priority reliability issues related to ac substation equipment. The ACSETF has gathered ac substation equipment failure data from multiple sources, including but not limited to the Event Analysis Program, TADS, a supplemental TADS survey conducted by the ACSETF, and the WECC trouble report dataset. The failure data is currently being analyzed by the ACSETF.

ACSETF Work Status

Based on the data reviewed through March of 2014, the ACSETF has observed:

1. The highest percentages of outages involve circuit breaker failures, as previously reported in the *State of Reliability 2013* report.[37]
2. The top-four sub-components that result in circuit breaker failures, in descending order of frequency, are: interrupters, mechanism, trip coil, and bushing.
3. Inherent in circuit breaker failure is an increased probability that additional BPS elements will also be out of service.
4. Inherent in transformer failure is an increased probability of longer outage duration.
5. Further data collection and analysis is needed, including maintenance strategies, bus configurations, and failure event SRI calculation.

The ACSETF will provide a summary of its analysis along with suggestions for improvement and other observations to the NERC PC and OC for review and approval. The final report is scheduled to be completed by December 31, 2014, and results are anticipated to be incorporated in *State of Reliability 2015* report.

Overview of NERC Actions Addressing AC Substation Equipment Failures

In addition, NERC is focusing on increasing awareness of this risk to reliability. For example, NERC developed the adequate level of reliability metric, ALR6-13 AC Transmission Outages Initiated by Failed AC Substation Equipment,

[37] http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2013_SOR_May%2015.pdf

to measure performance changes in failed ac substation equipment. The metric shows that outages per element demonstrates year-over-year improvement from 2011 to 2013; this is posted on NERC's website.[38]

Circuit breaker failures, in conjunction with another system fault, may lead to more BES facilities being removed from service than required to clear the original fault. High-voltage circuit breaker failures are one of the leading contributors of severe disturbances on the BES. When NERC identified a potential trend of 345 kV SF_6 puffer-type breakers failing, a Level 1 NERC Advisory was issued.[39]

Recommendation
NERC will assess the implementation and effectiveness of the Level 1 NERC Advisory issued to address 345 kV SF_6 puffer-type breaker failures. NERC will develop a plan with milestones to address the causes of substation equipment failures identified by the ACSETF. NERC will develop and facilitate data collection necessary to perform future analysis of substation equipment failures, as recommended by the ACSETF.

Key Finding 5: Use of Energy Emergency Alert Level 3 Declines

In 2013 there were seven Energy Emergency Alert (EEA) Level 3 events declared, which is significantly lower than the number that occurred in prior years. Additionally in 2013, changes were made to the metric ALR6-2 to include duration in hours that an EEA was in effect at any level and the amount of load shed that was necessitated by an EEA Level 3 event.

This data collection was first performed for 2013 EEA data, and it showed that of the seven EEA Level 3 events declared, only one resulted in any amount of load shed. The other six fell into two categories. One category pertained to significant unplanned outages of resource supply due to generator trip or equipment failure—either the unplanned loss of one or more generation resources, or the unplanned loss of a major transmission facility that supplied generation into an area. These included quickly evolving events in which the entity had to use its reserves to serve its load and had to prepare for load shed to meet the next possible contingency. The other category consisted of events in which transmission limitations in the form of Transmission Loading Relief (TLR)[40] events were in place and were affecting entities that rely upon import transactions to serve their load. These events did not involve unplanned loss of generation or equipment failures; rather, they occurred as loading increased over a period of time and the affected Transmission Operator (TOP) responded by requesting various levels of TLR relief. The entities in this category used the EEA Level 3 Alert to protect their firm transactions, to avoid having to reduce load, and to call upon reserve-sharing provisions to restore reserves.

Throughout 2013, there were eight instances of firm load shedding not driven by EEA Level 3 events. These eight load-shedding instances were distributed across four distinct events. Of the eight instances where firm load was shed, five instances were required to mitigate post-contingency transmission facility overloads, one instance was to mitigate actual transmission facility overloads and low voltages following a major transmission system disturbance, and one instance was to mitigate non-convergence of state estimation, indicating an unknown operating state. In all eight instances, the use of load shedding was successful at preventing greater and more widespread impacts.

Recommendation
NERC will analyze system events that resulted in firm load shedding to determine any common causes or trends that warrant action.

[38] Reliability Indicators: Automatic Outages Initiated by Failed AC Substation Equipment / Automatic Outages Initiated by Failed AC Circuit Equipment, http://www.nerc.com/pa/RAPA/ri/Pages/Automatic-OutagesInitiatedbyFailedACSubstationACCirc.aspx
[39] Industry Advisory: 345kV Breaker Failures Initial Distribution: August 27, 2013
[40] http://www.nerc.com/pa/rrm/TLR/Pages/default.aspx

Recent Changes

The state of reliability is an ever-changing landscape. A number of activities were pursued in 2013 to further improve the metrics and assessments:

Modified SRI calculation

In 2013, the Performance Assessment Subcommittee received concerns that the SRI calculation was dominated by loss-of-load impacts. Since the weather-related events often have distribution-related outages to a greater degree than generation or transmission impacts, the SRI calculation was modified to remove most of the distribution facility outage causes from the load-loss component of the calculation. Only load loss caused by loss of supply from either the generation or transmission system is now included in the SRI calculation. This report describes the new calculation of SRI, referred to as SRI_{bps}. Consistent with observations in prior state of reliability reports, severe weather remained a major contributor to many of the high-severity days.

Retired KCMI

The PAS reviewed the existing Key Compliance Monitoring Index (KCMI)[41] and in collaboration with the Compliance and Certification Committee (CCC) retired it in 2013. Prior state of reliability reports noted that the trend for this index continued to reflect fewer violations of standards. It became increasingly difficult to update the standards violations that were included in the KCMI to stay current with evolving Reliability Standards and provide a meaningful metric. As a part of NERC's three-element view of risk, compliance violations associated with Reliability Standards remain an important part of the analysis of reliability. Therefore, an effort has begun to create a new metric to track performance with regard to violations of Reliability Standard requirements that are considered to have a serious risk to the BES. The expectation is that the replacement of KCMI in 2014 with an improved compliance metric would provide more meaningful information on standards violations with a potentially serious impact to reliability.

Revised Adequate Level of Reliability Definition

In late 2012, NERC adopted a revised definition of Adequate Level of Reliability, which forms the basis for the reliability indicators that are used as metrics to evaluate the performance of the BES. The seven performance objectives and associated expected performance outcomes were developed to encompass NERC's responsibility to ensure reliability of the BES. This year's state of reliability report contains a mapping of the seven performance objectives to the existing performance metrics. Also, a new naming convention has been proposed to move from the former six-element definition to the new definition, which has seven categories of performance objectives.

Modification of Metrics

Finally, in the annual review of the existing metrics, efforts were made to consolidate metrics that were similar, and to add dimension to metrics in areas where additional information may provide insight, particularly in capturing duration of events and magnitude of impact to the BES with load interruption. To meet these goals, two metrics were retired, and several were modified to either add additional criteria or provide additional dimensions of data collection to the metrics. These modified metrics are included in more detail in Chapter 4.

Additional NERC Initiatives

NERC continues to develop solutions to evolving threats to reliability. The BPS is a highly interconnected system with some remaining challenges, including weather (e.g., droughts, floods, severe winter) and the potential for major cyber and physical attacks. Under the direction of the CIPC, the PAS is collaborating with the Bulk Electric System Security Metrics Working Group to develop security performance metrics.

[41] http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2013_SOR_May%2015.pdf KCMI definition, page 42

NERC's Standards department continues to review the standards to improve performance of the BPS via the Standards Development Plan.[42] This work focuses on improving the quality and content of standards while addressing key system risks as identified through analysis of existing trends.

In response to FERC directives, through 2014 NERC will continue to develop modifications to the CIP Reliability Standards when approving Version 5.[43] NERC is also developing a standard on Physical Security,[44] which will require owners or operators of the BPS, as appropriate, to identify facilities on the BPS that are critical to the reliable operation of the BPS. Additionally, owners or operators of those identified critical facilities will develop, validate, and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities.

Reliably integrating high levels of variable resources (wind, solar, and some forms of hydro) into the North American BPS will require significant changes to traditional methods used for system planning and operation. The amount of variable renewable generation is expected to grow considerably as policy and regulations on greenhouse gas emissions are being developed and implemented by federal authorities and individual states and provinces throughout North America. Power system planners must consider the impacts of variable generation in power system planning and design and develop the necessary practices and methods to maintain long-term BPS reliability. Operators will require new tools and practices, including potential enhancements to NERC Reliability Standards or guidelines to maintain BPS reliability.

NERC is continuing its focus on refining ICCs, including further analysis on the "Unknown" cause code. In the *State of Reliability 2013* report, transmission outages with an ICC of Unknown contributed to 19 percent of all TADS events. A recommendation was made to provide additional guidance to those entities reporting sustained outages with an ICC of Unknown.

The subject of TADS outages reported with initiating cause as Unknown was reviewed and discussed with the TADS Working Group (TADSWG). Results of statistical analyses on historical TADS event data (2008–2012) was presented by NERC staff and discussed at recent TADSWG meetings. The results indicated that:

- TADS events with ICCs of Lightning, Unknown, Contamination, and Foreign Interference tend to initiate Momentary Events.
- There is a statistically significant negative correlation between sustained events and TADS events with ICCs of Lightning, Unknown, Contamination and Foreign Interference.
- There is a statistically significant positive correlation between Sustained events and the following ICCs: Human Error, Failed AC Substation Equipment, Failed AC Circuit Equipment, Weather Excluding Lightning, Fire, Failed Protection System Equipment, Other, and Power System Condition.
- Approximately 40 percent of TADS event data are momentary events (an automatic outage less than one minute).

Further analysis has revealed that approximately 60 percent of TADS events with ICC Unknown are momentary events.

[42] NERC Reliability Standards Development Plan, http://www.nerc.com/pa/Stand/Pages/ReliabilityStandardsDevelopmentPlan.aspx
[43] Critical Infrastructure Protection Standards Version 5 Revisions, http://www.nerc.com/pa/Stand/Pages/Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions.aspx
[44] Physical Security, http://www.nerc.com/pa/Stand/Pages/Project-2014-04-Physical-Security.aspx

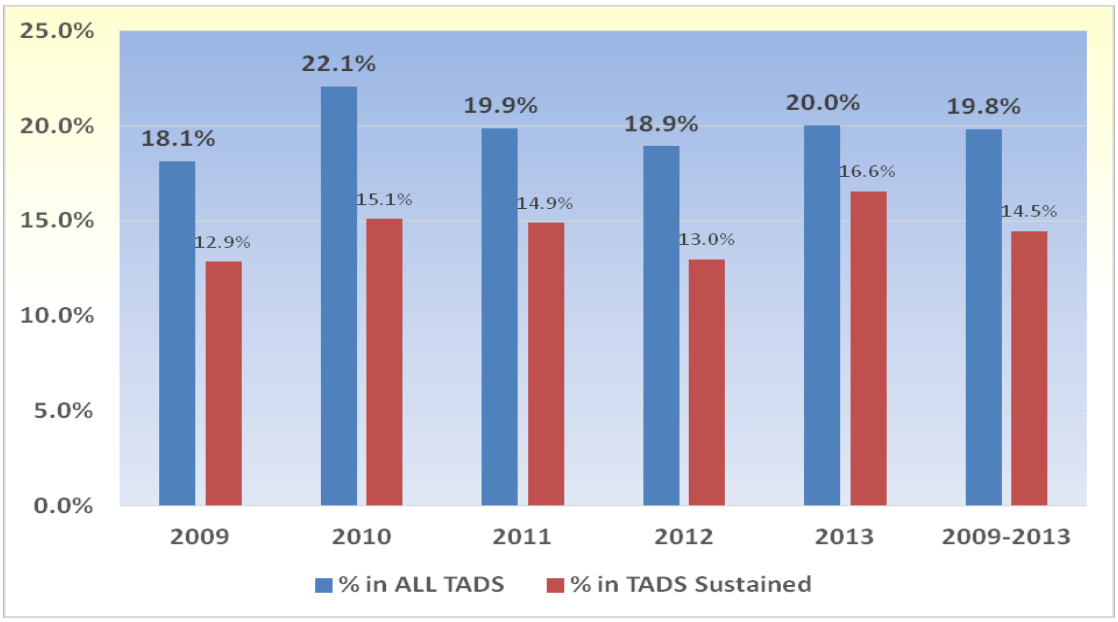


Figure 1.6: Percentage of Unknown Events in all TADS Events vs. in TADS Sustained Events

It is often not possible to confidently determine an ICC for momentary outages, so focus should be on sustained outage events with ICC of Unknown. It is possible that in certain cases, coding sustained outages as Unknown may be due to a lack of clarity on the part of reporting entities for coding events. The TADSWG continues to address questions from TADS reporting entities pertaining to TADS event coding. Specific outage scenarios are reviewed and clarifications to the TADS Data Reporting Manual are applied. These specific changes are reviewed during TADS training sessions, which are held annually with the TADS reporting entities. The TADSWG will continue to monitor the TADS outage data for the purpose of enhancing the cause coding process to minimize the number of sustained outages with ICC as Unknown. NERC will continue to identify and work with entities that report relatively high proportions of Unknown outages to resolve any outage coding issues.

Chapter 2 – Daily Performance Severity Risk Assessment

Overview

The PAS previously developed[45] Figure 2.1 to depict the metrics used to measure the major categories of risks to reliability.

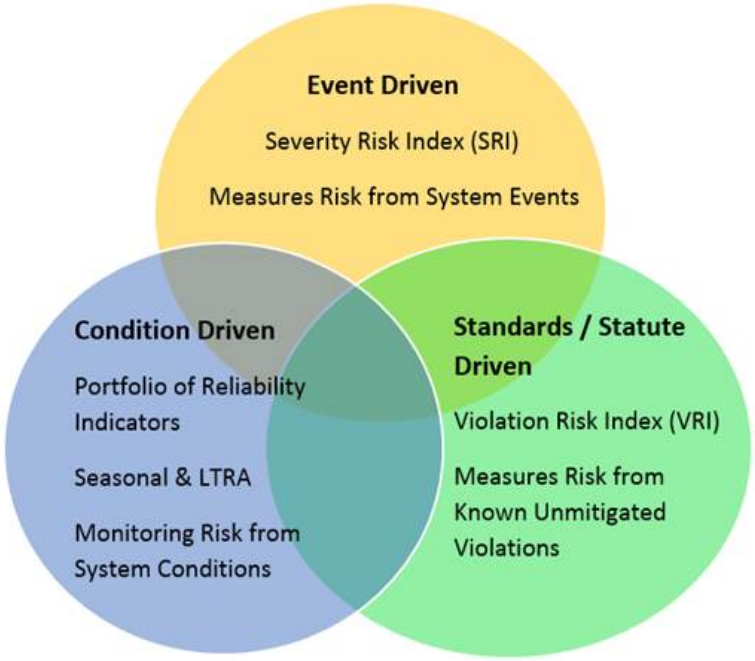


Figure 2.1: Conceptual Risk Model for Bulk Power System

The PAS also developed metrics designed to measure the performance of each of the categories of risk. While some of these metrics are still evolving, the use of the SRI[46] has proven to be a useful way of quantifying the daily performance of the BPS.

During 2013, the PAS undertook significant efforts to enhance the SRI, and it was recognized that the method of calculating the value relied on data that may not have aligned optimally with the index. As a result, revised data was developed, whereupon calculations were modified and results were tested. The SRI was calculated by using the historic method, labeled SRI_{OLD}, then compared against the revised method, labeled SRI_{bps}. These results were shared, along with the recommendation by the PAS to the OC and PC, who approved the revised calculation.

This year's analysis relies on this modified calculation, and all use of SRI_{OLD} has been discontinued in this year's *State of Reliability* report.

Key conclusions were:

- The performance on high-stress days was as good as that recorded in 2009 and 2010, which were the best years since data collection began.
- Contrary to prior years, load loss events were not the primary indicator of a high SRI day; in fact, three of the top-10 days for the year appeared to be driven by generation and transmission outage performance and did not significantly involve load loss (load loss severity was less than 1.0).

[45] Integrated Reliability Index Concepts, http://www.nerc.com/docs/pc/rmwg/Integrated_Reliability_Index_WhitePaper_DRAFT.pdf
[46] SRI Enhancement paper, http://www.nerc.com/comm/PC/Performance Analysis Subcommittee PAS 2013/SRI Enhancement Whitepaper.pdf

- There were several high-stress days resulting from extreme Weather events. In general, the SRI correctly correlated with those events, and the power system—while stressed—responded well.
- The majority of the top-10 most severe days in 2013 were initiated or exacerbated by Weather (seven of the 10 days).
- There were no high-stress days (SRI greater than 5.0) in 2013.
- For SRI values less than 5.0, 2013 had better average performance than all years except 2008, where its average value was very close to the 2008 average value.
- Generation outages contribute substantially to daily SRI_{bps} values.

NERC Assessment

Figure 2.2 captures the daily SRI_{bps} values from 2008 to 2013. The SRI is comprised of three key components: generation severity, transmission severity, and load-loss severity. For context throughout this report, each of these severity measures is calculated based on certain assumed and average values and does not rely on individual analyses that measured the specific impact of any given element's function. In particular, generation severity reflects the generation unavailability of a given unit with a plant capacity as a percentage of all available plant capacity. Transmission severity reflects the unscheduled availability of a particular TADS element for which the impact is calculated by a voltage-weighted value divided by the total inventory of TADS elements. Load-loss severity is calculated as an average customer usage at peak for the day the load-loss event occurred. The inset in Figure 2.2 highlights the highest stress days experienced in 2013 from the left side of the SRI curve.

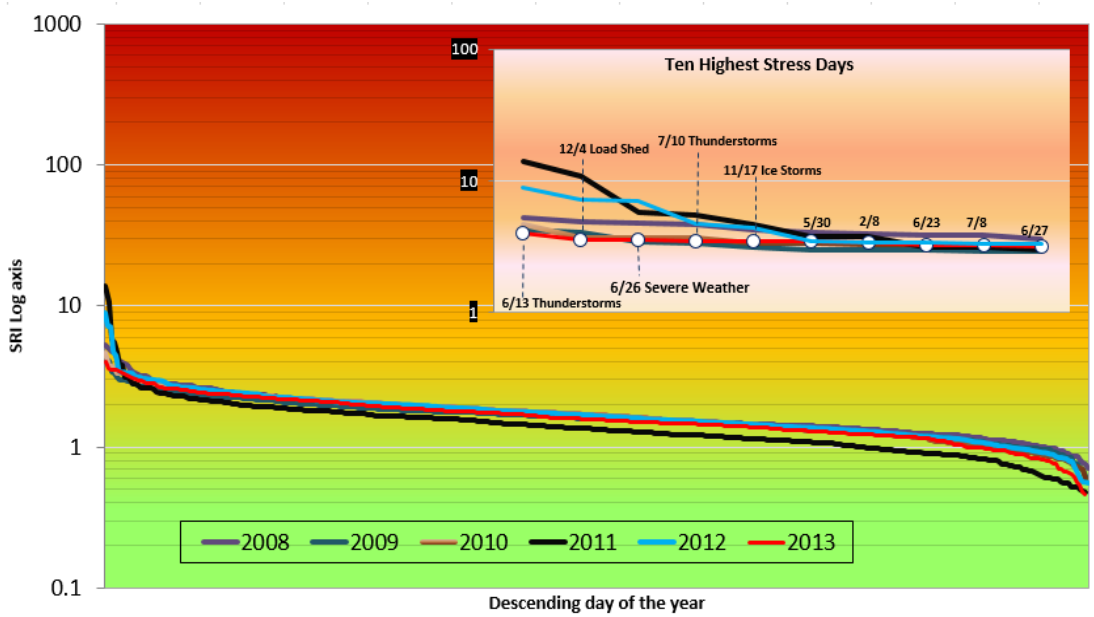


Figure 2.2: NERC Annual Daily Severity Risk Index Sorted Descending

As the year-to-year performance is evaluated in Figure 2.2, certain portions of the graph become relevant for specific analysis. First, the left side of the graph, where the system has been substantially stressed, should be considered in the context of the prior years' high-stress days. Next, the slope of the central part of the graph may reveal year-to-year changes in performance for the majority of the days of the year and demonstrate routine system resilience. Finally, the right portion of the curve may also provide useful information about how many days with lower SRIs occurred during any given year compared to another. The transition to SRI_{bps} allows the entire range of the curve to be used. Prior versions interpreting the right side of the curve may have been misleading, since load-loss calculations were not able to be performed for each calendar day of the year. As well, the left-hand

side of the graph, with the inclusion of distribution-related load-loss events, may have overstated the impact of the load-loss component that pertains to the BPS.

Table 2.1 provides a historical summary of the top-10 SRI_{bps} days. When comparing the values to those in previous state of reliability reports, consider that this summary is based on the updated SRI_{bps} methodology calculation.

Table 2.1: 2013 Top-Ten SRI Days

Date	NERC SRI and Components				Weather Influenced (Y/N)	Cause Description	Interconnection
		Components and Weighting					
	SRI_{bps}	Generation (10%)	Transmission (30%)	Load Loss (60%)			
6/13/2013	4.1	14.5	4.4	2.1	Y	Severe Thunderstorms	Eastern
12/4/2013	3.6	11.1	1.7	3.3	Y	Cold/Load Shed	Western
6/26/2013	3.6	16.8	4.9	0.7	Y	Severe Weather	Eastern and Western
7/10/2013	3.5	18.9	3.0	1.2	Y	Severe Thunderstorms	Eastern
11/17/2013	3.5	7.9	3.5	2.8	Y	Severe Ice & Snow Storm	Eastern
5/30/2013	3.5	18.9	4.7	0.3		Power System Condition, Fire	Western and Eastern
2/8/2013	3.4	9.9	0.2	3.9		Equipment Failure	Western
6/23/2013	3.3	8.9	3.5	2.2	Y	Weather	Western
7/8/2013	3.2	14.8	5.5	0.2	Y	Rainfall Leading to Flooding	Eastern
6/27/2013	3.2	13.2	3.8	1.2		Fault and Equipment Failure	Western and Eastern

In 2013 there were no days that the SRI_{bps} score exceeded 5.0, which is an indicator of a "noteworthy" day. A handful of days are identified on the inset. These include the five days in 2013 with the highest SRI_{bps} score, all of which have an SRI value less than 4.5. The year 2013 was comparable to 2009 and 2010, which were the best years recorded since this data began being collected.

Table 2.1 lists the 10 event dates with highest daily SRI values in 2013 and indicates the component contribution to the SRI_{bps}. The SRI_{bps} results were compared against Form OE-417 data to determine which ones were weather-related.[47] This comparison is shown on Table 2.2. Seven of the top-10 SRI days were weather-influenced, as compared to all of the top-10 SRI days in 2012.

Table 2.2: OE-417 Event Reports versus Load Loss Severity

Date Event Began	Date of Restoration	Area Affected	NERC Region	Event Type	Demand Loss (MW)	Number of Customers Affected	Customer Load Loss (mw) Associated with Significant SRI Day	Feed CAIDI	Restoration Promptness CAIDI Factor	Load Loss SRI	SRI Date
2/8/2013	2/8/2013	District of Columbia; Prince George's County Maryland	RFC	Equipment Trip & Failure	140	52,000	0.01017638	2,356	1	3.8721	2/8/2013
3/3/2013	3/3/2013	Merced County, California	WECC	Transmission System Interruption	300	58,850	0.00886310	691	1	1.2318	3/3/2013
6/13/2013	6/13/2013	District of Columbia; Maryland	RFC	Loss of 300+ MW Load; Severe Weather - Thunderstorms	700	40,000	0.01140619	1,462	1	2.1243	6/13/2013
6/13/2013	6/14/2013	Southern Company Territory	SERC	Severe Weather - Thunderstorms	550	165,798					
6/13/2013	6/14/2013	Richmond Metro area, Virginia	SERC	Severe Weather - Thunderstorms	900	283,000					
6/13/2013	6/14/2013	Western Piedmont North Carolina	SERC	Severe Weather - Thunderstorms	1,000	175,000					
6/13/2013	6/14/2013	Central and Eastern North Carolina	SERC	Severe Weather - Thunderstorms	Unknown	53,000					
6/23/2013	6/24/2013	Central Coast California	WECC	Severe Weather - Fog	Unknown	148,000					
6/24/2013	6/25/2013	Illinois	RFC	Severe Weather - Thunderstorms	Unknown	283,451	0.01332191	2,220	1	2.2356	6/23/2013
6/24/2013	6/26/2013	Indiana	RFC	Severe Weather - Thunderstorms	Unknown	86,615	0.01218406	850	1	1.1931	6/27/2013
7/10/2013	6/28/2013	South Eastern Michigan	RFC	Severe Weather - Thunderstorms	Unknown	138,000					
7/10/2013	7/11/2013	AEP Ohio Power Footprint	RFC	Severe Weather - Thunderstorms	N/A	122,314	0.01319868	928	1	1.1982	7/10/2013
8/23/2013	8/23/2013	No Report Submitted					0.01109535	1,693	1	1.1916	8/23/2013
8/25/2013	8/25/2013	No Report Submitted					0.01172407	1,371	1	1.3877	8/25/2013
9/15/2013	9/15/2013	No Report Submitted					0.00989165	1,571	1	1.2427	9/15/2013
11/1/2013	11/1/2013	No Report Submitted					0.00908129	848	1	1.1747	11/1/2013
11/17/2013	11/20/2013	Michigan	RFC	Severe Weather - Ice and Snow Storm	Unknown	325,325					
11/17/2013	11/17/2013	Rochelle, Indiana	RFC	System-wide voltage reductions of 3 percent or more	38	7,500					
11/17/2013	11/20/2013	Central Indiana	RFC	Severe Weather - Tornadoes	535	61,705					
11/17/2013	11/21/2013	Entire Lower Peninsula Michigan	RFC	Severe Weather - Thunderstorms	Unknown	50,000					
11/17/2013	11/20/2013	Central Missouri, Central Illinois	SERC	Severe Weather - Tornadoes	Unknown	200,000					
11/17/2013	11/20/2013	North Central Indiana	RFC	Severe Weather - Thunderstorms	Unknown	75,065					
11/17/2013	11/18/2013	Indiana, Michigan	RFC	Severe Weather - Thunderstorms	Unknown	77,346					
11/17/2013	11/17/2013	Entire ComEd Territory Illinois	RFC	Severe Weather - Thunderstorms	Unknown	190,000	0.01116756	1,604	1	2.7934	11/17/2013
12/4/2013	12/4/2013	Idaho Falls Area Idaho, Utah-Idaho Border Utah	WECC	Load Shed 100+ MW	150	Unknown	0.00958207	1,905	1	3.2665	12/4/2013

[47] OE-417 E-Filing System Training Reference Guide, https://www.oe.netl.doe.gov/docs/OE417_submission_instructions.pdf

Figure 2.3 shows each day's SRI. Note that Figure 2.3 presents the historic top-10 days with an Event ID label that refers to column 1 of Table 2.3. A general normal range of performance can be established from historic data. Days that were extreme can be detected by their deviation from that normal level. During 2013, there do not appear to be as many extreme days as have occurred in prior years.

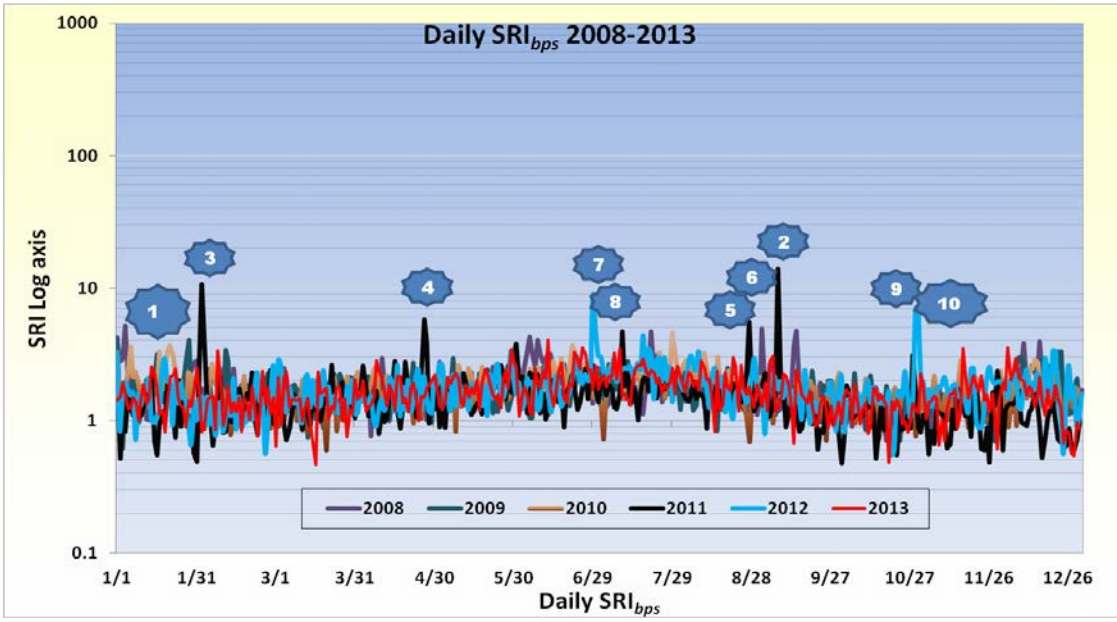


Figure 2.3: NERC Daily SRI (2008–2013)

Table 2.3: Top-10 SRI$_{bps}$ Days (2008-2013)

Event ID	Date	Event Ranking	SRI bps	Description
1	1/4/2008	8	5.30	Winter Storm
2	9/1/2008	9	4.90	Hurricane Ike
3	2/2/2011	2	10.80	Cold Weather Event
4	4/27/2011	6	5.80	Tornadoes, Severe Storm
5	8/28/2011	7	5.60	Hurricane Irene
6	9/8/2011	1	14.00	Southwest Blackout
7	6/29/2012	3	8.90	Thunderstorm Derecho
8	6/30/2012	10	4.70	Thunderstorm Derecho
9	10/29/2012	5	7.00	Hurricane Sandy
10	10/30/2012	4	7.20	Hurricane Sandy

Figure 2.4 shows annual cumulative performance of the BPS. If a step change occurs on the graph, it represents a stress day as measured by the SRI.

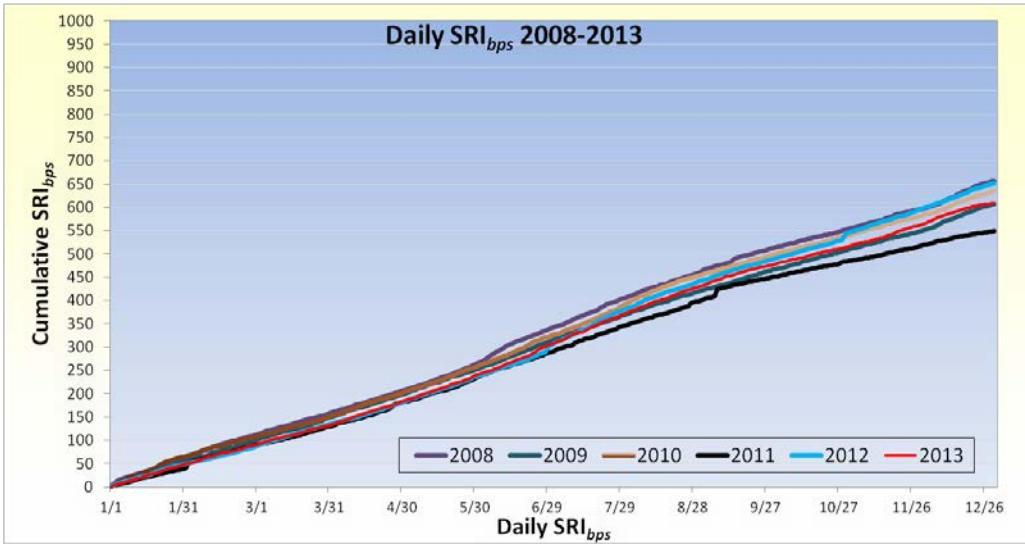


Figure 2.4: NERC Cumulative SRI (2008–2013)

Figure 2.5 breaks down the 2013 cumulative performance by BPS segment. The largest components are generation, transmission, and load loss, in that order. In Figure 2.4, the load-loss component shows day-to-day loss events but does not demonstrate any significant step changes, which was substantiated by the OE-417 data that was reviewed.

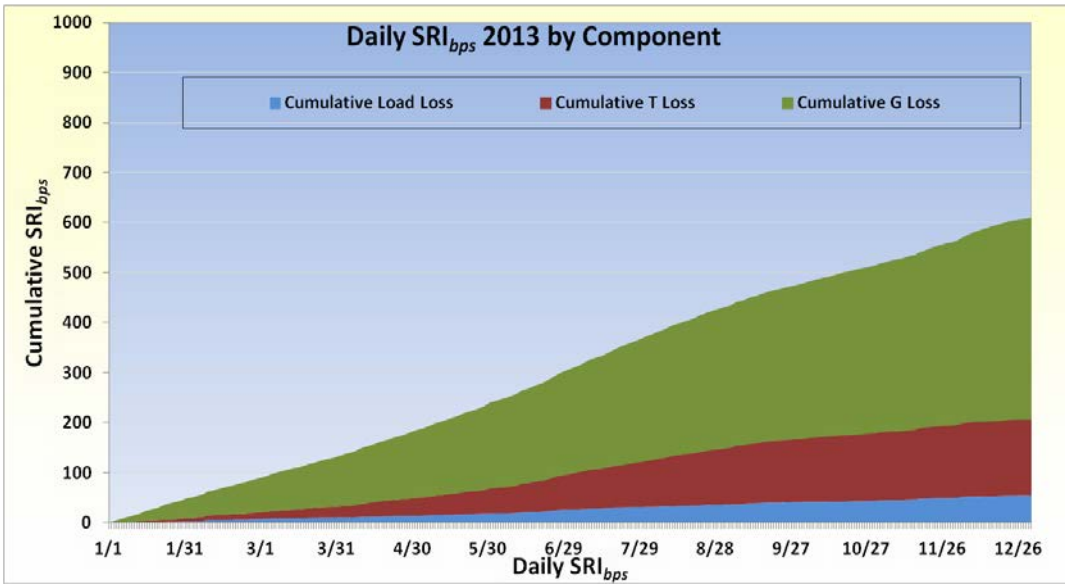


Figure 2.5: NERC Cumulative SRI by Component for 2013

Overall, 2013 had a lower SRI_{bps} score than 2008 and 2011 and was similar to 2009 and 2010. Also, the new calculation of SRI_{bps} shows that fewer stress days occurred in 2013 and that weather continues to contribute majorly to stress days. Additionally, it appears that with the modified method of calculating SRI_{bps}, generation severity plays a substantial role in the daily summary values as measured by SRI_{bps}. Future state of reliability reports will contain information assembled and analyzed from GADS, which is likely to bring greater understanding to these facilities and their role assessing the reliability of the BPS.

Chapter 3 – Risk Issue Identification and Transmission Severity Analysis

Overview

NERC uses disturbance event and equipment availability datasets to identify significant risk clusters to support making risk-informed decisions, prioritizing issues, and aligning resources to address those issues. The risk concentration areas enable NERC to identify priority projects that provide coordinated and effective solutions to identified risks to the reliability of the BPS. This chapter presents a conceptual framework using statistical analysis of transmission outage data to identify the top risks to the BPS. This transmission outage data is based on the data collected using the ICC identification provided by the NERC TADSWG. This framework and these risk analysis methods can be applied using other reliability datasets to further investigate risk concentration areas.

Based on the 2009–2013 automatic transmission outage data, the two significant risk clusters identified in this chapter are:

1. Protection system misoperations
2. AC substation equipment failure

In the *State of Reliability 2013* report, Misoperations (as an augmented ICC) were found to have the largest positive and statistically significant correlation with 2012 automatic transmission outage severity. This year's analysis shows that ac substation equipment failures now have the largest positive and statistically significant correlation with 2012–2013 automatic transmission outage severity. In addition, while these two ICCs remain the most statistically significant correlation with 2013 automatic transmission outage severity, the expected transmission severity associated with each of these ICCs has decreased from 2012's findings.

Failed AC Substation Equipment as an ICC was found statistically significant and positively correlated with 2009–2013 automatic transmission outage severity. Events initiated by Failed AC Substation Equipment are the largest contributor to the 2009–2013 transmission severity, excluding weather-related and unknown events. Chapter 5 contains a discussion of event analysis that shows that circuit breaker failures were reported as the most often failed equipment inside ac substations. A deeper investigation into the root causes of circuit breaker failures that contribute to disturbance events continues to be a high priority.

NERC is in the process of revising a number of Reliability Standards involving protection systems.[48] In addition, NERC has documented lessons learned from Generator Owners (GOs) and Transmission Owners (TOs) that achieve high protection system performance. In 2014, NERC staff is coordinating with the North American Transmission Forum to find ways to reduce protection system misoperations and develop ways to minimize the impact of misoperations.

Study Method

Defining BPS Impact from Transmission Risk

As described in Chapter 2, the SRI was developed to quantitatively compare events. The SRI is the calculation of a daily index that includes a component related to transmission system outages. The TADS outage data is used to populate the transmission outage impact component of the SRI. Since transmission outages are a significant contributor to the SRI, this chapter focuses on categorizing the individual transmission events based on TADS outage ICCs. A complete description of this methodology is contained in Appendix A.

[48] http://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx

Determining Initiating Causes and Probability

TADS events are categorized by ICCs. The ICCs facilitate the study of cause-effect relationships between each event's ICC and the severity of the event. As shown in Figure 3.1, for single-mode outage TADS events, the outage ICC is selected for the event's ICC. For common or dependent-mode TADS events, logical rules were applied to determine the initiating outage. The ICC is used to determine the event's ICC.

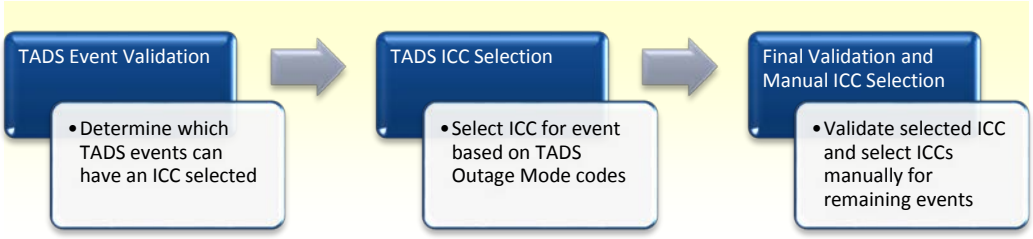


Figure 3.1 TADS Event Initiating Cause Code Selection Procedure

For TADS events initiated by a common cause, the probability[49] of observing the initiation of an event during a given hour is estimated using the corresponding historical event occurrences reported in TADS. Namely, the probability of the occurrence of the event is the total number of a given type of event observed during the historical data period divided by the total number of hours in the same period. Therefore, the sum of the estimated probabilities for all events is equal to the estimated probability of any event during a given hour. With the development of the transmission severity measure and TADS event ICCs, it is possible to statistically analyze the most recent five years of TADS data (2009–2013). The analysis shows which ICCs result in the highest transmission severity and finds significant changes in transmission severity by ICC over time.

Determining Relative Risk

Studies were performed to determine the correlation between each ICC and transmission severity, and whether a statistically significant confidence level could be established. This process is demonstrated in Figure 3.2. Then, sample distributions were studied to determine any statistically significant pair-wise differences in expected transmission severity between ICCs, including a time trend analysis where applicable. Finally, the relative risk was calculated for each ICC group. A description of this methodology is provided in Appendix A.

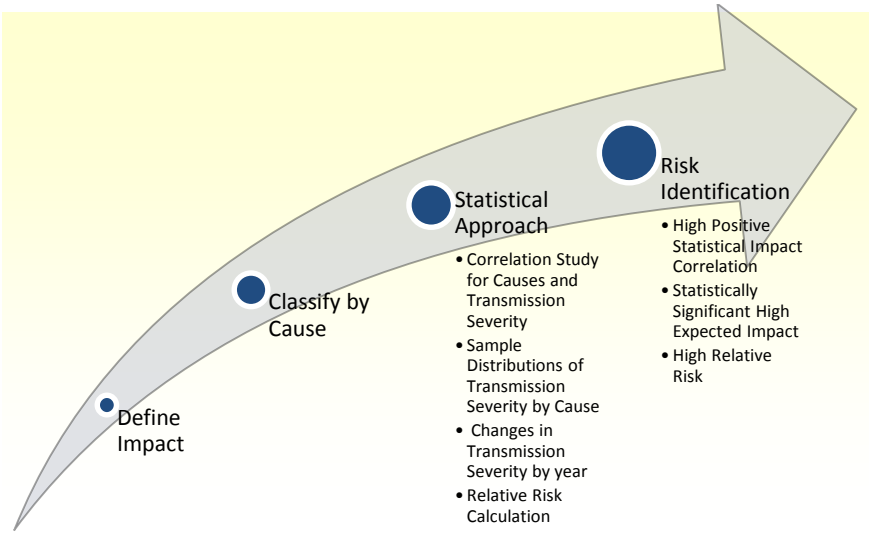


Figure 3.2: Risk Identification Method

[49] Probability is estimated using event occurrence frequency of each ICC type without taking into account the event duration.

Risk Identification Findings

2009–2013 Combined Study

TOs provide transmission performance information using the NERC TADS process. The data used in these studies includes momentary and sustained automatic outages of ac transmission circuits (overhead and underground) that operate at voltages greater than or equal to 200 kV.

Table 3.1 lists a total count of TADS events by ICC for 2009–2013. The three largest groups of events correspond to the following ICCs: Lightning, Unknown, and Weather Excluding Lightning. The next four groups of events are initiated by Human Error, Failed AC Circuit Equipment, Failed AC Substation Equipment, and Failed Protection System Equipment.

Table 3.1: TADS Outage Events by ICC (2009–2013)

Initiating Cause Code	2009	2010	2011	2012	2013	2009–2013
Lightning	789	741	822	852	814	**4018**
Unknown	673	821	782	710	712	**3698**
Weather Excluding Lightning	534	673	539	446	434	**2626**
Human Error	291	305	291	307	280	**1474**
Failed AC Circuit Equipment	257	277	306	261	248	**1349**
Failed AC Substation Equipment	266	238	289	248	192	**1233**
Failed Protection System Equipment	229	234	234	226	188	**1111**
Foreign Interference	199	173	170	170	181	**893**
Contamination	96	145	132	160	152	**685**
Power System Condition	112	74	121	77	109	**493**
Fire	92	84	63	106	130	**475**
Other	107	84	91	104	64	**450**
Vegetation	29	27	44	43	36	**179**
Vandalism, Terrorism, or Malicious Acts	4	6	5	10	9	**34**
Environmental	5	11	5	4	8	**33**
Failed AC/DC Terminal Equipment	1	2	0	0	0	**3**
All TADS Events	**3705**	**3917**	**3934**	**3753**	**3557**	**18866**
All with ICC Assigned	**3684**	**3895**	**3894**	**3724**	**3557**	**18754**

Almost all ICC groups have a sample size sufficient to be used for statistical analysis. However, four ICCs (Vegetation; Vandalism, Terrorism, or Malicious Acts; Environmental, and Failed AC/DC Terminal Equipment) have an insufficient sample size and are grouped together in this report and labeled “Combined Smaller ICC groups” for statistical analysis. They are then compared as a group to other ICC groups and studied for annual changes in transmission severity.

Figure 3.3 shows the correlation between calculated transmission severity and each ICC. A red bar in Figure 3.3 corresponds to an ICC that has a statistically significant positive correlation with transmission severity; a green bar corresponds to an ICC that has a statistically significant negative correlation; and a blue bar corresponds to an ICC that is not statistically significant. A statistically significant positive correlation of ICC with transmission outage severity would indicate a higher likelihood that an event with this ICC will result in a higher transmission outage severity. A statistically significant negative correlation indicates the contrary; in this case, a lower transmission outage severity would be likely. If a correlation is not statistically significant, this implies that a positive or negative correlation was very likely observed by mere chance, and there is, in fact, no linear relationship between ICC and the transmission outage severity. The events with this ICC have the expected transmission severity similar to all other events from the database.

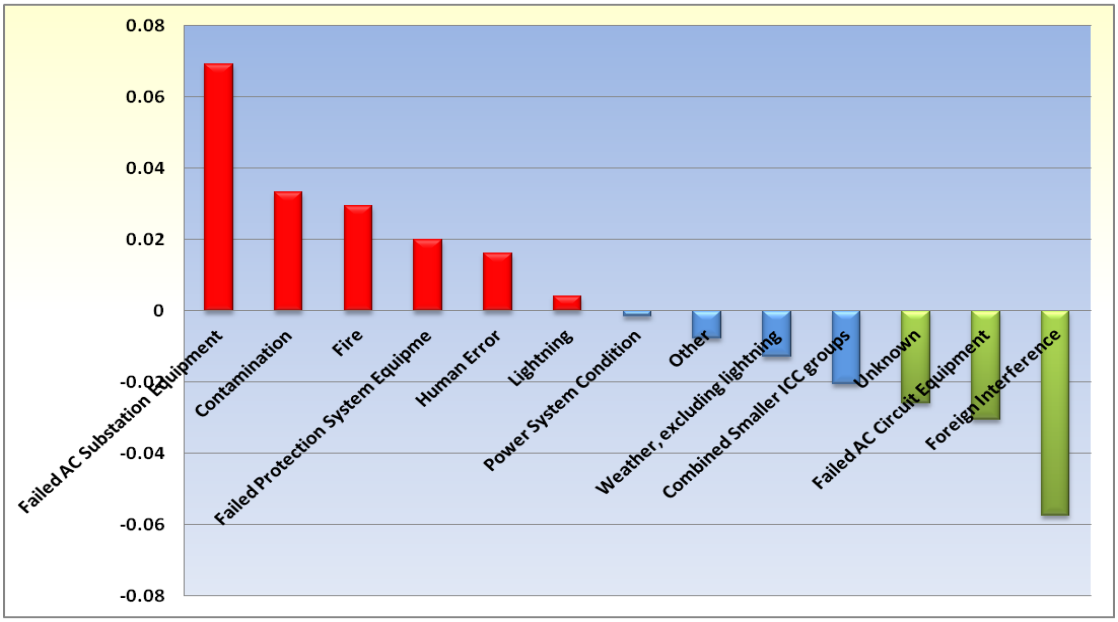


Figure 3.3: Correlation between ICC and TS of TADS Events (2009–2013)

Failed AC Substation Equipment is found to have the largest and most statistically significant positive correlation with 2009–2013 automatic transmission outage severity. In other words, 2009–2013 TADS events initiated by this cause tended to result in higher transmission severity than all other TADS events that occurred from 2009 to 2013.

Table 3.2 provides the transmission risk of each ICC as the product of the probability of the ICC event and its calculated transmission severity. The risk is then expressed as a percentage for each ICC relative to the other ICCs. As shown in Table 3.2, events related to weather represent the largest percentage of transmission severity. These are provided in two ICC groups in TADS: Lightning, and Weather Excluding Lightning. TADS events with an ICC of Lightning result in the greatest combined transmission severity for all TADS events. These Lightning events are typically momentary, single-mode outages and restore quickly, so therefore are not a significant impact to overall system reliability. Weather Excluding Lightning was found not to have a statistically significant correlation with transmission severity.

Table 3.2: Evaluation of ICC Relative Risk (2009–2013)

Group of TADS Events	Probability that an Event from a Group Starts during a Gven Hour	Expected Impact (Expected Transmission Severity of an Event)	Risk Associated with a Group Per Hour	Relative Risk by Group (%)
Lightning	0.092	0.164	0.015	21.3
Unknown	0.084	0.158	0.013	18.8
Weather Excluding Lightning	0.060	0.160	0.010	13.6
Human Error	0.034	0.169	0.006	8.0
Failed AC Substation Equipment	0.028	0.191	0.005	7.6
Failed AC Circuit Equipment	0.031	0.152	0.005	6.6
Failed Protection System	0.025	0.172	0.004	6.2
Contamination	0.016	0.182	0.003	4.0
Foreign Interference	0.020	0.136	0.003	3.9
Fire	0.011	0.183	0.002	2.8
Power System Condition	0.011	0.163	0.002	2.6
Other	0.010	0.158	0.002	2.3
Combined Smaller ICC groups	0.006	0.144	0.001	1.2
All TADS Events	**0.430**	**0.165**	**0.071**	**100.0**
All with ICC Assigned	**0.428**	**0.164**	**0.070**	**98.8**

Among non-weather-related ICCs (excluding Unknown), Human Error and Failed AC Substation Equipment are the two largest contributors to transmission severity. These two are tracked through closely related adequate level of reliability (ALR) metrics. As shown in Figure 3.3, TADS events initiated by either of these two causes have statistically significant greater expected severity than TADS non-weather ICC events. This is because a single substation element (equipment) failure may lead to multiple line outages on lines emanating from the same substation bus or end point. Therefore, the ac substation equipment failure would have the potential to substantially impact multiple locations. Further investigation into the Human Error ICC has led to a revision of the ICC data summary in the *State of Reliability 2013* report. Starting in 2012, more granular code data is available, and the ICC data summaries were modified, or augmented, as described in the following section of this chapter.

Finally, a series of statistical tests determined that both the average transmission severity of an event and the total transmission severity of TADS events in 2013 were statistically significantly smaller than in any other year from 2009 to 2012. Details of the statistical analysis of annual changes for the entire database as well as by ICC are described in Appendix A.

2012–2013 Study with Augmented Event Types

TADS event type reporting was modified in 2012 to further distinguish normal clearing events from abnormal clearing events. Components of the Human Error ICC are subdivided by type codes, which first became available in 2012. For the purpose of the report, two specific components related to protection system misoperation have

been removed from the Human Error ICC and added to the ICC for Failed Protection System Equipment. This augmented ICC is labeled "Misoperation." To introduce the additional data into this study where this level of detail is not available for prior years, TADS events with protection system misoperations—event types 61 dependability[50] (failure to operate) and 62 security[51] (unintended operation)—are used to modify (or augment) ICCs as shown in Table 3.3. The new Misoperation ICC is analogous to protection system misoperations, which are comprised of Failed Protection System Equipment (FPSE) and Human Error (HE) with event type 61 or 62 (HE and Type 61/62). Aggregate totals of 2012–2013 TADS events by augmented ICC are provided in Table 3.3. Events initiated by Misoperations comprise 8.2 percent of all TADS events and represent the fourth-largest group of events (after weather-related and Unknown ICCs.) Chapter 3's transmission analysis covers the most recent five-year period. After three more years of data collection, the augmented ICC data collection method will have a full five years of data and will become the method used for studying the TADS event data.

Table 3.3: TADS Outage Events by Augmented ICC (2012–2013)

Initiating Cause Code	2012	2013	2012–2013
Lightning	852	813	1665
Unknown	710	712	1422
Weather Excluding Lightning	446	433	879
Misoperation: FPSE OR (HE AND Type 61/62)	321	281	602
Failed AC Circuit Equipment	261	248	509
Failed AC Substation Equipment	248	191	439
Human Error AND NOT (Type 61 OR Type 62)	212	191	403
Foreign Interference	170	181	351
Contamination	160	151	311
Fire	106	130	236
Power System Condition	77	109	186
Other	104	64	168
Vegetation	43	36	79
Vandalism, Terrorism, or Malicious Acts	10	9	19
Environmental	4	8	12
All with ICC Assigned	**3724**	**3557**	**7281**
In TADS	**3753**	**3557**	**7310**

[50] Event Type 61 Dependability (failure to operate): one or more automatic outages with delayed fault clearing due to failure of a single protection system (primary or secondary backup) under either of these conditions:

- Failure to initiate the isolation of a faulted power system Element as designed, or within its designed operating time, or
- In the absence of a fault, failure to operate as intended within its designed operating time.

[51] Event Type 62 Security (unintended operation): one or more automatic outages caused by improper operation (e.g., overtrip) of a protection system resulting in isolating one or more TADS elements it is not intended to isolate, either during a fault or in the absence of a fault.

Figure 3.4 shows the correlation between calculated transmission severity and each ICC in the same format as Figure 3.3. Using this augmented ICC data, Failed AC Substation Equipment and Misoperations had the largest and most statistically significant positive correlation with 2012–2013 ATO severity. In other words, TADS events initiated by these two causes tended to have higher transmission severity than other TADS events that occurred in 2012 and 2013. Power System Condition is the only other ICC with a statistically significant correlation to transmission severity, but the correlation is much smaller than Failed AC Substation Equipment and Misoperations. Therefore, the remaining discussion won't focus on TADS data from 2012 and 2013.

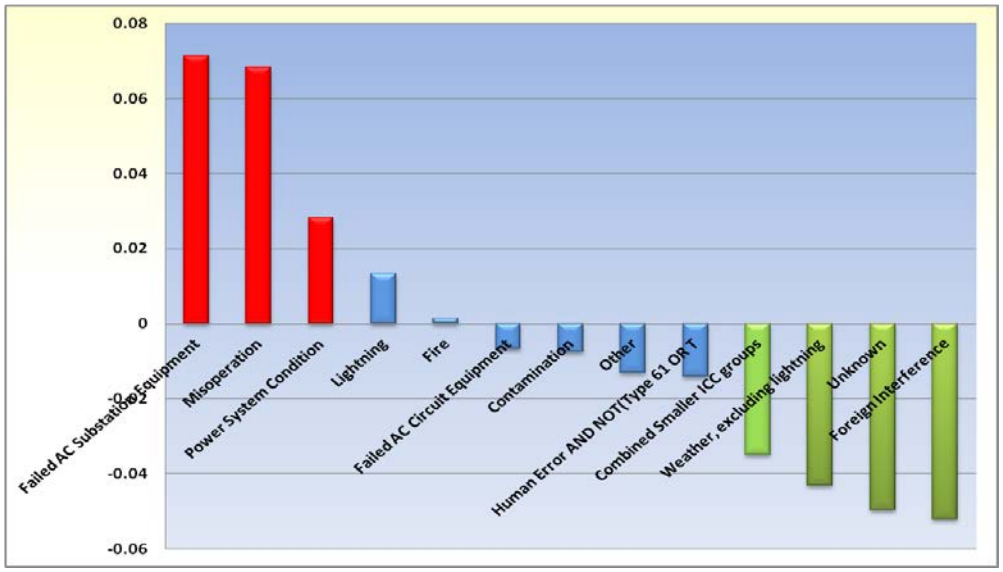


Figure 3.4: Correlation between Augmented ICC and TS of TADS Events (2012–2013)

Relative risk of the 2012–2013 TADS events by augmented ICC is listed in Table 3.4. The probability that an event from a given group initiated during a given hour is estimated from the frequency of the events of each type without taking into account the event duration. Excluding weather-related and Unknown events, events initiated by Misoperations and by Failed AC Substation Equipment had the largest shares in the total transmission severity and contributed 9.4 and 7.1 percent, respectively, to transmission severity relative risk.

Table 3.4: Relative Risk by Augmented ICC (2012–2013)

Group of TADS Events	Probability that an Event from a Group Starts during a Given Hour	Expected Impact (Expected Transmission Severity of an Event)	Risk Associated with a Group Per Hour	Relative Risk by Group (%)
Lightning	0.095	0.155	0.015	**23.1**
Unknown	0.081	0.143	0.012	**18.2**
Weather Excluding Lightning	0.050	0.143	0.007	**11.2**
Misoperation	0.034	0.175	0.006	**9.4**
Failed AC Substation Equipment	0.025	0.180	0.005	**7.1**
Failed AC Circuit Equipment	0.029	0.151	0.004	**6.9**
Human Error AND NOT(Type 61 OR Type 62)	0.023	0.150	0.003	**5.4**
Contamination	0.018	0.149	0.003	**4.2**
Foreign Interference	0.020	0.130	0.003	**4.1**
Fire	0.013	0.154	0.002	**3.2**
Power System Condition	0.011	0.170	0.002	**2.8**
Other	0.010	0.145	0.001	**2.2**
Combined Smaller ICC groups	**0.006**	**0.126**	**0.001**	**1.2**
All TADS Events	**0.417**	**0.153**	**0.064**	**100.0**
All with ICC Assigned	**0.415**	**0.152**	**0.063**	**99.1**

Focusing the statistical analysis of the 2012–2013 TADS augmented ICC data on the transmission severity and initiating causes of TADS events, and aligning that information with misoperations, yields the following results and observations:

- After excluding weather-related and Unknown ICCs, Misoperations and Failed AC Substation Equipment are the two largest contributors to the transmission severity risk.
- TADS events initiated by either of these ICCs have greater severity than all other TADS events.
- Among other ICCs, only Power System Condition[52] has a statistically significant positive correlation with transmission severity, but events initiated by this cause are infrequent and together contribute only 2.8 percent to the total transmission severity of the 2012–2013 TADS.

Common/Dependent Mode Event ICC Study (2009–2013)

TADS data also provides information to classify outages as single-mode or common or dependent mode (CDM) events that should be evaluated separately from single-mode events. CDM events result in multiple transmission element outages. It is important to monitor and understand CDM events due to their potential risk to system reliability.

Table 3.5 lists CDM events by ICC in the 2009–2013 database and their percentages with respect to all TADS events with a given ICC. Similar to all TADS events, Lightning initiated the largest number of CDM events. CDM events initiated by Failed AC Substation Equipment comprise the second largest group, followed by Weather Excluding Lightning and Human Error. Overall, 3,227 CDM events were defined, representing 17.1 percent of all TADS events from 2009 to 2013. Out of these, 3,136 are assigned to one of the 17 ICCs.

Table 3.5: CDM Events and Hourly Event Probability by ICC (2009–2013)

Initiating Cause Code	ALL TADS Events	CDM Events	CDM as % of ALL	Event Probability/Hour
Reliability Metrics	**5167**	**1249**	**24.2**	**0.0285**
Failed AC Substation Equipment	1233	444	36.0	0.0101
Failed Protection System Equipment	1111	296	26.6	0.0068
Human Error	1474	324	22.0	0.0074
Failed AC Circuit Equipment	1349	185	13.7	0.0042
Lightning	4018	559	13.9	0.0128
Weather Excluding Lightning	2626	334	12.7	0.0076
Unknown	3698	306	8.3	0.0070
Power System Condition	493	310	62.9	0.0071
Other	450	109	24.2	0.0025
Foreign Interference	893	97	10.9	0.0022
Fire	475	77	16.2	0.0018
Contamination	685	59	8.6	0.0013
Combined Smaller ICC groups	**249**	**36**	**14.5**	**0.0008**
Vegetation	179	14	7.8	0.0003
Environmental	33	11	33.3	0.0003
Failed AC/DC Terminal Equipment	3	3	100.0	0.0001
Vandalism, Terrorism, or Malicious Acts	34	8	23.5	0.0002
All In TADS	**18866**	**3227**	**17.1**	**0.0736**
All with ICC Assigned	**18754**	**3136**	**16.7**	**0.0716**

[52] Defined as "Automatic Outages caused by power system conditions such as instability, overload trip, out-of-step, abnormal voltage, abnormal frequency, or unique system configurations (e.g., an abnormal terminal configuration due to existing condition with one breaker already out of service)."

Almost all ICC groups of CDM events for five years have a sufficient sample size to be used in a statistical analysis, but the sample size is not enough to track statistically significant year-over-year changes in transmission severity. Four ICCs (Vegetation; Vandalism, Terrorism, or Malicious Acts; Environmental, Failed AC/DC Terminal Equipment) must be combined to comprise a new group, Combined Smaller ICC Groups, that can be statistically compared to every other group.

Figure 3.5 shows the correlation between calculated transmission severity and each ICC in the same format as Figure 3.3.

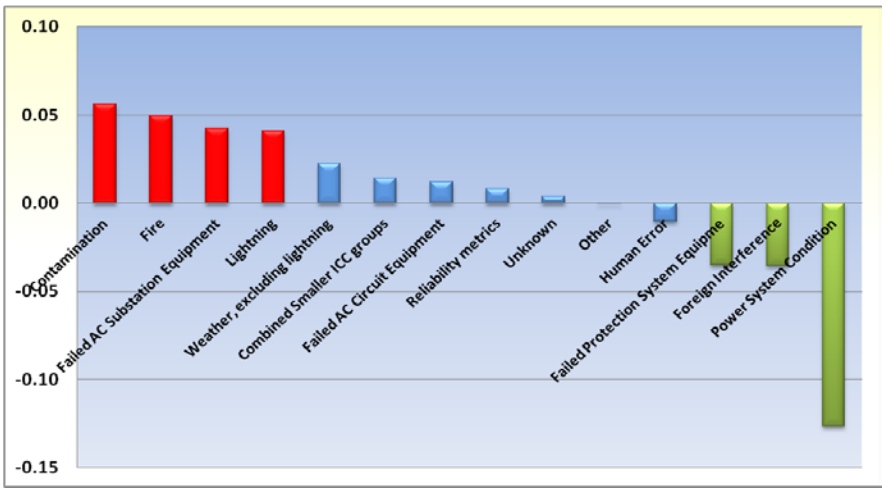


Figure 3.5: Correlation between ICC and TS of TADS CDM Events (2009–2013)

CDM events are a subset of the previously evaluated TADS events. Table 3.6 provides a breakdown of relative risk of CDM events by ICC.

Table 3.6: Evaluation of CDM Event ICC Contribution to Transmission Severity (2009–2013)

Group of TADS Events	Probability that an Event from a Group Starts during a Given Hour	Expected Impact (Expected Transmission severity of an event)	Risk Associated with a Group Per Hour	Relative Risk by Group (%)
CDM Lightning	0.013	0.258	0.003	4.6
CDM Failed AC Substation Equipment	0.010	0.261	0.003	3.7
CDM Weather Excluding Lightning	0.008	0.253	0.002	2.7
CDM Human Error	0.007	0.236	0.002	2.5
CDM Unknown	0.007	0.244	0.002	2.4
CDM Failed Protection System Equipment	0.007	0.221	0.001	2.1
CDM Power System Condition	0.007	0.170	0.001	1.7
CDM Failed AC Circuit Equipment	0.004	0.250	0.001	1.5
CDM Other	0.002	0.241	0.001	0.8
CDM Fire	0.002	0.300	0.001	0.7
CDM Foreign Interference	0.002	0.204	0.000	0.6
CDM Contamination	0.001	0.317	0.000	0.6
CDM Combined Smaller ICC groups	0.001	0.257	0.000	0.3
All TADS Events	**0.430**	**0.165**	**0.071**	**100.0**
All CDM Events	**0.074**	**0.244**	**0.018**	**25.4**
All with ICC assigned	**0.072**	**0.241**	**0.017**	**24.4**

Analysis of the TADS CDM events indicated that events with ICCs of Failed AC Substation Equipment and Human Error are the two largest contributors to transmission severity with the exception of weather-related events. CDM events initiated by Failed AC Substation Equipment have statistically greater expected severity than other CDM events; however, the difference in transmission severity of CDM events initiated by Human Error and all other CDM events is not statistically significant. In other words, CDM events initiated by Human Error on average have the same transmission severity as all the other CDM events that occurred between 2009 and 2013.

Summary of Analysis

Figure 3.6 represents an analysis of the risk profile of the 2009–2013 TADS events combined study. The horizontal axis is the magnitude of the correlation of a given ICC with transmission severity. The vertical axis represents the expected transmission severity of an event when it occurs. The color of the marker indicates if there is a correlation of transmission severity with the given ICC (either positive - Red, negative - Green, or no significant correlation- Blue). The size of the marker indicates the probability of an event initiating in any hour with a given ICC. Failed AC Substation Equipment shows a statistically significant positive correlation of transmission severity and a higher relative transmission risk based on the probability of a failure initiating in any hour and the expected transmission severity when it occurs. Human error and failed protection system equipment both show a statistically significant positive correlation of transmission severity but individually show a moderately higher relative transmission risk. Fire, while showing a positive correlation of transmission severity, has a low relative transmission risk.

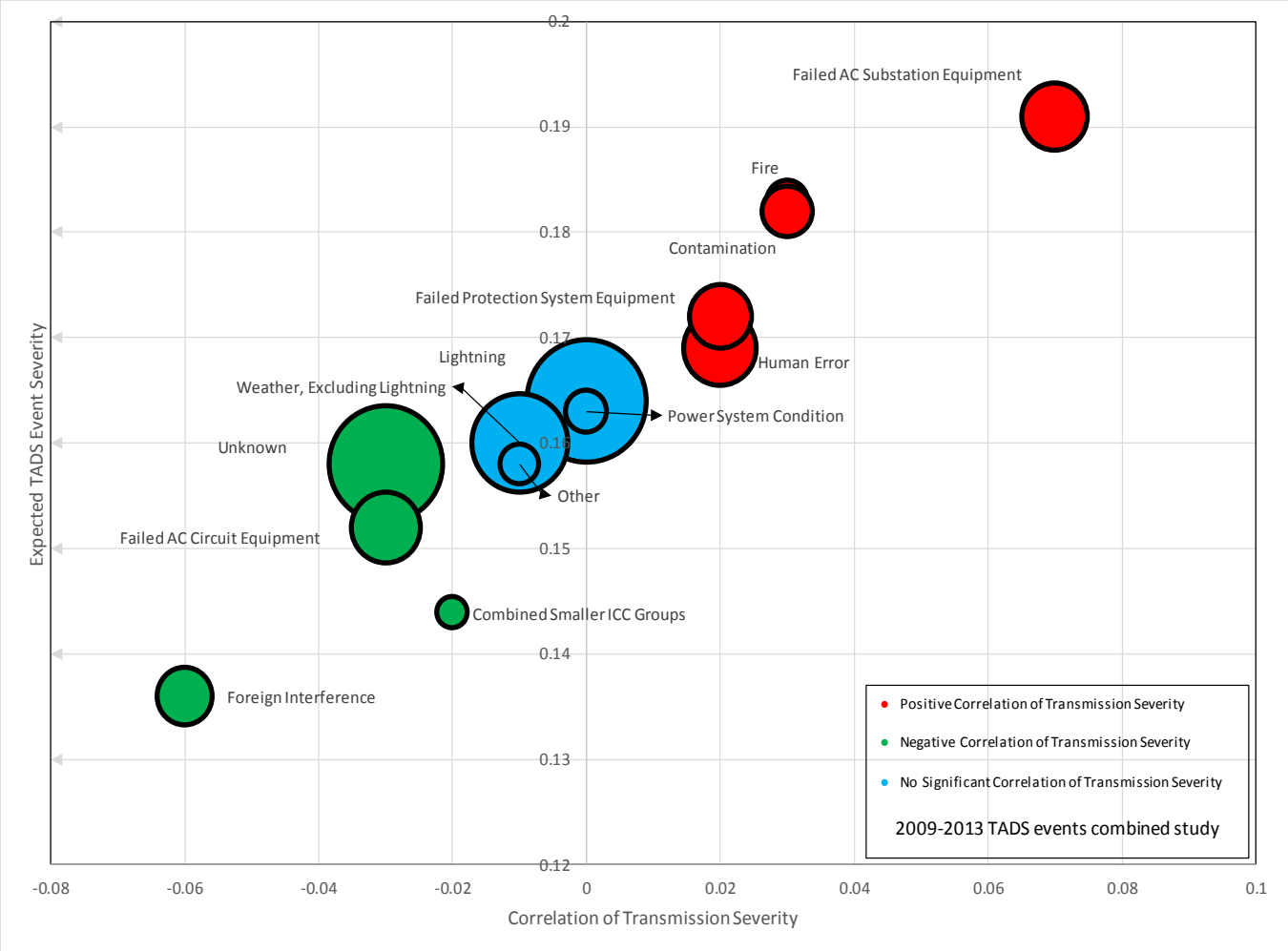


Figure 3.6: Risk Profile of the 2009–2013 TADS Events Combined Study

Figure 3.7 represents an analysis of the risk profile of the 2012–2013 study with augmented event types (augmented to further distinguish normal clearing events from abnormal clearing events). The parameters for the chart remain the same as in Figure 3.6. With the introduction of the Misoperation ICC (which combines Failed Protection System Equipment and Human Error associated with Misoperations), Failed AC Substation Equipment and Misoperations both show a statistically significant positive correlation with transmission severity and show a higher relative transmission risk. Power System Condition, while showing a positive correlation of transmission severity, has a lower relative transmission risk, based on the probability of this TADS event initiating in any hour and its expected transmission severity. On the other end of the risk spectrum, Lightning shows a high relative transmission risk but has no significant correlation with transmission severity.

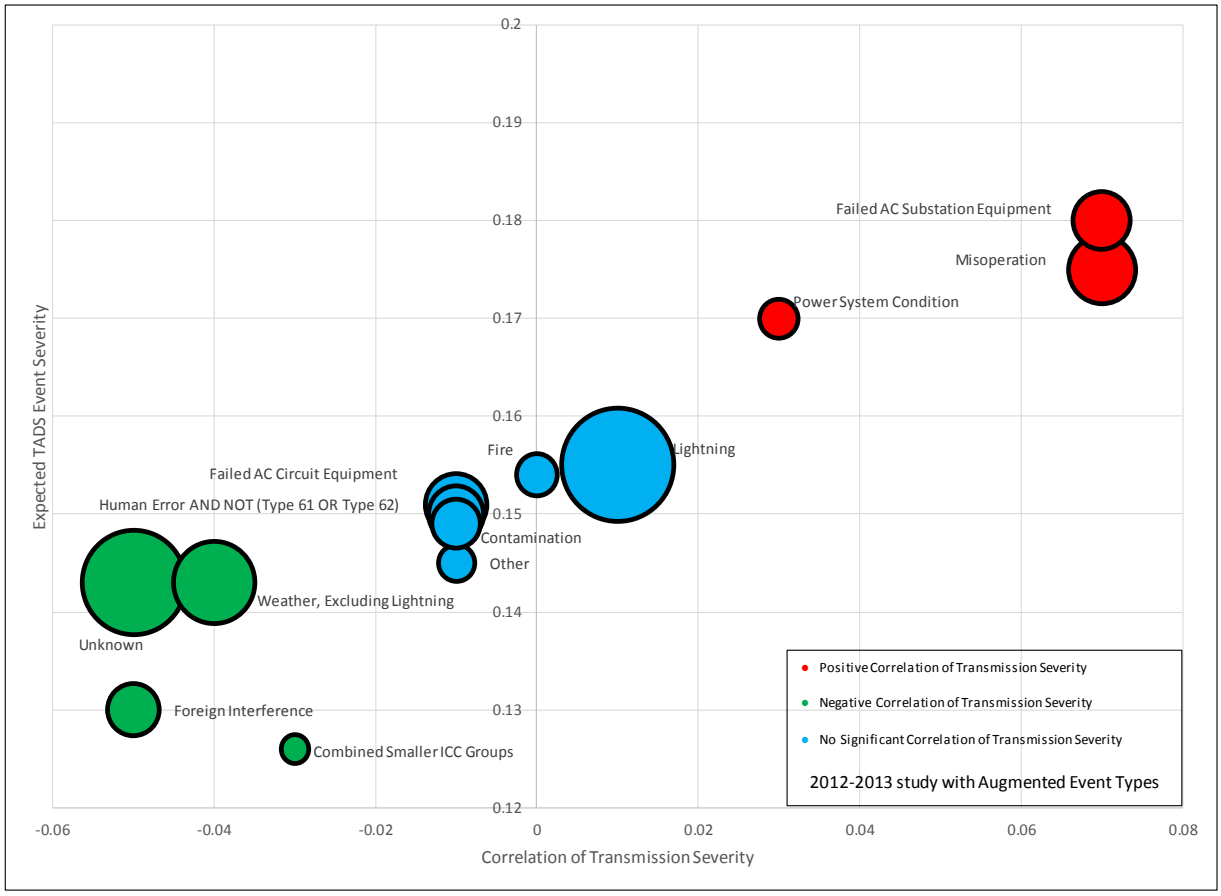


Figure 3.7: Risk Profile of the 2012–2013 TADS Events by Augmented ICC

Figure 3.8 represents an analysis of the risk profile of the 2009–2013 Common/Dependent Mode Event ICC Study. The parameters for the chart remain the same as in Figure 3.6 and Figure 3.7. Failed AC Substation Equipment and Lightning both show a statistically significant positive correlation with transmission severity and show a higher relative transmission risk. On the other end of the risk spectrum, Weather Excluding Lightning shows a high relative transmission risk but has no significant correlation with transmission severity.

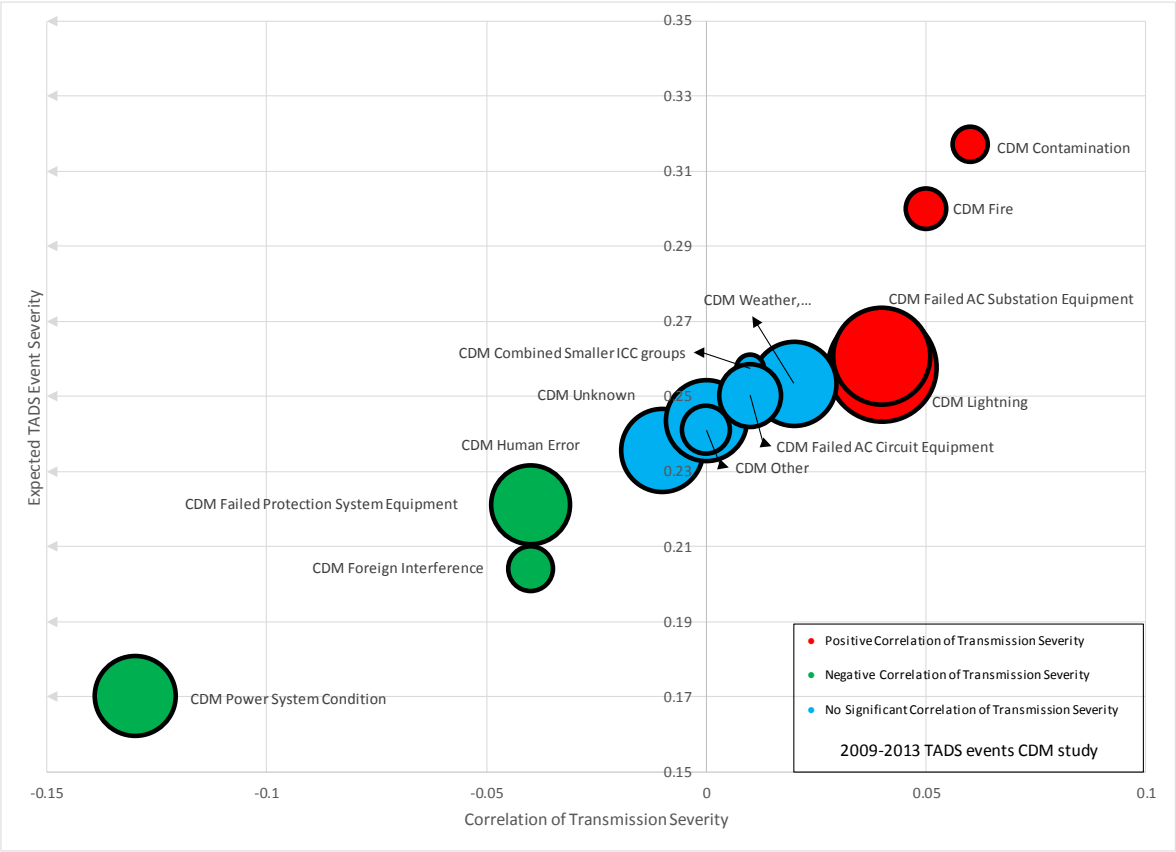


Figure 3.8: Risk Profile of the 2009–2013 Common/Dependent Mode Event ICC Study

Focusing the statistical analysis of the 2012–2013 TADS data on the transmission severity and initiating causes of TADS events and aligning that information with misoperations yields the following results and observations:

- After excluding weather-related and Unknown ICCs, Misoperations and Failed AC Substation Equipment are the two largest contributors to transmission severity risk.
- TADS events initiated by either of these ICCs have statistically significant greater expected severity than all other TADS events.
- Among other ICCs, only Power System Condition has a statistically significant positive correlation with transmission severity, but events initiated by this cause are less frequent and together contribute only 2.8 percent to the total transmission severity of the 2012–2013 TADS.
- Statistical tests resulted in the conclusion that both the average transmission severity of the events initiated by Misoperations and their total transmission severity significantly decreased in 2013 versus 2012.
- Based on the five-year statistical analysis, the average and total transmission severity and the relative transmission risk of Failed AC Substation Equipment significantly decreased in 2013, compared with 2011 and 2012.

Chapter 4 – Reliability Indicator Trends

Reliability Indicator Trends – Summary

NERC reliability indicators are intended to tie the actual performance of the BES to the set of specified objectives and outcomes for the NERC reliability objectives to measure whether an adequate level of reliability exists. Based on the events that occurred in 2013 and the metrics data analyzed, the system shows a continuing trend toward maintaining reliability. In other words, the system experienced a wide range of operating conditions and the BES operated as planned and designed.

One of the stated purposes for the new ALR definition is for the NERC PAS to assess BES reliability and identify gaps in data collection. In 2013, the PAS focused on aligning the existing ALR reliability indicators with the new ALR definition.[53] Table 4.1 shows the mapping of the 16 metrics monitored in 2013 to the seven reliability performance objectives of the new ALR definition. With the revised ALR definition that was approved in 2012, the existing metric naming convention no longer maps well to the objectives in the ALR definition. Therefore, the PAS is recommending a new naming convention for the existing 16 metrics, shown in parentheses below.

Table 4.1 Adequate Level of Reliability Metrics

Reliability Performance Objectives	System Stability	System Frequency	System Voltage	Manage Contingencies	Coordinate Restoration	Transmission Adequacy	Resource Adequacy
ALR Metrics (New ID)	ALR1-4 (M-2) ALR1-12 (M-4) ALR4-1 (M-9)	ALR1-12 (M-4) ALR2-4 (M-6)	ALR1-5 (M-3)	ALR1-4 (M-2) ALR2-3 (M-5) ALR2-4 (M-6) ALR2-5 (M-7) ALR3-5 (M-8) ALR6-2 (M-11)	ALR1-4 (M-2) ALR2-3 (M-5) ALR6-2 (M-11)	ALR1-4 (M-2) ALR3-5 (M-8) ALR6-1 (M-10) ALR6-11 (M-12) ALR6-12 (M-13) ALR6-13 (M-14) ALR6-14 (M-15) ALR6-15 (M-16)	ALR1-3 (M-1) ALR6-2 (M-11)

These metrics exist within a reliability framework. The existing 16 performance metrics align with the performance objectives for the design, planning, and operation of the BES. These metrics contribute to the reliability performance objectives, which will lead to a more resilient and reliable BES. There is at least one existing performance metric associated with each of the performance objectives listed in the table.

The definition of ALR speaks to the state of the BES in which the performance objectives are met. It is therefore intuitive that one could not base such an assessment of reliability on one metric only; rather, it is necessary to look at the entire set of metrics to evaluate that the ALR state has been attained. Any comparisons of individual metrics alone or between regions should therefore be evaluated with care.

Another metric reporting principle is to retain anonymity of individual reporting organizations. Thus, details are presented in this report at a NERC level and a regional level and do not compromise anonymity of individual reporting organizations.

Process Overview

Building upon previous metric reviews, the results of the approved performance metrics continue to be assessed. Each metric is designed to provide a measure of one or more performance objectives.

[53] http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Informational_Filing_Definition_Adequate_Level_Reliability_20130510.pdf

Due to varying data availability, each of the performance metrics does not address the same time period (some metrics have just been established or modified, while others represent data collected over many years). At this time, the number of metrics is expected to remain relatively stable; however, the PAS annually reviews them. Working with industry subject matter experts, the RAS may recommend changes to metrics, or new metrics, as gaps are identified in reliability data. In 2013, such a review was performed that resulted in the retirement of two existing metrics and the modification of several others. Specific changes to metrics that were approved in 2013 and early 2014 will be described in greater detail further in this section.

Table 4.2 provides an overview of the ALR metric trends through 2013. Although a number of performance categories have been assessed, some do not yet have sufficient data to derive conclusions from the metric results. Assessment of these metrics should continue as additional data becomes available to determine if the metric is a good indicator of the performance objective it is meant to measure.

Table 4.2: Metric Trend Ratings		
ALR	System Stability	**Trend Rating**
ALR1-4 (M-2)	BPS Transmission-Related Events Resulting in Loss of Load (modified in early 2014)	◑
ALR1-12 (M-4)	Interconnection Frequency Response	◑*
ALR4-1(M-9)	Automatic Transmission Outages Caused by Failed Protection System Equipment (modified in 2013)	◑*
	System Frequency	
ALR1-12 (M-4)	Interconnection Frequency Response	◑*
ALR2-4 (M-6)	Average Percent Non-Recovery Disturbance Control Standard Events	◑*
	System Voltage	
ALR1-5 (M-3)	System Voltage Performance	◑***
	Manage Contingencies	
ALR1-4 (M-2)	BPS Transmission-Related Events Resulting in Loss of Load (modified in early 2014)	◑
ALR2-3 (M-5)	Activation of Underfrequency Load Shedding	◑**
ALR2-4 (M-6)	Average Percent Non-Recovery Disturbance Control Standard Events	◑*
ALR2-5 (M-7)	Disturbance Control Events Greater than Most Severe Single Contingency	◑*
ALR3-5 (M-8)	Interconnected Reliability Operating Limit/System Operating Limit (IROL/SOL) Exceedances (modified in 2013)	◑*
ALR6-2 (M-11)	Energy Emergency Alerts (modified in 2013)	●
	Coordinate Restoration	
ALR1-4 (M-2)	BPS Transmission-Related Events Resulting in Loss of Load (modified in early 2014)	◑
ALR2-3 (M-5)	Activation of Underfrequency Load Shedding	◑**
ALR6-2 (M-11)	Energy Emergency Alerts (modified in 2013)	●
	Transmission Adequacy	
ALR1-4 (M-2)	BPS Transmission-Related Events Resulting in Loss of Load (modified in early 2014)	◑
ALR3-5 (M-8)	Interconnected Reliability Operating Limit/System Operating Limit (IROL/SOL) Exceedances (modified in 2013)	◑*
ALR6-1 (M-10)	Transmission Constraint Mitigation	◑**
ALR6-11 (M-12)	Automatic AC Transmission Outages Initiated by Failed Protection System Equipment	◑*

ALR6-12 (M-13)	Automatic AC Transmission Outages Initiated by Human Error	◑*
ALR6-13 (M-14)	Automatic AC Transmission Outages Initiated by Failed AC Substation Equipment	◑*
ALR6-14 (M-15)	Automatic AC Transmission Outages Initiated by Failed AC Circuit Equipment	◑*
ALR6-15 (M-16)	Element Availability Percentage (modified and combined with 6-16 in 2013)	◑*
	Resource Adequacy	
ALR1-3 (M-1)	Planning Reserve Margin	◑*
ALR6-2 (M-11)	Energy Emergency Alerts (modified in 2013)	●

Trend Rating Symbols	
Significant Improvement	●
Slight Improvement	◕
No Change	◑
Inconclusive/Mixed	◑*
Slight Deterioration	◔
Significant Deterioration ⚠⚠	○
New Data	◑***
Incomplete Dataset/not enough to draw any conclusion	◑**

This chapter provides a discussion of the ALR metric trend ratings and activity on certain metrics where some changes have been implemented and which are associated to some key findings and conclusions. The full set of metrics and their descriptions, along with the results and trending, are on the NERC public website.[54]

ALR1-4 (M-2) BPS Transmission-Related Events Resulting in Loss of Load

Background

This metric measures BPS transmission-related events resulting in the loss of load, excluding weather-related outages. Planners and operators can use this metric to validate their design and operating criteria by identifying the number of instances when loss of load occurs. For the purposes of this metric and to be consistent with the revised metric approved by the OC and PC in March 2014, an "event" is an unplanned disturbance that produces an abnormal system condition due to equipment failures or system operational actions (either intentional or unintentional) that result in the loss of firm system demands. The metric analysis uses the subset of data provided by entities as specified in EOP-004-2. The reporting criteria for such events beginning with data for 2013 are outlined below:[55]

1. Loss of firm load for 15 minutes or more:

   a. 300 MW or more for entities with previous year's demand of 3,000 MW or more.

   b. 200 MW or more for all other entities.

2. BES Emergency requiring manual firm load shedding of 100 MW or more.

3. BES Emergency resulting in automatic firm load shedding of 100 MW or more (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS).

[54] Assessments & Trends: Reliability Indicator, http://www.nerc.com/pa/RAPA/Pages/ReliabilityIndicators.aspx
[55] http://www.nerc.com/pa/rrm/ea/EA Program Document Library/Final_ERO_EA_Process_V2.1.pdf

4. Transmission loss event with an unexpected loss within an entity's area, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing) resulting in a firm load loss of 50 MW or more.

This metric was reviewed in 2013, and changes were made to make the criteria more consistent with the approved changes to EOP-004-2 reporting criteria that pertain to transmission-related events that result in loss of load. The criteria presented above were approved for implementation in the first quarter of 2014. Changes in the annual measurement between 2012 and 2013 therefore reflect the addition of the new criteria applied to the 2013 data.

Assessment

Figure 4.1 shows that the number of BPS transmission-related events resulting in loss of firm load from 2002 to 2011 is relatively constant. The year 2012 was better in terms of transmission-related load loss events, with only two events having resulted in total load loss of 1,055 MW. There were fewer events in 2013 than prior years, with the exception of 2007 and 2012. On average, eight to 10 events were experienced per year. The top-three years in terms of load loss are 2003, 2008, and 2011, as shown in Figure 4.2. In 2003 and 2011, one event accounted for over two-thirds of the total load loss, while in 2008, a single event accounted for over one-third of the total load loss. In 2013, there was a lower-than-average level of load lost in megawatt-hours with total load loss less than all previous years studied except for 2012.

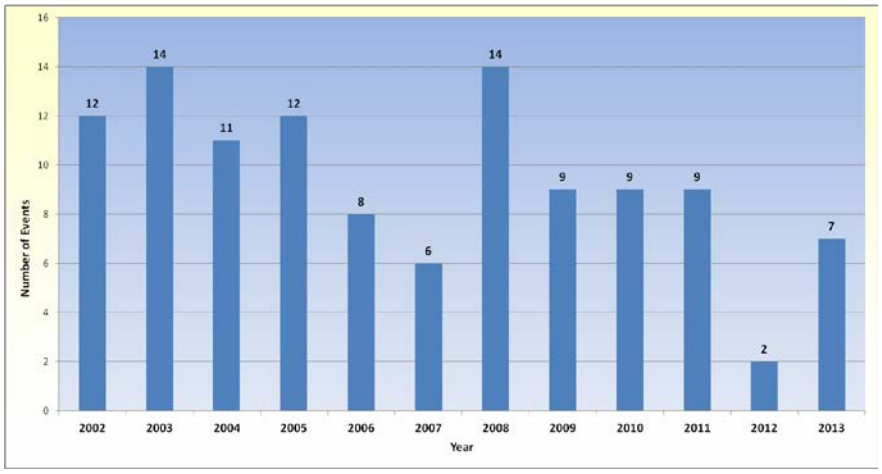


Figure 4.1: ALR1-4 BPS Transmission-Related Events Resulting in Load Loss (2002–2013)

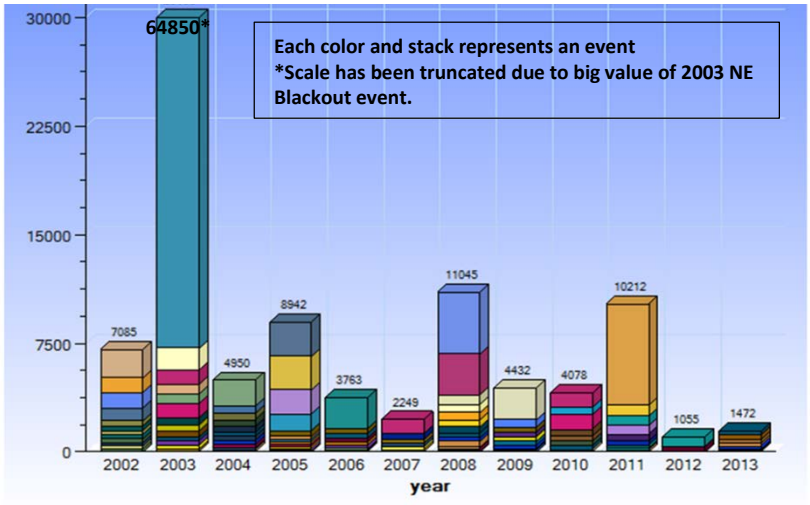


Figure 4.2: ALR1-4 BPS Transmission-Related Events Resulting in Load Loss (2002–2013)

Figure 4.3 is a new addition to this metric; it shows total megawatt loss values and duration of events resulting in firm load loss of 50 MW or greater. So, this figure shows that in addition to the seven events reported under the previous criteria, there are an additional seven events that were associated with the new criteria indicate events with load loss less than 100 MW and greater than or equal to 50 MW which is a new addition to the ALR1-4 Metric. So, while Figure 4.1 and 4.2 show 2013 transmission-related load-loss events based on the historical metric language, Figure 4.3 provides magnitude and duration of megawatt load loss for transmission-related load-loss events in 2013. It includes the new criteria in the metric to capture transmission-loss events with an unexpected loss in an entity's area of three or more BES elements (contrary to design) caused by a common disturbance (excluding successful automatic reclosing) that results in a firm load loss of 50 MW or more. Further analysis and continued assessment of the trends over time will continue in future years.

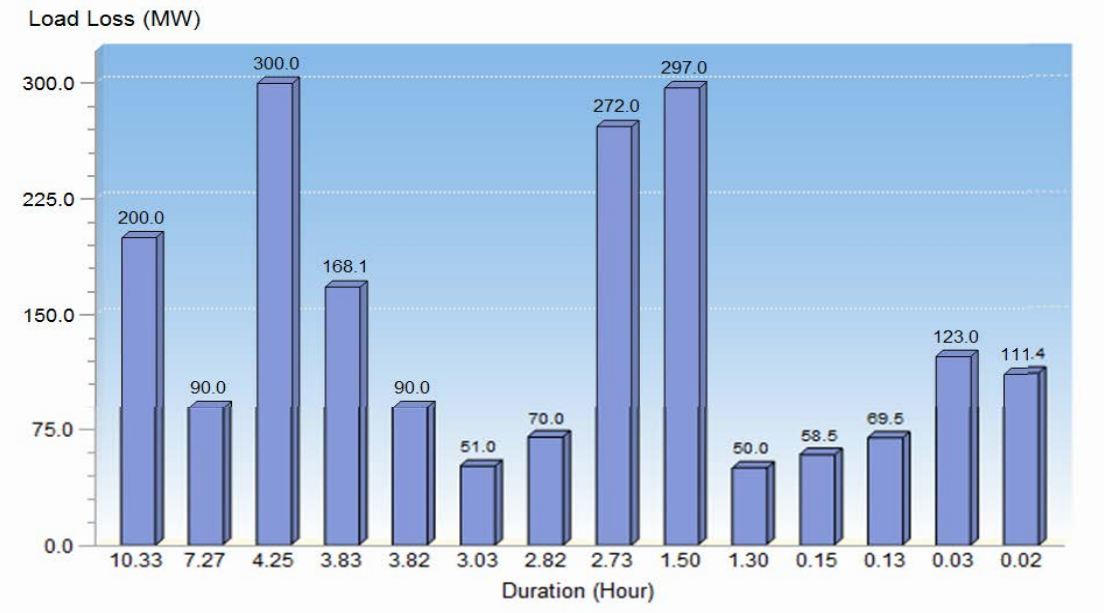


Figure 4.3: ALR1-4: 2013 Events with Load Loss ≥ 50 MW

Special Considerations

The collected data does not indicate whether load loss during an event occurred as designed or not as designed. Going forward, NERC will continue to refine data collection for this metric to allow grouping the data into categories such as separating load loss as designed versus unexpected firm load loss. NERC should support differentiating between load loss as a direct consequence of an outage and load loss as a result of operator-controlled action to mitigate an IROL/SOL exceedance.

ALR1-12 Metric Interconnection Frequency Response

Background

This metric is used to track and monitor interconnection frequency response. Frequency response is a measure of an interconnection's ability to stabilize frequency immediately following the sudden loss of generation or load. It is a critical component to the reliable operation of the BPS, particularly during disturbances. The metric measures the average frequency response for all events where frequency deviates more than the interconnection's defined threshold, as shown in Table 4.3.

The following are frequency response calculations of the Eastern Interconnection, Western Interconnection, ERCOT Interconnection, and Québec Interconnection. The frequency response should not be compared within interconnections, because their BPS characteristics differ significantly in terms of number of facilities, miles of line, operating principles, and simple physical, geographic, and climatic conditions.

Table 4.3: Frequency Event Triggers

Interconnection	ΔFrequency (mHz)	MW Loss Threshold	Rolling Windows (seconds)
Eastern	36 or Point C below 59.960 Hz and delta Hz more than 30 mHz within 15 second time window	800	15
Western	70	700	15
ERCOT	90 or Point C below 59.900 Hz or above 60.100 Hz	450	15
Québec	350	450	15

Figure 4.4 shows the criteria for calculating average values A and B used to report frequency response. The event starts at time t±0. Value A is the average from t-16 to t-2 seconds, and Value B is the average from t+20 to t+52 seconds. The difference of value A and B is the change in frequency[56] used for calculating frequency response. The monthly frequency event candidate lists are posted on the NERC Resources Subcommittee[57] website. These lists are vetted by the NERC Frequency Working Group and the final list is published on a quarterly basis. The data is used to support the frequency response standard BAL-003 – Frequency Response and Bias. The frequency event data collection process is described in the BAL-003 Frequency Response Standard Supporting Document.[58]

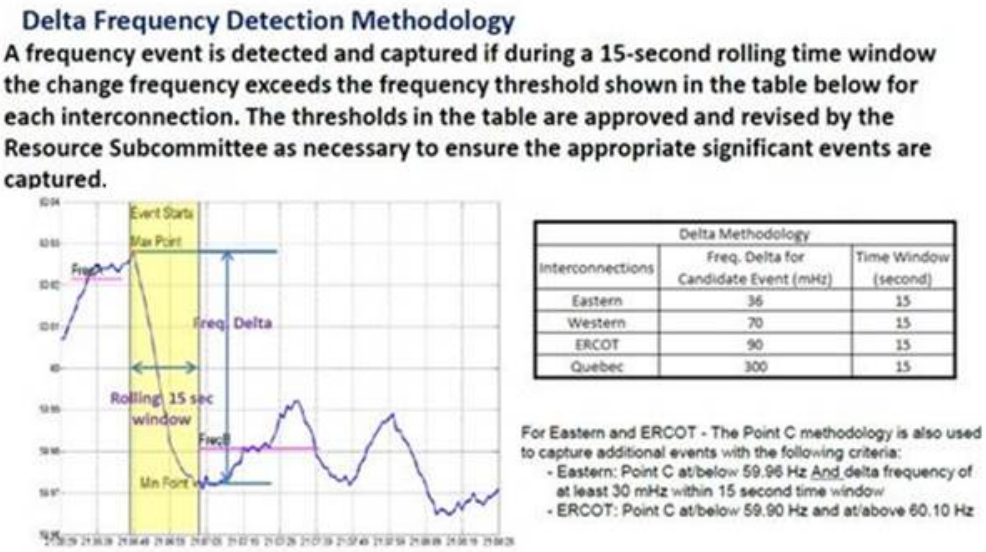


Figure 4.4: Criteria for Calculating Value A and Value B

The actual megawatt loss for the frequency event is determined jointly by NERC and Regional Entity situation awareness staff to develop the monthly frequency event candidate list. Both the change in frequency and the megawatt loss determine whether the event qualifies for further consideration for use in the ALR 1-12 metric or for the measurement of BA performance under Standard BAL-003 – Frequency Response and Bias by the NERC Frequency Working Group. If the event qualifies, then the actual megawatt loss is converted to a beta value (MW/.1 Hz) for use in Figure 4.4 above. The final monthly datasets of approved frequency events[59] are then used to analyze the interconnection frequency response performance.

[56] ALR1-12 Frequency Response Data Collections Process, Slide 18 of Presentation 1, 10/26-27/2011 http://www.nerc.com/docs/oc/rs/RS_Presentation_October_2011.pdf

[57] Resource Subcommittee (RS), http://www.nerc.com/comm/OC/Pages/Resources-Subcommittee-(RS)-2013.aspx

[58] BAL-003-1 Frequency Response & Frequency Bias Setting Standard, 07/18/2011, http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/NOPR_Proposal for BAL-003-1.pdf

[59] Starting in 2014, all frequency events selected for use in BAL-003 shall be also used for the ALR 1-12 frequency performance metric.

Table 4.4 shows the number of frequency events per year for each interconnection from 2009 through 2013. The increase in the number of events for the Eastern Interconnection in 2013 is because of the new threshold, which is 36 mHz, or Point C below 59.960 Hz and delta Hz more than 30 mHz within a 15-second time window.

Table 4.4: Yearly Number of Frequency Events

Interconnection	2009	2010	2011	2012	2013
Western	25	29	25	12	28
Eastern	44	49	65	28	71
ERCOT	51	67	65	63	52
Québec	-	-	20	28	37

Care is taken to select events that impact the frequency beyond the expected dead-band settings for that interconnection. Beta megawatt projections for events that are just slightly larger than the interconnection megawatt cutoff threshold can potentially result in outliers. The resulting frequency response for these smaller events may be quite minimal if generator governors have dead-bands set higher than the expected value. Another factor that can impact the projected beta megawatt value is the 32 second average value chosen for point B. If the frequency response is not sustained for the duration of the 32 second average, the resulting frequency response will be lower and consequently result in a lower beta megawatt value. Lack of sustained frequency response is evident in the Eastern Interconnection and is referred to as the "Lazy L" in frequency/time charts.

Assessment

NERC annually applies statistical tests to interconnection frequency response datasets,[60] and additional analyses on time of year, load levels, and other attributes were conducted in 2013. Frequency response is the ratio of the megawatts lost when generation is tripped and the difference in frequency before and after the event. A large value of frequency response is considered better than a small value.

Frequency Response Trending

From 2009 through 2013, the historical frequency response shows the following trends:

- The Eastern Interconnection has shown steady frequency response performance. A decreasing but not statistically significant time trend for frequency response was observed (there is a high probability the negative slope of the trend line occurred by pure chance). In 2013 the frequency response had the smallest average value observed over the five years studied; moreover, there was a statistically significant decrease of frequency response compared with 2011, which had the best frequency response performance over the same time period.
- The ERCOT Interconnection has had a statistically significant frequency response increase with the average monthly growth of 3.3 MW/0.1Hz; one of the contributing factors was the continued increase in wind generation in ERCOT that typically operates at maximum output. Without margin in the up direction, the interconnection only benefits by curtailing wind generators during high-frequency excursions from these generators. When low-frequency excursions occur, the wind generators cannot provide additional output to increase interconnection frequency.
- The Québec Interconnection (only for 2011–2013) has shown steady frequency response performance; and
- The Western Interconnection has shown steady frequency response performance.

[60] Datasets described in the Frequency Response Initiative Report, October 2012, http://www.nerc.com/docs/pc/FRI_Report_10-30-12_Master_w-appendices.pdf

Figure 4.5 uses a time-trend regression line to show year-to-year time trends by interconnection. The study methods and statistical results are summarized in Chapter 4 and Appendix B.

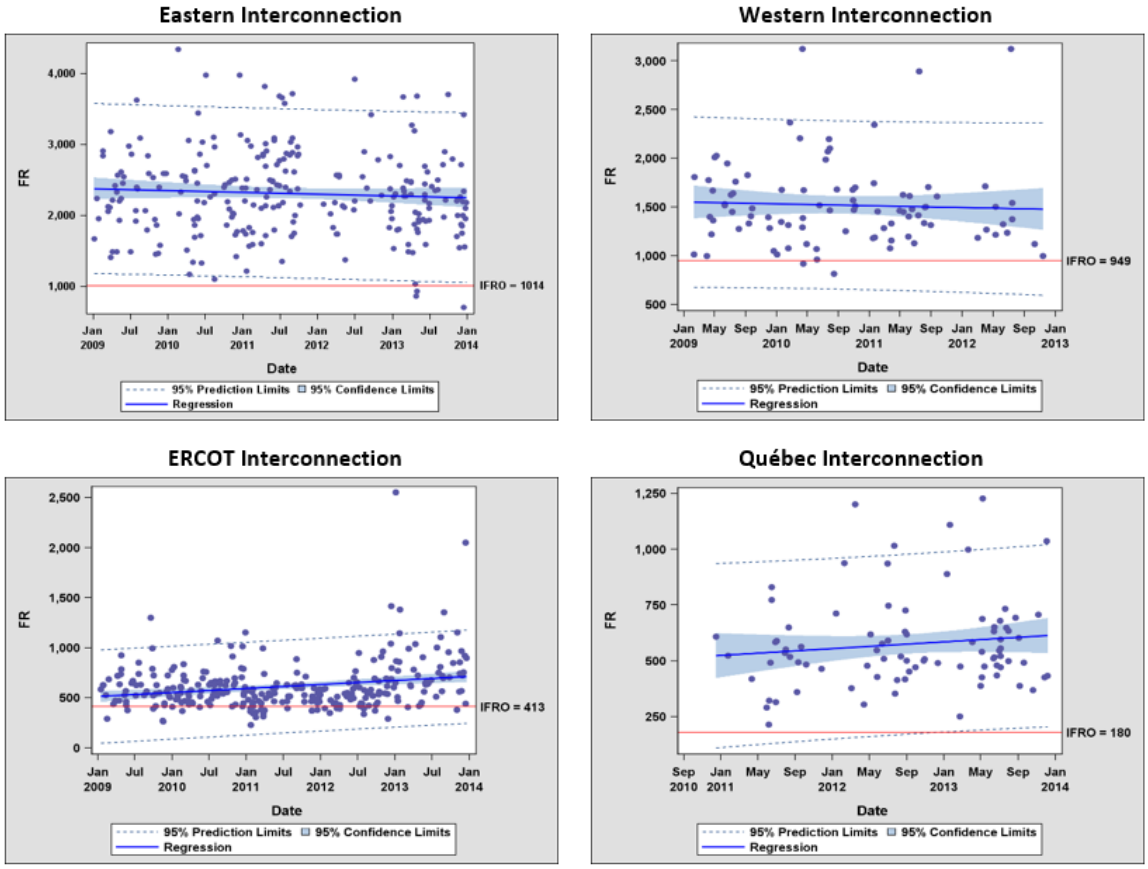


Figure 4.5 Interconnection Frequency Response Trend (2009–2013)

Relation to Interconnection Frequency Response Obligations

The expected frequency response for each interconnection was compared to its respective IFROs from the 2013 Frequency Response Annual Analysis. In all cases, the statistically expected frequency response for each interconnection has been higher than the recommended absolute values of IFRO.[61]

However, the historical frequency responses show (details in Appendix B):

- The Eastern Interconnection has had three events (1.2 percent of all Eastern Interconnection events) with the frequency response value below the absolute IFRO, all of which occurred in 2013;
- The ERCOT Interconnection has had 34 events (11.4 percent of all ERCOT events) with the frequency response value below the absolute IFRO, none of which occurred in 2013;
- The Québec Interconnection has had no events with the frequency response value below the absolute IFRO; and
- The Western Interconnection has had three events (2.5 percent of all Western Interconnection events) with the frequency response value below the absolute IFRO, none of which occurred in 2013.

[61] Current recommended IFRO values are presented in the Frequency Response Annual Analysis, December 2013, Annual Analysis, http://www.nerc.com/FilingsOrders/us/NERC Filings to FER DL/FR Annual Report 12-27-13 Final.pdf

Several factors contributed to the frequency response performance in ERCOT during the years the frequency response did not meet the recommended IFRO (2011 and 2012).

- ERCOT has a small hydro fleet that suffered significantly due to the extreme drought of 2011. There was some relief in 2012, but not in the geographical area of these hydro facilities. Additionally, the owners of the facilities have changed the facilities' operation. Prior to the ERCOT nodal market implementation in December 2010, many of these facilities were operated as frequency responsive reserves. They were on-line in synchronous condenser mode and ramped to full output in about 20 seconds anytime frequency dropped to 59.900 Hz or below, providing 50 to 240 MW of primary frequency response (during the first 20 seconds of a disturbance). Since early 2011, this service has been discontinued. The drought along the Colorado River that provides water to most of the hydro plants in Texas has not improved much. As of March 18, 2014, the watershed area for this river remains in extreme drought or severe drought conditions and has not recovered since 2011.

ERCOT's frequency response performance improved in 2013 for the following reasons:

- Natural gas prices have risen above coal and lignite prices, and solid fuel plants are again dispatched ahead of combined-cycle plants. However, the effort that began in September 2012 by the Texas Reliability Entity (TRE) has proven to be the major contributor to improved frequency response performance in ERCOT. The TRE has followed up with mitigation plans developed by generators of all fuel types to improve their frequency response. As these generators completed these efforts in 2013, the grid frequency response improved.
- FERC approved BAL-001-TRE-1 earlier this year, and the implementation phase began on April 1, 2014. This regional standard will help maintain the frequency response performance of generators in ERCOT and will standardize the dead-band settings of these generators. It is not yet known how much improvement in frequency response will result from this standard since many of the generators have already implemented the required settings. Some improvement in the RMS1 of frequency may be observed as more generators implement the lower governor dead-band settings.

Statistical significance tests have been applied to interconnection frequency response datasets, and additional analysis on time of year, load levels, and other attributes were also conducted. The overall observations and test results are summarized below:

- The Eastern Interconnection frequency response was stable from 2009 through 2013.[62]
- The ERCOT Interconnection frequency response grew from 2009 through 2013.[63]
- The Québec Interconnection[64] frequency response was stable from 2011 through 2013.[65]

[62] The correlation between time variable and frequency response is negative and this is equivalent to the fact that the slope is negative and the trend line is decreasing function. However, the correlation is not statistically significant. This leads to the failure to reject the null hypothesis of zero correlation. So even though the decreasing trend for frequency response in time was observed, there is a high probability that the negative correlation and the negative slope occurred by chance.

[63] The correlation between time variable and frequency response is positive, and this is equivalent to the fact that the slope is positive and the trend line is increasing function with the average monthly growth of 3.3 MW/Hz*0.1; moreover, the correlation is statistically significant ($p<0.0001$). This leads to the rejection of the null hypothesis of zero correlation. So, the observed increasing trend for frequency response is very unlikely occurred by chance.

[64] Only 2011–2013 data is available for Québec Interconnection.

[65] The correlation between time variable and frequency response is positive and this is equivalent to the fact that the slope is positive and the trend line is increasing function. However, the correlation is not statistically significant. This leads to the failure to reject the null hypothesis of zero correlation. So even though the increasing trend for frequency response in time was observed, there is a high probability that the positive correlation and the positive slope occurred by chance.

- The Western Interconnection frequency response was stable from 2009 through 2013.[66]

Special Considerations – Explanatory Variables

As recommended in the *2012 State of Reliability* report,[67] specific attributes have been further studied in order to understand their influence on the severity of frequency deviation events. For each interconnection, a set of six attributes was selected to be studied as explanatory variables for the interconnection frequency response. First, the correlation analysis was carried out to find statistically significant[68] contributors to frequency response; then, the explanatory variables were used as regressors in the multiple regression model that describes the interconnection frequency response. The model selection methods help identify important contributors and remove insignificant or highly correlated regressors to avoid redundancy. The following six specific attributes are included in the studies and tested for the frequency response data of each interconnection. The details of this analysis can be found in Appendix B.

- Summer
- Winter
- High Pre-Disturbance Frequency
- On-peak Hours
- Time
- Interconnection Load Level

For the Eastern Interconnection, only two variables (load level and high pre-disturbance frequency) have a statistically significant correlation with frequency response. The load level has the largest impact on frequency response, followed by the indicator of high pre-disturbance frequency. Interconnection load is positively correlated with frequency response, and high pre-disturbance frequency is negatively correlated with frequency response. There are a number of potential reasons why frequency response can improve as interconnection load level increases. Additional generators will typically be online at higher load periods. This can potentially increase the overall headroom of the generation that is online. It can also increase overall governor participation. In general, the Eastern Interconnection average frequency response of 2,308 MW/0.1 Hz provides a safe margin above the first step of underfrequency load shedding (59.7 Hz) for the single-event criteria loss of 4,500 MW.

For the ERCOT Interconnection, two variables (high pre-disturbance frequency and time) have a statistically significant correlation with frequency response. The indicator of high pre-disturbance frequency has the largest impact on frequency response, followed by time. High pre-disturbance frequency is negatively correlated with frequency response, while time is positively correlated with frequency response. Statistically significant positive correlation with time implies a frequency response improvement with time.

For the Québec Interconnection, three variables (load level, winter, and on-peak hours) have a statistically significant correlation with frequency response. Interconnection load has the biggest impact on frequency response, followed by the indicators of winter and on-peak hours. All these variables are positively correlated with frequency response.

For the Western Interconnection, only one variable (high pre-disturbance frequency) has a statistically significant negative correlation with frequency response.

---

[66] The correlation between time variable and frequency response is negative and this is equivalent to the fact that the slope is negative and the trend line is decreasing function. However, the correlation is not statistically significant. This leads to the failure to reject the null hypothesis of zero correlation. So even though the decreasing trend for frequency response in time was observed, there is a high probability that the negative correlation and the negative slope occurred by chance.

[67] 2012 State of Reliability Report, May 2012, http://www.nerc.com/files/2012_SOR.pdf

[68] At significance level of 0.1.

In summary, a high pre-disturbance frequency and interconnection load level are the two factors that significantly affect frequency response—the high pre-disturbance frequency results in a longer time for the frequency to fall below the governor dead-band setting and degrades frequency response.

ALR3-5 (M-8) Interconnection Reliability Operating Limit Exceedances

Background

The *State of Reliability 2013* report reviewed the Interconnection Reliability Operating Limit/System Operating Limit (IROL/SOL) Exceedances metric. In the past, this metric has been used to determine the number of times an IROL was exceeded in the Eastern Interconnection and the number of times an SOL was exceeded in the Western and ERCOT Interconnections. Since the metric was first introduced, all regions now recognize IROLs and are anticipated to be able to report on IROL exceedances in 2014. Therefore, metric ALR 3-5 (M8) was modified to remove the SOL reporting language in late 2013.

This metric measures the number of times that a defined IROL was exceeded and the duration of these exceedances. Exceeding an IROL could lead to widespread outages if prompt operator control actions are not taken to return the system to within normal operating limits. In addition, exceeding the limits may not directly lead to an outage but may put the system at unacceptable risk if the operating limits are exceeded beyond T_v.[69] To monitor how quickly an IROL is returned to within normal limits, the data is grouped into four time segments, as shown in Table 4.5.

Table 4.5: Exceedance Duration Segment

Time Range	IROL/SOL Duration
Time Range 1	10 secs < Duration ≤ 10 mins
Time Range 2	10 mins < Duration ≤ 20 mins
Time Range 3	20 mins < Duration ≤ 30 mins
Time Range 4	Duration > 30 mins

[69] T_v is the maximum time that an Interconnection Reliability Operating Limit can be violated before the risk to the interconnection or other Reliability Coordinator Area(s) becomes greater than acceptable. Each Interconnection Reliability Operating Limit's T_v shall be less than or equal to 30 minutes.

Eastern Interconnection

Figure 4.6 shows the number of IROL exceedances by quarter and time range of exceedance for the Eastern Interconnection for 2011–2013. The second quarter shows the most exceedances for the Eastern Interconnection in all years due to planned transmission outages resulting in congestion and higher flows on the remaining paths.

It is notable that most of the exceedances occur in Time Range 1 and 2, and that for the three years included in the analysis, the number of exceedances decreased in both of those time ranges. However, in 2013, there were also exceedances that had durations that put them into Time Range 3 and Time Range 4, meaning that the duration of these three exceedances were greater than 20 minutes; two of them were greater than 30 minutes.

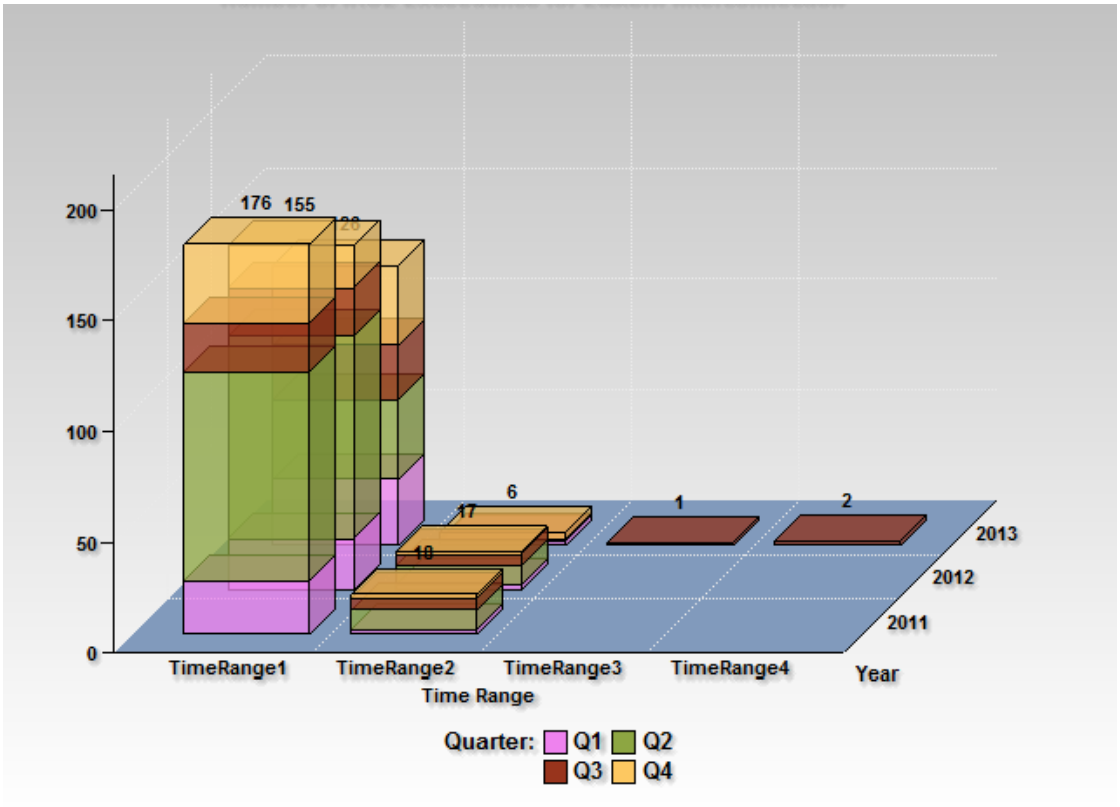


Figure 4.6: Eastern Interconnection IROL Exceedances

Western Interconnection

WECC is making changes in 2014 to the way its limits are calculated to allow the calculation of IROL limits and will therefore be able to report on IROL exceedances going forward. Figure 4.7 shows the number of SOL exceedances separated by quarter and segment type for the Western Interconnection from 2011 through 2013.

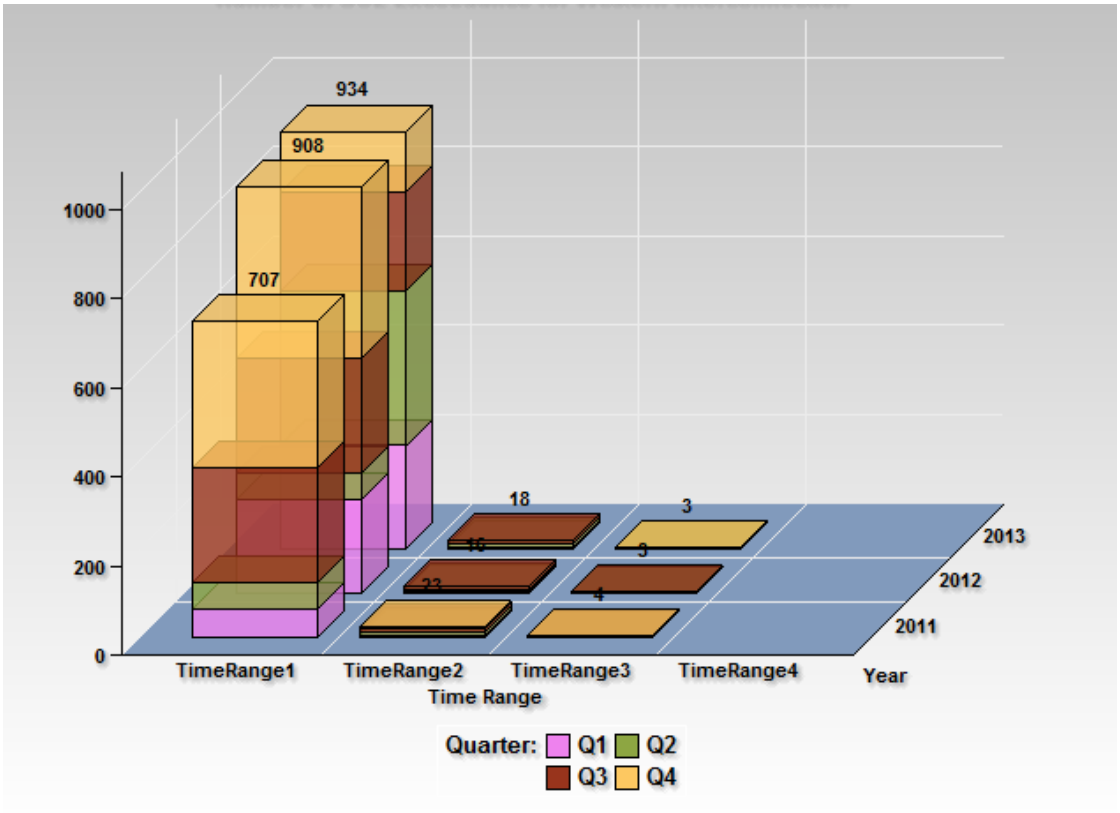


Figure 4.7: Western Interconnection ALR3-5 SOL Exceedances

ERCOT Interconnection

Figure 4.8 shows that the number of IROL exceedances was greatly reduced from 2011 through 2013. Some contributions to the improved performance are smoother transitions in limit values due to the implementation of real-time analysis tools, and more available transmission. The completion of a major transmission expansion project resulted in a major drop in exceedances between the fourth quarter of 2012 and the first quarter of 2013. The result is that the IROL that contributed to most of the exceedances has been mitigated, so exceedances are not expected to occur going forward.

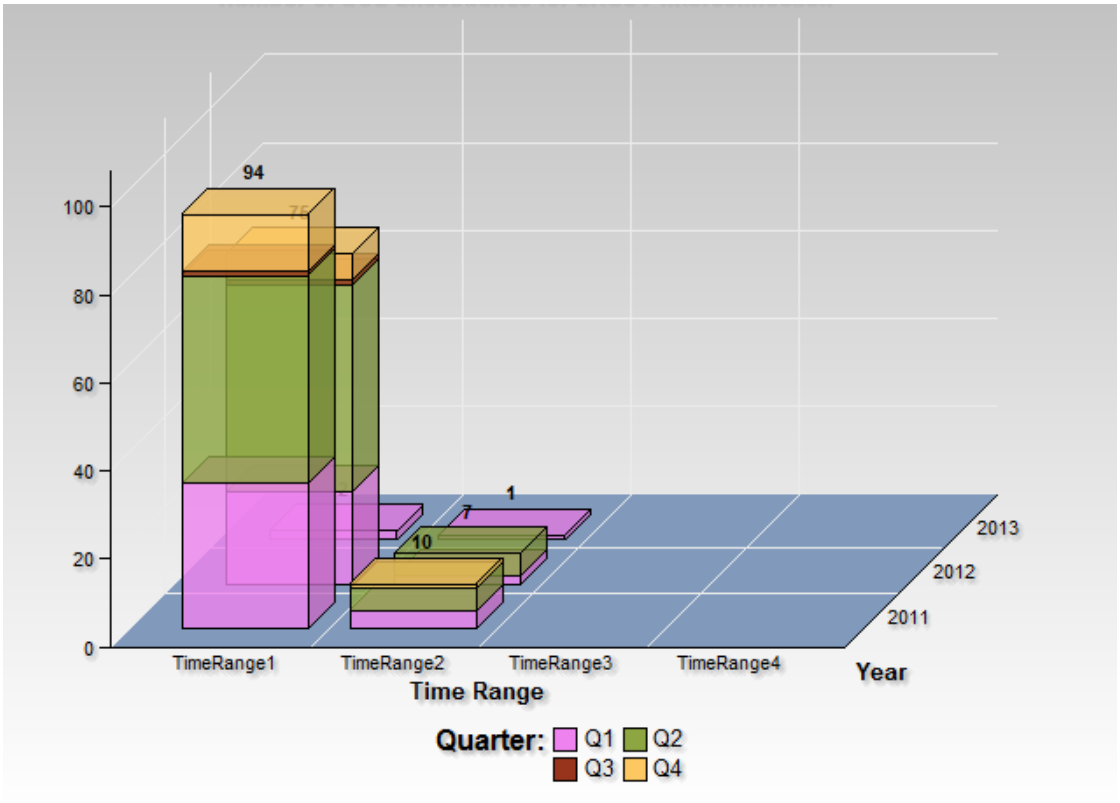


Figure 4.8: ERCOT Interconnection ALR3-5 SOL Exceedances

Québec Interconnection

To maintain the anonymity of the reporting entity, information regarding the assessment of Québec Interconnection is not disclosed, despite the data's being available.

ALR4-1 (M-9) Protection System Misoperations

Background

Protection system misoperations were identified as an area that requires further analysis in the *State of Reliability 2013* report. The improvements to the data collection process that the Protection System Misoperations Task Force (PSMTF) and System Protection Control Subcommittee (SPCS) proposed in 2013 have been implemented and should improve the accuracy of future misoperation reporting. Based on the recommendation by the PSMTF and SPCS, the respective protection system subcommittees within each Regional Entity began analyzing misoperations on an annual basis in early 2014. The *State of Reliability 2013* report also recommended that additional analysis be performed to determine how often misoperations are involved with reportable system

disturbances and whether the misoperation was causal to the event or exacerbated the seriousness of the disturbance.

Assessment

Figure 4.9 shows the misoperation rate by Region. The misoperation rate reflects the ratio of misoperations to total operations for the entire BES, 100 kV and above. This ratio provides a stable way to trend the rate of misoperations as compared to a misoperation count alone, where weather and other factors can influence the count. Total protection system operations was first requested with the fourth quarter 2012 misoperation data. Having the total number of operations for the reporting periods in 2013 allows for a consistent way to normalize and trend protection system misoperations over time.

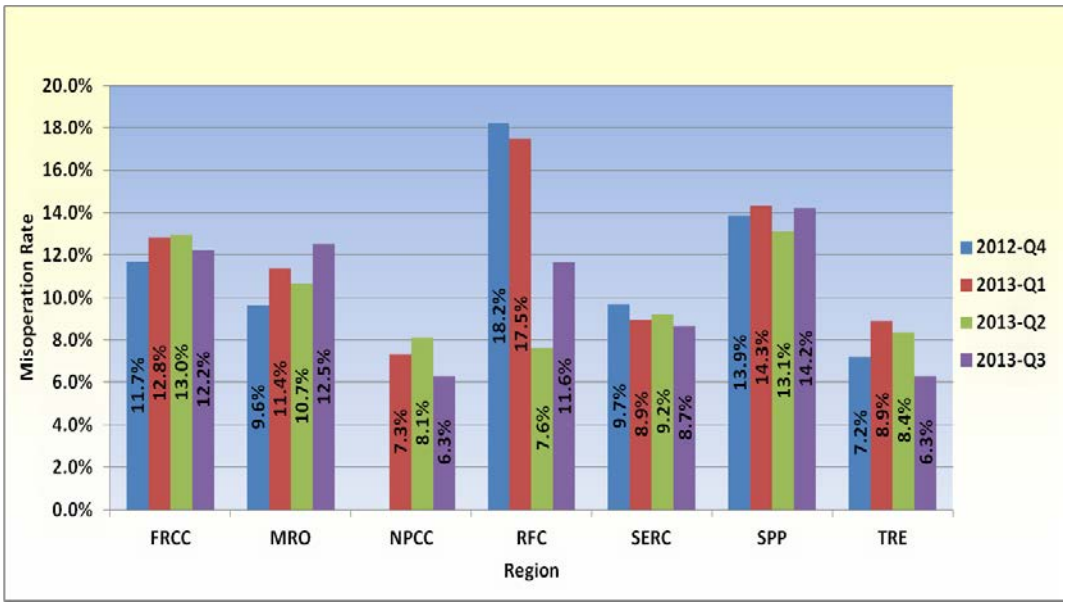


Figure 4.9: ALR4-1 Misoperation Rate by Region

Figure 4.10 shows misoperations on a monthly basis from April 1, 2011, to September 30, 2013. Overall, the trend is periodic, with peaks in the spring and summer months of all three years.

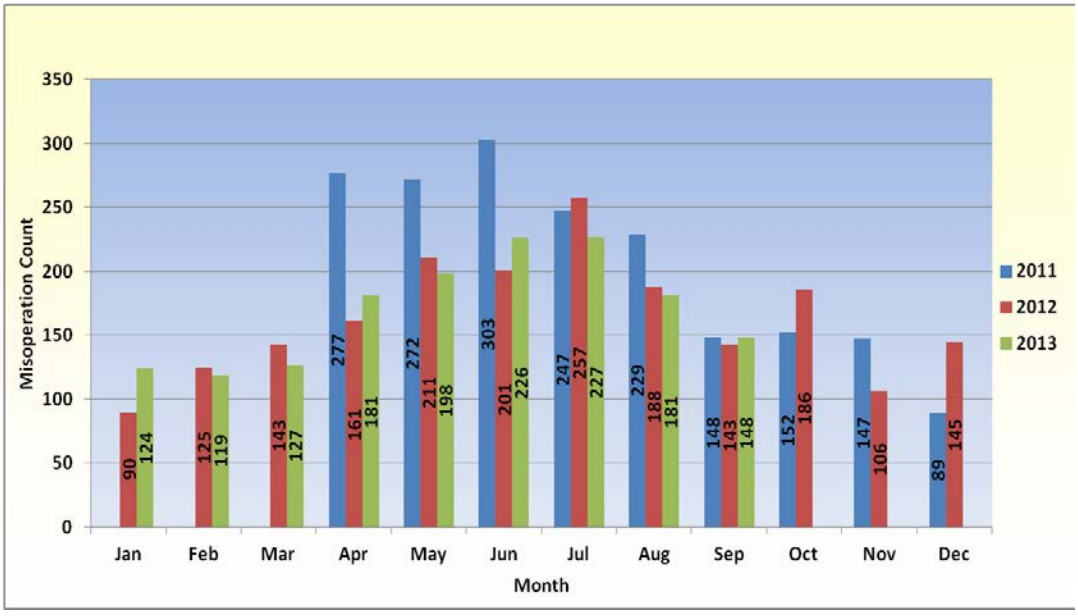


Figure 4.10: NERC Misoperations by Month (2Q2011–4Q2013)

Figure 4.11 illustrates the top-three cause codes being assigned to misoperations by the TOs: incorrect setting, logic, or design error; relay failures/malfunctions; and communication failure. These three cause codes have consistently accounted for 65 percent of all misoperations since data collection started in 2011.

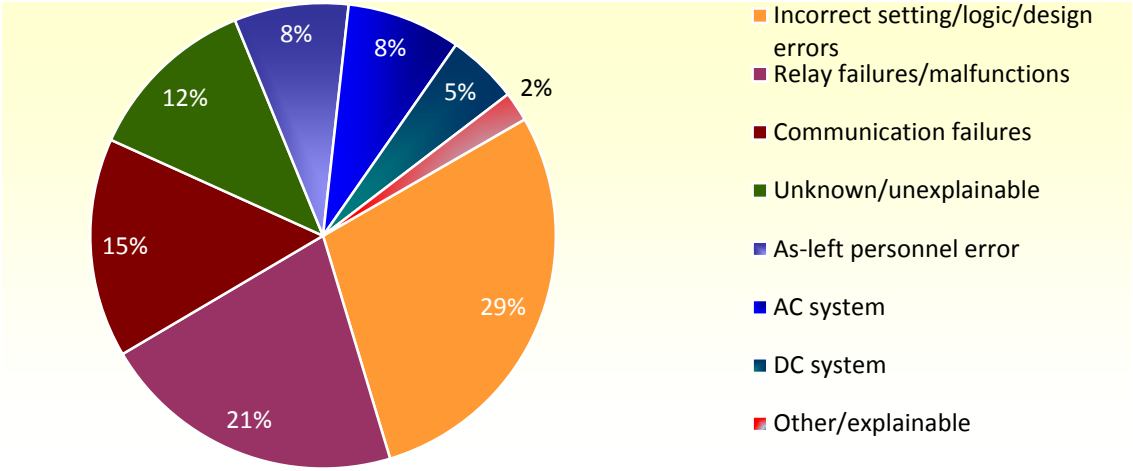


Figure 4.11: NERC Misoperations by Cause Code from 2011Q2 to 2013Q3[70]

In 2013, 71 transmission-related system disturbances resulted in a NERC Event Analysis reported event. Of those 71 events, 47 events (about 66 percent), had associated misoperations. Of these 47 events, 38 events (about 81 percent), experienced misoperations that were contributory to and/or exacerbated the severity of the event. In several cases, multiple misoperations occurred during a single disturbance. Cause coding has not yet been completed for all 2013 events, but it is estimated that there were 60–75 misoperations associated with these 38 reportable events. Therefore, out of approximately 2,000 total misoperations in 2013, approximately 3.0 to 3.5 percent were causal to or exacerbated the severity of reportable system disturbances.

NERC is in the process of revising a number of Reliability Standards involving protection system misoperations.[71] To increase awareness and transparency, NERC will continue to conduct industry webinars[72] on protection systems and document success stories on how GOs and TOs are achieving high levels of protection system performance. The quarterly protection system misoperation trending by NERC and the Regional Entities can be viewed on NERC's website.[73]

As identified in the 2013 PSMTF final report, there are several areas where misoperation reduction is possible for entities. First, relay applications requiring coordination of functionally different relay elements should be avoided. Secondly, misoperations due to setting errors can potentially be reduced. Techniques that could be used to reduce the application of incorrect settings include peer reviews, increased training, more extensive fault studies, standard templates for setting standard schemes using complex relays, and periodic reviews of existing settings when there is a change in system topography. Finally, firmware updates may affect relay protection settings, logic, communications, and general information stored and reported by the relay. Entities should be aware of what version of firmware they have on their microprocessor-based relays. Entities should also monitor if the relay vendor has issued updated relay firmware.

[70] Cause-coded Misoperation data for 2013 4Q is not available at this point.
[71] http://www.nerc.com/pa/Stand/Pages/Project2010-05_Protection_System_Misoperations.aspx
[72] http://www.nerc.com/files/misoperations_webinar_master_deck_final.pdf
[73] http://www.nerc.com/pa/RAPA/ri/Pages/ProtectionSystemMisoperations.aspx

Special Considerations

In the annual review of metrics, the PAS made a minor modification to ALR4-1 (M-9) to remove the interim method for calculation of the total number of operations. Previously, automatic operations were only available through TADS data, which only includes operations at 200 kV and above. This change was approved in December 2013.

NERC undertook an effort to collect data on total protection system operations to create a more useful metric for monitoring protection system misoperation performance. This data collection began with the reporting of fourth quarter 2012 misoperation data. Having the total number of operations for the reporting periods in 2013 facilitates a way to normalize and trend protection system misoperations over time.

ALR6-2 (M-11) Energy Emergency Alerts

Background

This metric was enhanced in 2013 by expanding the data collection to include counts and duration of all EEA events of all levels and unserved energy data for all EEA Level 3 occurrences that result in load shedding. This metric will account for the number and duration of Energy Emergency Alerts that are issued. All EEA Level 1, Level 2, and Level 3 occurrences can then be tracked to see whether there are any changes in frequency, duration, and load shed magnitudes of EEA occurrences over time.

As historical data is gathered on EEAs, trends provide a relative indication of performance measured at a BA or interconnection level. By definition, when an EEA Level 3 Alert is issued, firm-load interruptions are imminent or in progress. An EEA Level 3 indicates an issue with the real-time adequacy of the electric supply system. It may be due to a lack of fuel or dependence on transmission for imports into a constrained area, not simply a lack of available generation resources. The contributing factors for EEA Level 3 events need to be considered.

Reporting the duration and unserved energy of load shed events aids in determining the likelihood and duration of a load shed event following the issuance of an EEA Level 3. EEA Level 3 events are currently reported, collected, and maintained in NERC's Reliability Coordinator Information System (RCIS), as defined in NERC Standard EOP-002.[74]

Assessment

Table 4.6 shows the number of EEA Level 3 events from 2006 to 2013 at the Regional Entity level. Interactive quarterly trending is available at the Reliability Indicator's page.[75] In 2013 there were seven EEA Level 3 Alerts issued, with only one resulting in a loss-of-load event. Seven EEA Level 3 events were declared in 2013, which is significantly lower than the number that occurred in prior years.

Table 4.6: Energy Emergency Alert 3

Number of Events	Year							
	2006	2007	2008	2009	2010	2011	2012	2013
NERC	7	23	12	41	11	23	16	7
FRCC	0	0	0	0	0	0	0	1
MRO	0	0	0	0	0	0	0	0
NPCC	0	0	1	1	0	0	0	0
RF	0	3	1	0	2	0	1	0
SERC	4	14	2	3	4	2	7	0
SPP	1	5	3	35	4	15	6	2
TRE	0	0	0	0	0	1	1	0
WECC	2	1	5	2	1	5	1	4

[74] The latest version of EOP-002 is available at: http://www.nerc.com/files/EOP-002-3_1.pdf

[75] The EEA3 interactive presentation is available on the NERC website at: http://www.nerc.com/pa/RAPA/ri/Pages/EEA2andEEA3.aspx

The one EEA Level 3 event that resulted in load shed involved the interruption of 200 MW of load for two hours, or unserved energy of 400 MWh. This event was due to a number of factors that culminated with the failure of transmission system equipment that reduced the ability to serve all the load in the affected area.

The other six reported EEA Level 3 Alerts did not result in any loss-of-load events. These EEA Level 3 events fell into two categories. One category pertained to significant unplanned outages of resource supply due to generator trip or equipment failure, either the unplanned loss of one or more generation resources, or the unplanned loss of a major transmission facility that supplied generation into an area. These included quickly evolving events in which the entity had to use its reserves to serve its load and had to prepare for load shed to meet the next possible contingency. The other category consists of events in which transmission limitations in the form of Transmission Loading Relief (TLR)[76] events were in place and were affecting entities that rely upon import transactions to serve their load. These events did not involve sudden loss of generation or equipment failures; rather, they occur as loading increases over a period of time and the affected TOP responds by requesting various levels of TLR relief. The entities in this category used the EEA Level 3 to protect their firm transactions to avoid having to reduce load, and they called upon reserve sharing provisions to restore reserves.

In 2013, NERC began assessing the EEA Level 1 and Level 2 events as a part of this metric. Table 4.7 shows the number of EEA events at each of the levels and displays all the EEA alerts reported in 2013 by region (except for TRE). It is intuitive that more events occurred at Level 1 and Level 2, as those represent situations in which capacity emergencies are developing.

Table 4.7: EEA Level by Region

Region	EEA1	EEA2	EEA3	Total
FRCC	2	3	1	6
MRO	11	0	0	11
NPCC	5	11	0	16
RF	5	11	0	16
SERC	2	3	0	5
SPP	2	0	2	4
WECC	20	9	4	33
Grand Total	**47**	**37**	**7**	**91**

Figure 4.12 displays the cumulative amount of time at each EEA alert level. Since this data for all the alerts was only collected for 2013, there is not sufficient history to trend the data, which will continue to be gathered and analyzed going forward.

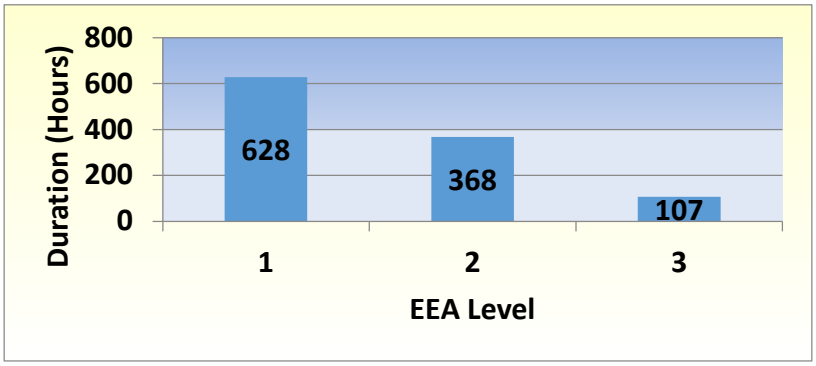


Figure 4.12: Duration (Hours) by EEA Level

[76] http://www.nerc.com/pa/rrm/TLR/Pages/default.aspx

Chapter 5 – Event Analysis

Background

The industry's voluntary event analysis program is providing valuable information for the ERO and industry to use to address potential threats or vulnerabilities to the reliability of the BPS. Since its initial implementation in October of 2010, the process has resulted in the collection of 399 qualified events being reported to the ERO and yielded more than 77 lessons learned, including 14 published in 2013.[77] NERC and the Regions assess every event to identify and share with industry the possible threats to reliability. This year the NERC Cause Code Assignment Process (CCAP) provided greater ability for historical trending and predictive analysis. Industry has actively participated in the assignment of cause codes as events, providing greater transparency on how NERC trends events; it also provides a great venue for active collaboration and sharing. This active collaboration is a testament to how much effort and resources are being expended in this area by the industry, as well as how important it is for the ERO and industry to truly understand the different contributors to events. The OC's Event Analysis Subcommittee (EAS) has been essential in the maturation of this process and has facilitated the active disseminations of many of the products that have been delivered to date. This chapter highlights some of the significant products that have been produced from this active collaboration.

Bulk Power System Awareness

The process for understanding the potential threats or vulnerabilities to the reliability of the BPS starts with understanding events and occurrences in the context in which they occur. NERC's Bulk Power System Awareness (BPSA) group and the eight Regional Entities monitor BPS conditions, significant events, and emerging threats for the 15 Reliability Coordinator regions in North America to understand the conditions and situations that could impact the BPS's reliable operation. This group also supports the development and publication of alerts and awareness products and facilitates information sharing among industry, the Regions, and the government during crisis situations and major system disturbances.

The first step in NERC's Event Analysis Program is to monitor and be aware of BPS events above a certain threshold of impact or risk. The group partners with Regional Entity staffs to monitor conditions on the BPS and allow the ERO to conduct in-depth, critical self-analysis of these events to identify trends and provide experience-based insight to prevent repeat occurrences. NERC's BPSA, in close coordination with the Regional Entities, shares the needed information with NERC and Regional Entity Event Analysis staff.

Overview and Accomplishments of the ERO BPSA Group

By The Numbers – Bulk Power System Awareness

- 480 new Event Analysis database entries initiated
- 250 daily reports published
- 46 special reports published during major system disturbances
- Received and processed:
  - 316 OE-417 reports
  - 42 EOP-004 system disturbance reports
  - 7 EOP-002 reports
  - 1,990 Intelligent Alarms notifications
  - 2,582 FNet notifications
  - 4,562 WECCnet messages
  - 1,709 Reliability Coordinator Information System messages
  - 156 Space Weather Predictive Center notifications
  - 149 Department of Homeland Security notifications
- 1 advisory (Level 1) alert issued
- 4 advisory (Level 1) alerts published, assisting ES-ISAC

[77] The link to the NERC Lessons Learned page: http://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx

As recognizable from the data above, many occurrences, notifications, and alarms occur frequently, with little or no real impact on the system at large. Being aware of the daily occurrences aids in the understanding of the size and complexity of the system. Registered entities continue to inform and collaborate with the ERO well beyond what is required in an effort to make sure all stay abreast of the state of the grid. Only a small subset of the occurrences of which the BPSA group is made aware rise to the level of a reportable event. When a registered entity experiences an event, the registered entity will recommend an initial category for the event, as outlined in the figure below. The categories listed in the Categorization of Events section do not cover all possible events.

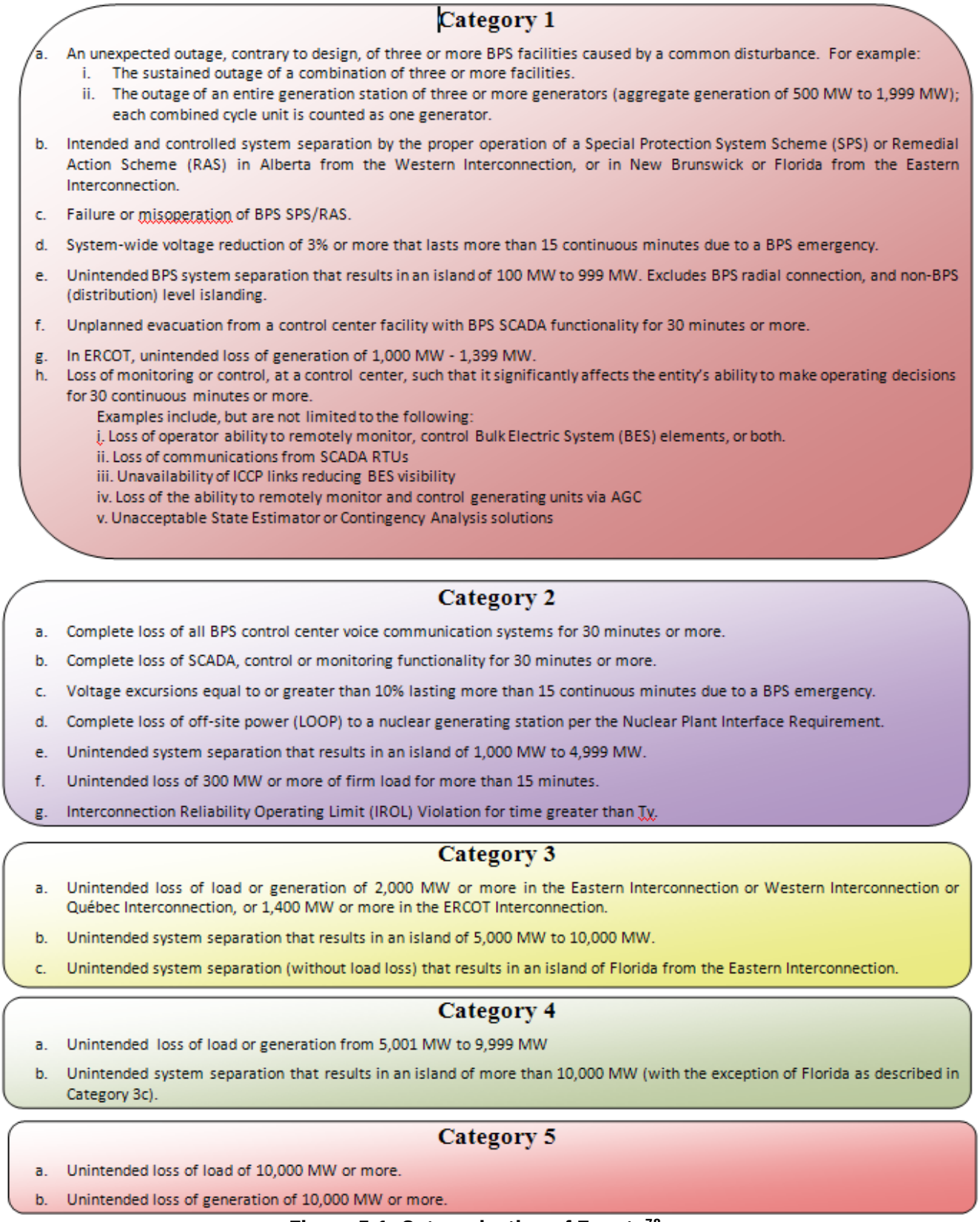


Figure 5.1. Categorization of Events[78]

[78] Qualifying events are assigned to one of five categories based on the impact to the reliability of the BPS. The event categories are intended to allow the registered entity and Regional Entity to objectively identify event thresholds. For a more thorough review of the process see: http://www.nerc.com/pa/rrm/ea/EA Program Document Library/Final_ERO_EA_Process_V2.1.pdf

In 2013, the NERC CCAP provided valuable information to the industry, including greater ability for historical trending and predictive analysis. The active participation by industry has greatly enhanced the accuracy in the assignment of cause codes as events are analyzed and trended, providing greater transparency on how NERC and the Regional Entities trend events. The process provides an ideal venue for active collaboration and sharing. See Table 5.1 for a consolidated chart of the reportable events since the program's inception and for 2013.

Table 5.1: Event Analysis Event Summary. The events by category since the initial implementation in 2010 and the event count for 2013

Event Category	Count (Total)	Count (2013)	Comments
CAT 1	267	102	
CAT 2	114	33	30 - EMS events (2b) (2013) 2 - LOOP events (2d) (2013) 1 – Loss of >300MW firm load for >15 minutes(2f)
CAT 3	14	6	
CAT 4	3	0	SW Winter Weather (2011) SW Blackout (2011) Derecho (2012)
CAT 5	1	0	Hurricane Sandy (2012)
Total CAT 1-5 Events	**399**	**141**	
Non-Qualified Occurrences reported	**1715**	**342**	

The plotting of the number events over time allows one to see if there is any sort of trending that is moving outside of the normal event count averages and is one indicator of the consistent reliability of the grid through a variety of external and environmental conditions (Figure 5.2).

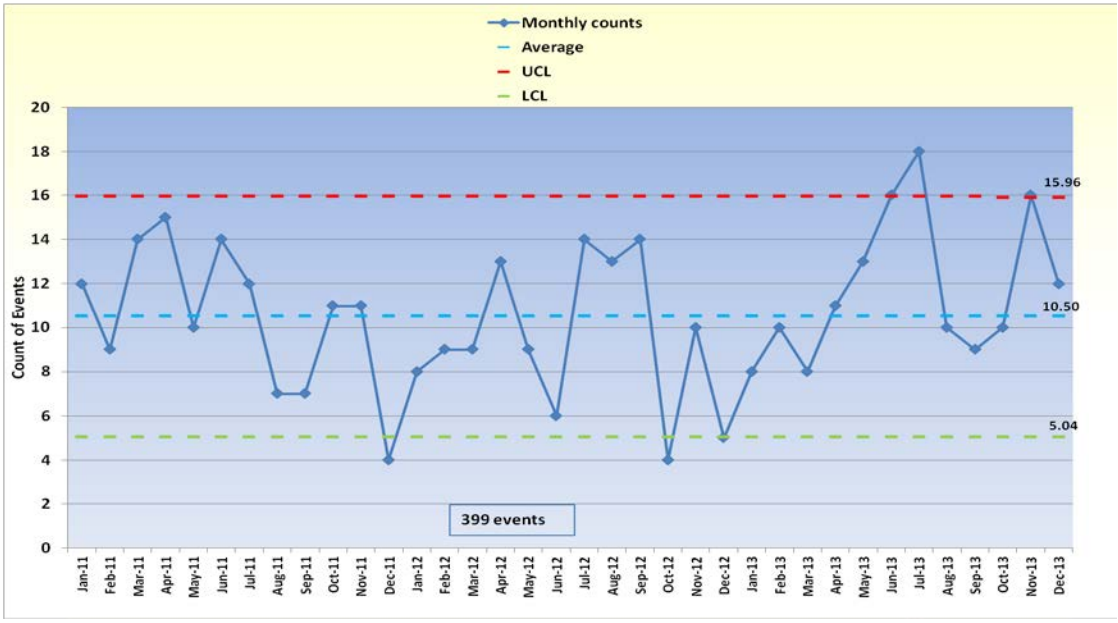


Figure 5.2: Trending of the Number Events over Time[79]

[79] Count of events by month with three-month average for control limit calculation. Surpassing the upper control limit in July of 2013 was largely due to environmental conditions, in this case, flooding and forest fires.

The above trending graph is of the 399 qualified events through 2013. The quality of the event reports is vital for the success of the NERC Event Analysis Program. The quality, detailed analysis, and investigations that entities performed have led to quality reports.[80] Good quality event analysis reports allow for more accurate cause coding of events and has led to better trending. Better trending leads to timely identification of issues being communicated back to the industry.

Through the Event Analysis Program, NERC assesses every event report to identify and then share with industry the apparent threats to reliability that may be emerging. The NERC CCAP manual[81] was updated in February 2013. Cause coding has allowed for easier trending for all event causes. While the root cause of every event can not necessarily be determined, many of the contributing causes or failed defenses can be determined, analyzed, and trended to provide valuable information to the industry. Figure 5.3 shows the overall trends for the contributing causes of events.

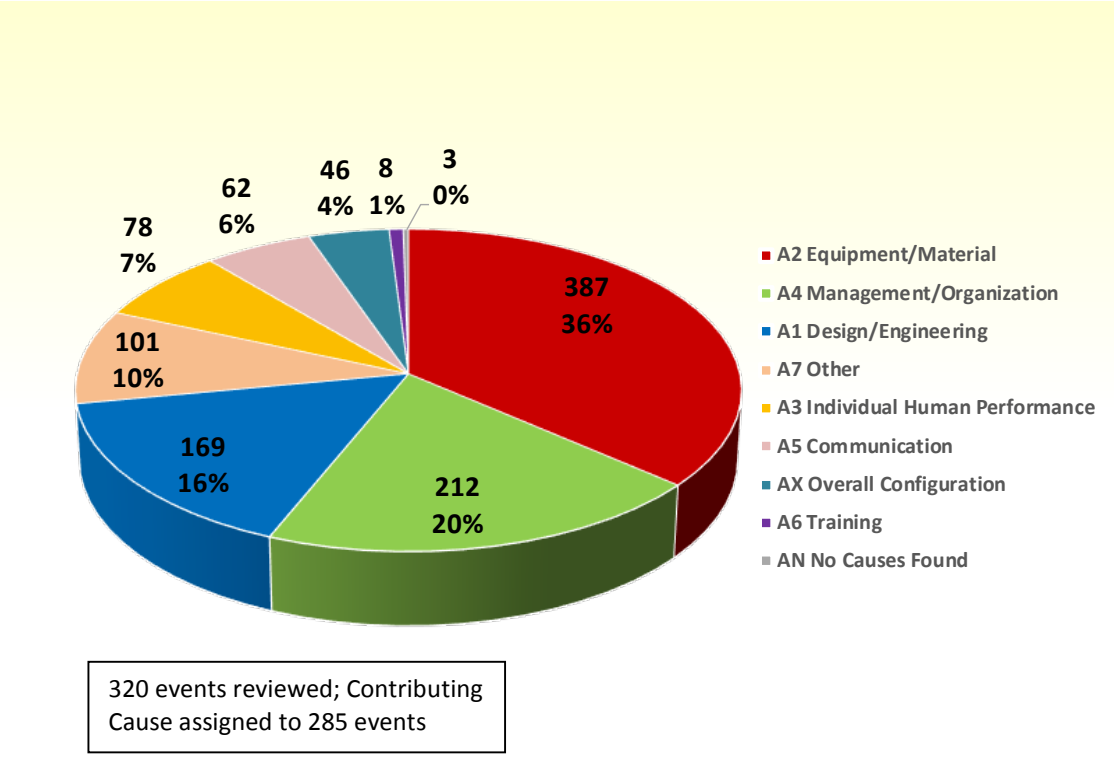


Figure 5.3: The Percentage of Contributing Causes by Major Category

Identification of these large areas of concern allow NERC and industry to prioritize and search for actionable threats to reliability. For example, from the chart above, one can see the large amount of equipment that is damaged or fails that is linked to the causes of events. With the systematic approach to trending all of the event data, the different types of failed or damaged equipment can be parsed from the aggregate data. In this case, circuit breaker failures were found to be the single-largest contributor to events (see Figure 5.4). This is often the failure mode of an event—what one sees as the apparent cause. Note that when possible, the distinction is made between equipment that fails due to damage (both human caused and nature caused), end of life, or other related attributes that result in the equipment or material not functioning as desired. For the purpose of the following

[80] http://www.nerc.com/pa/rrm/ea/EA Program Document Library/NERC-Report-Quality.pdf

[81] http://www.nerc.com/pa/rrm/ea/EA%20Program%20Document%20Library/NERC_Cause_Code_Assignment_Process_March_2014_rev20140324%20SLS.pdf

analysis, failed equipment relates to all of the aforementioned attributes, unless a specific failure mechanism is mentioned.

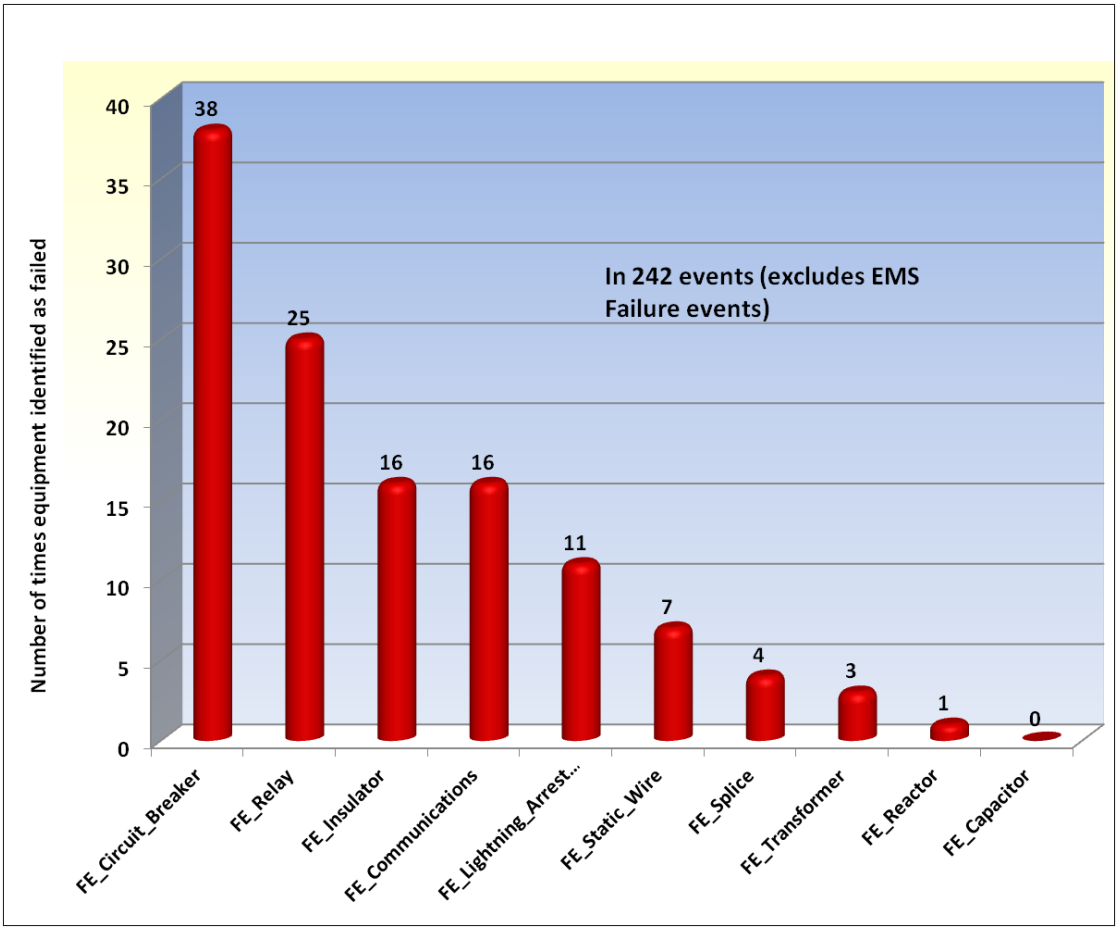


Figure 5.4: Failed Equipment Identified during Review of Event Reports

Further analysis of circuit breakers suggested a trend for a specific type of circuit breaker in many of the observed and reported events. NERC was then able to develop a case history. An example of the benefits of industry and NERC analyzing events is a recently identified trend related to the failure mode of a specific type of 345 kV breaker.

Figure 5.5 shows a timeline during which a trend was identified for a specific type of 345 kV SF_6 puffer-type circuit breaker failure.

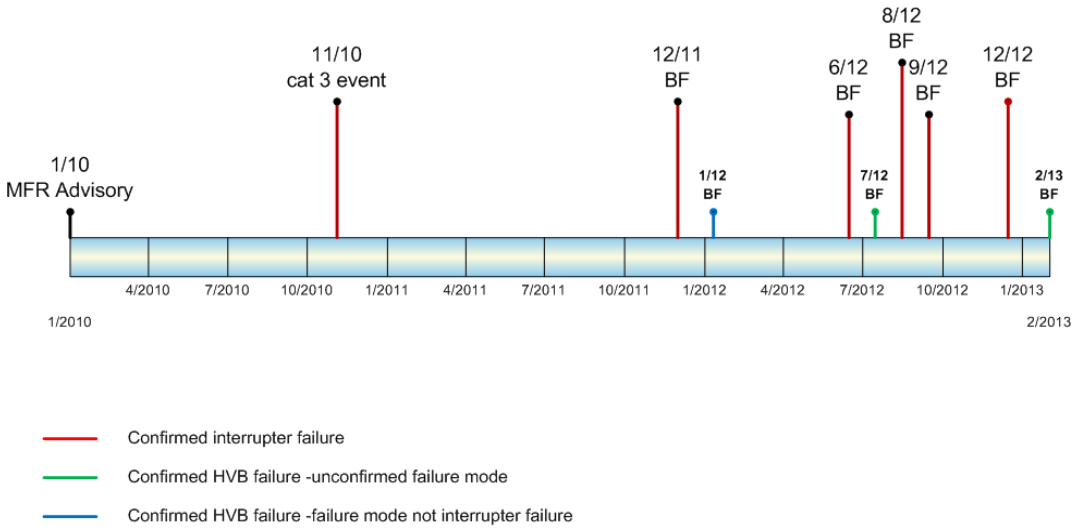


Figure 5.5. Timeline for Identification of a Trend in 345-kV SF_6 Puffer-Type Circuit Breaker Failures

These analyses resulted in NERC's issuing a Level 1 Advisory Alert regarding identification of a trend in 345 kV SF_6 puffer-type circuit breaker failures and the potential risk it posed to the reliability of the BPS. The purpose of the alert was to ensure that industry was aware of the recent failures and previously published maintenance advisories, so appropriate action could be taken by entities that utilize this particular equipment.

While the alert was advisory in nature and did not require specific action to be taken, this was a reliability risk suited for close collaboration with the North American Generator Forum and North American Transmission Forum, as well as certain trade associations with members that may have this particular 345 kV equipment. This advisory provided an excellent opportunity for NERC to work directly with the forums and trades to determine the extent of the condition and address the potential risk to the BPS.

NERC continues to conduct cause analysis training with staff from the Regions and registered entities. As of December 2013, personnel from all eight Regions and 668 persons from 145 different registered entities have received cause analysis training—more than 5,400 hours of training.

A similar identification of trends can be observed in the large contribution of "less than adequate" or "needs improvement" areas of management and organizational practices that contribute to events. Many of these threats can be identified and shared with the industry for awareness. For example, in Figure 5.6, the identification of some of the particular challenges to organization and management effectiveness are identified.

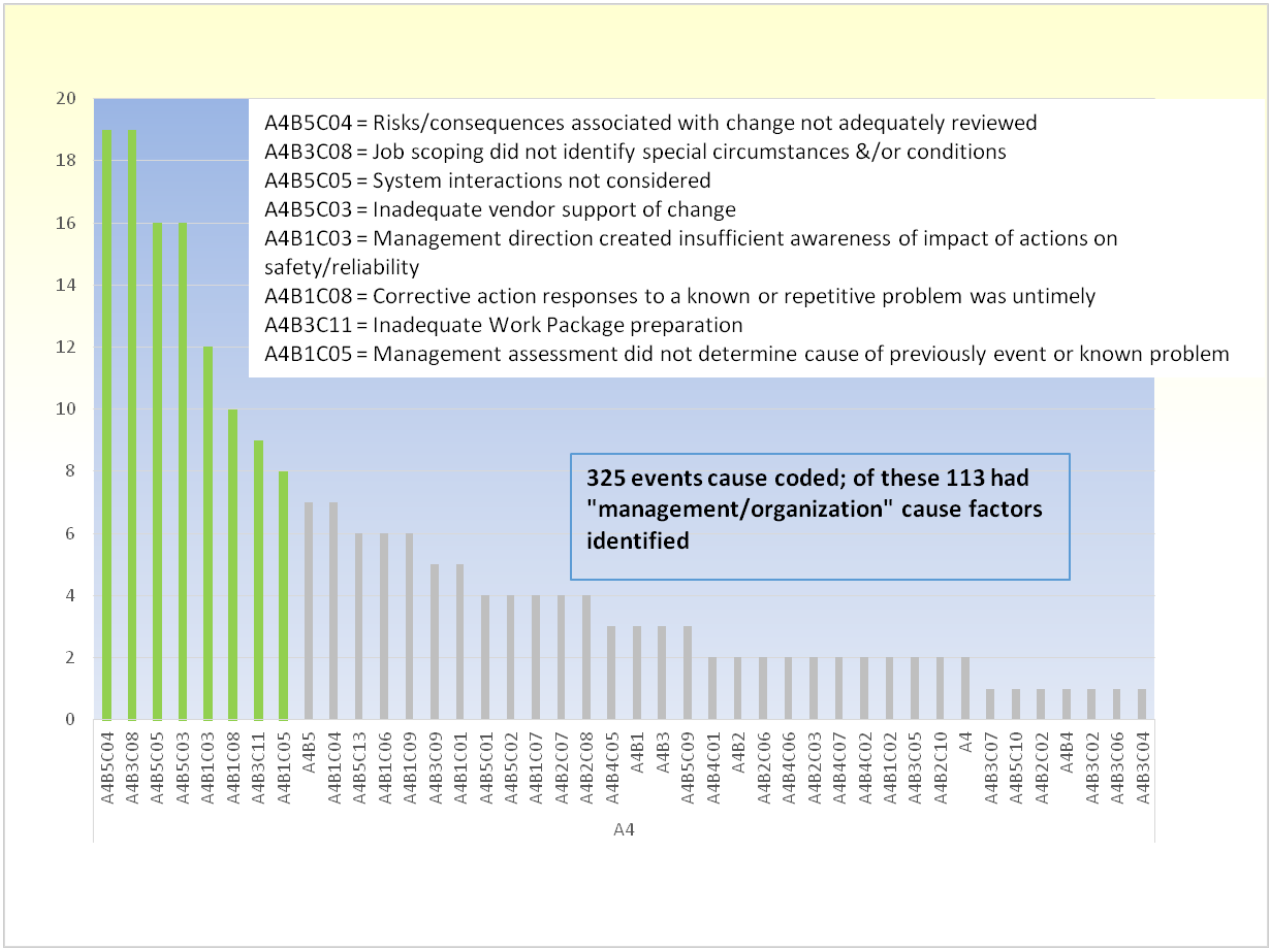


Figure 5.6: "Less than adequate" or "Needs improvement" Management/Organization Challenges that Contributed to an Event

Management of complex systems and organizations is a challenge in every industry, and the percentage of events with these contributing factors is collectively found in other industries.

Many of the most frequently identified contributing causes for events seen in Figure 5.6 were found present in the severe cold weather events. NERC, in close collaboration with the regional staff and the industry, published a report titled, *Assessment of Previous Severe Winter Weather Reports 1983-2011* to provide a review and comparison of previous winter weather events.[82] This review and a cold weather training package were provided to the industry to assist in their winter weather preparation.

Additionally, NERC conducted an industry-wide webinar in October 2013. Over 350 owners, users, and operators attended a webinar that provided the industry reports and training material in preparation for the upcoming winter weather forecasts and entity cold weather preparedness. During the webinar, the impacts from both the February 2011 Southwest Cold Weather Event and previous cold weather events were discussed. The webinar encouraged GOs and GOPs to focus on areas that were observed in past events, such as inspecting and maintaining

[82] These reports can be found at http://www.nerc.com/pa/rrm/ea/Pages/February-2011-Southwest-Cold-Weather-Event.aspx .

heat trace equipment and thermal insulation, erecting adequate wind breaks and enclosures, and taking measures to protect instrument lines and equipment prior to the onset of winter weather.

NERC also reviewed the *Assessment of Previous Severe Winter Weather Reports 1983-2011* during the webinar. This report provides a review and comparison of the previous winter events cited in the FERC and NERC staff Report.[83] This was to remind industry that generators experienced weather-related outages and rolling blackouts in previous events, and lessons learned from these events could have prevented outages in more recent winter events.

The OC-developed Reliability Guideline[84] was also reviewed. This guideline provides a general framework for developing an effective winter weather readiness program for generating units throughout North America. Although the NERC *Winter Reliability Assessment 2013-14* was expected to be published later in November, attendees were given a preview of the draft. NERC also covered the NOAA Winter Outlook, resource adequacy, and seasonal reliability issues were also covered during the webinar.

Attendees were also introduced to a Cold Weather Event Training Package[85] designed by NERC training staff to assist non-traditional cold weather registered entities properly prepare for cold weather events. The materials were designed to be a guide to training sessions. These materials have been created as a foundation for training and remain in PowerPoint format to allow for customization based on registered entity needs. The NERC Event Analysis Program continues to establish the appropriate balance of data reporting for analysis and use by the industry. NERC is investigating ways to sustain positive efforts and improve the process.

Individual Human Performance

Analysis of event reports to date has identified possible workforce capability and human performance challenges that pose threats to reliability. Workforce capability and human performance is a broad topic and can most simply be divided into management, team, and individual levels. The following paragraphs provide more details on the types of errors that were observed in BPS events since the inception of the NERC Event Analysis Program, specifically events that involved human error or less-than-adequate training.

Generally, individual error is classified using the mode of performance in which the individual was operating when the error was committed. The NERC CCAP uses a popular methodology developed by Jens Rasmussen[86] in which errors occur in one of three modes of human performance, depending on the nature of the task and the level of experience with the particular situation. When information is first perceived and interpreted in the processing system, that information is processed cognitively in either the skill-based, knowledge-based, or rule-based levels.

Additionally, when contributing causes are considered, over half of the event reports to date indicate some management or organizational challenges. In an effort to support industry with these challenges, NERC held its second annual Human Performance conference in Atlanta, *Improving Human Performance on the Grid,* at the end of March 2013. The focus this year was not only on individual human performance, but the organizational and management challenges around human capital. The conference included industry and related professionals in the field, with over 200 attendees from all regions. The conference and associated workshops were very well received. NERC supported similar venues for industry in the spring in Edmonton, Canada, as well as in the fall in Salt Lake City. NERC provided industry support in this area to well over 250 registered entities across the eight Regions.

[83] http://www.nerc.com/pa/rrm/ea/February%202011%20Southwest%20Cold%20Weather%20Event/SW_Cold_Weather_Event_Final.pdf

[84] http://www.nerc.com/pa/rrm/ea/ColdWeatherTrainingMaterials/Relibility_Guideline_Generating_Unit_Winter_Weather_Readiness.pdf

[85] http://www.nerc.com/pa/rrm/ea/Pages/February-2011-Southwest-Cold-Weather-Event.aspx

[86] *Skills, rules, and knowledge: signals, signs and symbols and other distinctions in human performance models*. IEEE Transactions: Systems, Man & Cybernetics, 1983, SMC-13, pp.257-267.

The full conference presentations for the past Human Performance conference at NERC can be found at http://www.nerc.com/pa/rrm/hp/Pages/default.aspx.

Monitoring and Situation Awareness (Real-Time Tools)

Energy Management Systems (EMSes), including SCADA, digital or analog communications, and real-time tools, are vital for maintaining situational awareness and making operating decisions at both the individual and the organizational level. EMS systems are extremely reliable and are highly redundant. However, an outage of the EMS reduces visibility into a portion of the BES and increases the potential risk to the reliability of the BPS. The NERC Event Analysis Program has received over 80 Category 2b event reports in which a complete loss of SCADA, monitoring, or control has lasted for more than 30 minutes. NERC's commitment to active collaboration and sharing has allowed more information about these events to be adequately reviewed and shared among NERC Regions and the affected entities.

The Events Analysis Subcommittee (EAS) developed an Energy Management System Task Force (EMSTF) to analyze the events and data that were being collected about EMS outages and challenges. Industry also recognized that many EMS outages were significantly less than the 2b categorization yet impacted the decision-making activities for which the EMS is used. The 1h event category was created to learn more about these type of events. This category allows the EMSTF to collect a greater number of the occurrences of EMS partial outages and share this information with the industry.

From the event analysis reports and the work of the EAS, NERC published four lessons learned specifically about EMS outages and worked to build and support an industry-led EMS task force to support the EAS, under the NERC OC. The hard work and active sharing of this task force has reduced some of the residual risk associated with the potential loss of situation awareness and monitoring capability associated with this type of event and will continue to provide valuable information to the industry.

With the support of the EMSTF, NERC hosted its first Monitoring and Situational Awareness Conference Focused on Improving Energy Management Systems (EMS) reliability in Denver, September 18–19, 2013. The conference was scheduled to coincide with the NERC OC/PC/CIPC meetings. The conference brought together more than 90 operations and EMS experts from more than 55 registered entities, and a variety of vendors and consultants. The entities that attended came from all of the Regions.

The first day of the conference focused on the analysis of EMS outages and response strategies for alleviating the risk involved when EMS functionality is degraded or completely lost. The feedback from participants has been extremely positive. Attendees liked the technical nature of the presentations and the takeaways they could use to improve the processes and procedures at their own companies. Attendees greatly appreciated the openness with which the EMS shared their issues and corrective actions. Also appreciated was the platform that NERC provided to transparently share the events and learn from them. Industry requested a second workshop for 2014.

SCADA and real-time reliability tools are vital for maintaining situational awareness and making operating decisions at both the individual and the organizational level. EMS systems are typically extremely reliable and redundant; however, an outage of the EMS system increases the risk to the reliability of the BPS. Industry has demonstrated appropriate responses to EMS outages, and the ERO can now more accurately assess the residual risk to the BPS from EMS outages.

The full conference presentations for the past Monitoring and Situation Awareness conference can be found at http://www.nerc.com/pa/rrm/Resources/Pages/Conferences-and-Workshops.aspx.

Summary

The Event Analysis Program continues to provide valuable information for the industry to use to address potential threats or vulnerabilities to the reliability of the BPS. This continued active collaboration remains a testament to how much effort and how many resources are being expended in this area by the industry, as well as how important it is for the ERO and industry to truly understand the different contributors to events. The continued cooperation and collaboration with the industry is the hallmark to this program's success.

The ability to identify specific pieces of equipment that are potential threats, as well as emerging trends that increase risk to the system, illustrates the value of the event analysis program. These outcomes, coupled with the ability to actively share the information through lessons learned, webinars, technical conferences, and related venues, remain critical to the sustainment of high reliability.

Chapter 6 – Spare Equipment Database Initiative (2014)

Background

In June 2010, NERC issued a report titled *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*.[87] In a postulated high-impact low-frequency (HILF) event, such as a coordinated physical or cyber attack or a severe geomagnetic disturbance (GMD), long-lead-time electric transmission system equipment may be damaged. This could adversely impact system reliability.

Following a HILF event, increased intercompany coordination will help maximize the use of available spares in restoring the grid, thereby increasing the resiliency of the system. This chapter discusses a framework to facilitate that coordination.

Purpose

The purpose of the Spare Equipment Database Working Group (SEDWG) is to recommend a uniform approach to collecting information on long-lead-time electric transmission system equipment and develop a process for utilities to request assistance from other utilities.[88] Data collection is contained in the Spare Equipment Database (SED). The intent of the database is not to replace or supersede other existing transformer-sharing agreements. Rather, the intent is to facilitate timely communication of available equipment following a HILF event.

Spare Equipment Database

SEDWG reviewed various types of long-lead-time equipment, where "long lead time" is defined as six months or more. Following the review, it was determined that the initial focus should be large power transformers and generator step-up (GSU) transformers. In addition to long lead times, large power transformers also require substantial capital to secure. For these reasons, owners typically maintain an appropriate limited number of spares in the event of a failure. It may be beneficial in the future to expand SED to include other types of long-lead-time equipment.

2013 and 2014 Activities

In 2013, the primary focus of SEDWG was to increase participation. To that end, SEDWG worked with NERC to host a webinar to explain the program to registered entities and to solicit new participants. In addition, presentations were made at a variety of industry forums, including the NERC PC, MRO and RF regional meetings, and the American Public Power Association. The SEDWG also initiated development of a metric. In 2014, SEDWG will continue to increase SED awareness and participation and will complete the development and proposal for the metric.

Confidentiality of SED Process

Confidentiality has been and continues to be an important aspect of the SED. Participating organizations voluntarily identify and report spare equipment that meets predefined criteria in the database. The data collected provides essential information to enable automated queries of available equipment. In addition, equipment owner information is required to facilitate communication following a HILF event.

To maintain confidentiality of the information, SED utilizes a double-blind approach to preserve the anonymity of the registered SED participants, the requestor and the owner of the equipment.

---

[87] *High Impact, Low Frequency Event Risk to the North American Bulk Power System*, June 2010, http://www.nerc.com/pa/ci/resources/documents/hilf_report.pdf

[88] This task force will support the Electricity Sub-sector Coordinating Council's Critical Infrastructure Protection Roadmap, work plan items: 1) G - Critical Spares, and 2) P- GMD – Restore the Bulk Power System.

To initiate the search, the requestor completes an online form in SED and the program conducts a search. Upon completion, the requestor and NERC administrator are notified of the success of the search. From there, the SED program initiates a double-blind search-response procedure. SED generates messages to each unnamed TO identified by the search without disclosing what equipment is needed, how many pieces of equipment are requested, or the name of the requestor.

Owners who wish to proceed with discussing a sale/lease/exchange can use the double-blind search process to respond to the unnamed requestor to open an active discussion. Any decision to provide additional information is the responsibility of the owners. The NERC SED administrator is informed of all communications conducted via the SED link. The requestor and owner may then work toward a settlement acceptable to both parties.

A complete description of the SED search process and a special report on the SED can be found on NERC's website.[89]

Registration and Contact Information

For further information related to the SED program, please visit:
http://www.nerc.com/pa/RAPA/sed/Pages/Spare-Equipment-Database-(SED).aspx

[89] *Special Report: Spare Equipment Database System*, October 2011, http://www.nerc.com/docs/pc/sedtf/SEDTF_Special_Report_October_2011.pdf

Appendix A – Statistical Analysis for Chapter 3

Study Method

Defining BPS Impact from Transmission Risk

To define the impact, or severity, of each TADS event, the SRI quantitatively compares events. The TADS outage data is used to populate the statistical analysis study. For this analysis, the transmission outage impact component of the SRI quantifies BPS impacts. Since transmission outages are a significant contributor to the overall SRI, this chapter focuses on categorizing the individual TADS events based on TADS outage ICCs.

The SRI presented in Chapter 2 consists of several weighted risk impact components: generation, transmission, and load loss.[90] The transmission outage impact component of the SRI is defined as $w_T \times N_T$ where w_T is a weighting factor of 30 percent and N_T is the severity impact of a given day's transmission outages on the BPS based on TADS outages.

In this appendix and in Chapter 3, Equation A.1 is used to calculate the transmission severity component of a TADS event. The severity of a transmission outage is calculated based on its assumed contribution of power flow through transmission circuits. The average power flow MVA values, or equivalent MVA values used in Equation A.1, are shown in Table A.1. These equivalent MVA values are also applied to the denominator of the transmission severity equation to normalize the function. The TADS event severity is then analyzed by ICC to investigate relative information between the ICCs instead of being added to generation and load-loss components to calculate a daily SRI as used in Chapter 2.

For normalization, the total number of transmission circuits from the same year as the event is multiplied by each voltage class's equivalent MVA rating. For example, if an outage occurred in 2009, the normalization would use the total number of transmission circuits in 2009. This allows comparison of TADS events across years while taking into account the changing number of circuits within the BPS.

$$Transmission\ Severity_{Trans} = \frac{\sum_{Voltage\ Class}(MVA_{avg} \times AC\ Circuits\ Outages)}{\sum_{Voltage\ Class}(MVA_{avg} \times Total\ AC\ Circuits)}$$

Equation A.1

Table A.1: Transmission Severity Equivalent MVA Values

Voltage Class	Equivalent MVA Value
200–299 kV	700
300–399 kV	1300
400–599 kV	2000
600–799 kV	3000

[90] http://www.nerc.com/docs/pc/rmwg/pas/index_team/sri_equation_refinement_may6_2011.pdf, pp. 2-3.

Determining Initiating Causes and Probability

TADS events are categorized by ICCs.[91] These ICCs facilitate the study of cause-effect relationships between each event's ICC and event severity. The procedure illustrated in Figure A.1 is used to determine a TADS event's ICC. The procedure that defines ICCs for a TADS event allows ICC assignment to a majority of transmission outage events recorded in TADS. There are 18,754 events with ICCs assigned, comprising 99.4 percent of the total number of TADS events for the years 2008–2013. These events reflect 98.8 percent of the total calculated transmission severity of the database. Table A.2 provides the corresponding available event data by year.

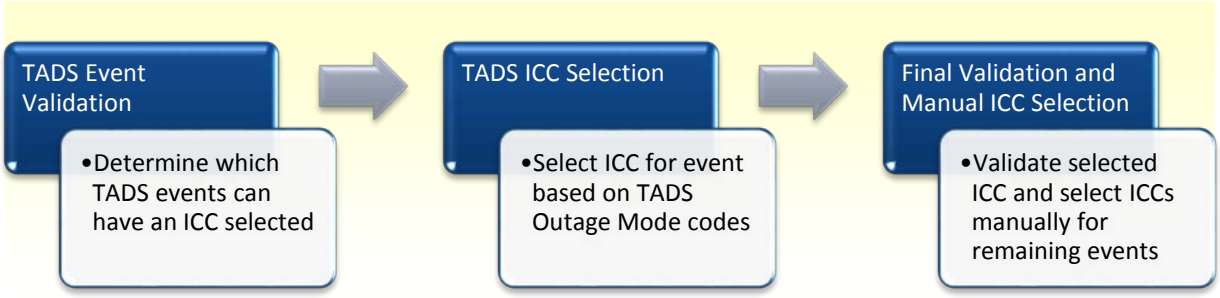


Figure A.1 TADS Event Initiating Cause Code Selection Procedure

Table A.2: TADS Outage Events Summary (2009–2013)

Summary	2009	2010	2011	2012	2013	2009-2013
Number of TADS events	3,705	3,917	3,934	3,753	3,557	18,866
Number of events with ICC assigned	3,684	3,895	3,894	3,724	3,557	18,754
Percentage of events with ICC assigned	99.4%	99.4%	99.0%	99.2%	100.0%	99.4%
Transmission severity all TADS events	643.8	675.8	665.7	612.4	506.0	3,103.7
Transmission severity of events with ICC assigned	636.8	667.5	654.6	602.1	506.0	3,066.9
Percentage of Transmission severity of events with ICC assigned	98.9%	98.8%	98.3%	98.3%	100.0%	98.8%

For TADS events initiated by a common cause, the probability[92] of observing that the event initiates during a given hour is estimated using the corresponding event occurrences reported in TADS. Namely, the probability of the occurrence of the event is the total number of a given type of event during the study period divided by the total number of hours in the same period. Therefore, the sum of the estimated probabilities for all events is equal to the estimated probability of any event during a given hour. With the development of the transmission severity measure and TADS event ICCs, it is possible to statistically analyze the most recent five years of TADS data (2009–2013). The analysis shows which ICCs result in the highest transmission severity and finds statistically significant changes in transmission severity by ICC over time.

[91] For detailed definitions of TADS cause codes, please refer to: http://www.nerc.com/pa/RAPA/tads/Transmission Availability Data System Working Group/TADS Definitions (Appendix 7).pdf, January 14, 2013, pp. 19-20.

[92] Probability is estimated using event occurrence frequency of each ICC type without taking into account the event duration.

Determining Relative Risk

Each study followed a similar approach, as shown in Figure A.2. Each study was performed to determine the correlation between each ICC and transmission severity, and whether a statistically significant confidence level was 95 percent or higher. Then, sample distributions were studied to determine any statistically significant pair-wise differences in expected transmission severity between ICCs, including a time trend analysis where applicable. Finally, the relative risk was calculated for each ICC group.

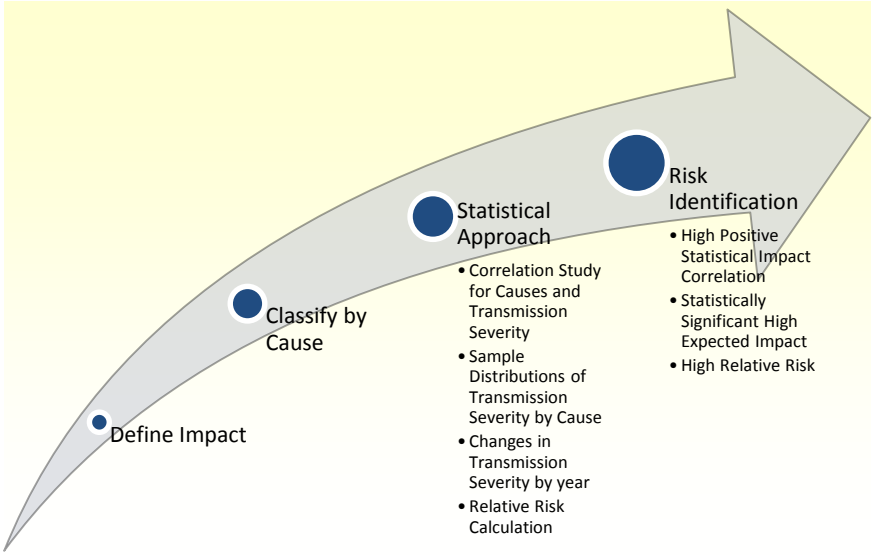


Figure A.2: Risk Identification Method

To study the relationship between ICCs and the transmission severity of TADS events, NERC investigated the statistical significance of the correlation between transmission severity and the indicator function[93] of a given ICC.[94] The test is able to determine a statistically significant positive or negative correlation between ICC and transmission severity.

Distributions of transmission severity for the entire dataset were examined separately for events with a given ICC. A series of t-tests[95] were performed to compare the expected transmission severity of a given ICC with the expected severity of the rest of the events at significance level of 0.05. Then, the Fisher's Least Square[96] difference method was applied to determine statistically significant[97] differences in the expected transmission severity for all pairs of ICCs.

Where applicable, a time trend analysis was performed. Statistically significant differences in the expected transmission severity for each ICC group were analyzed for each year of data. This showed if the average transmission severity for a given ICC group had changed over time.

[93] The indicator function of a given ICC assigns value 1 to an event with this ICC and value 0 to the rest of the events.

[94] For each ICC, a null statistical hypothesis on zero correlation at significance level 0.05 was tested. If the test resulted in rejection of the hypothesis, it is concluded that a statistically significant positive or negative correlation between an ICC and transmission severity exists; the failure to reject the null hypothesis indicates no significant correlation between ICC and transmission severity.

[95] For t-test, see D. C. Montgomery and G. C. Runger, Applied Statistics and Probability for Engineers. Fifth Edition. 2011. John Wiley & Sons. Pp. 361-369.

[96] For Fisher's Least Significance Difference (LSD) method or test, see D. C. Montgomery and G. C. Runger, Applied Statistics and Probability for Engineers. Fifth Edition. 2011. John Wiley & Sons. Pp. 524-526.

[97] At significance level of 0.05.

Finally, relative risk was calculated for each ICC group. The impact of an outage event was defined as the expected transmission severity associated with a particular ICC group. The probability that an event from a given group initiates during a given hour is estimated from the frequency of the events of each type without taking into account the event duration. The risk per hour of a given ICC was calculated as the product of the probability per hour and the expected severity (impact) of an event from this group. The relative risk was then defined as the percentage of the risk associated with each ICC out of the total (combined for all ICC events) risk per hour.

Table A.3 lists annual counts and hourly event probability of TADS events by ICC.[98] The three ICCs with the largest number of events are weather (with and without lightning), Unknown, and a group defined as Reliability Metrics (composed of ICCs of Human Error, Failed AC Circuit Equipment, Failed AC Substation Equipment, and Failed Protection System Equipment). The four ICCs grouped as Reliability Metrics are related to ALR6-12, ALR6-14, ALR6-13 and ALR6-11 and are combined in one section of the table. Metrics are provided for each of the ICCs in the group, as well as for the group as a whole.

Almost all TADS ICC groups have sufficient data available to be used in a statistical analysis. Only four ICCs (Vegetation; Vandalism, Terrorism, or Malicious Acts; Environmental; and Failed AC/DC Terminal Equipment) do not have enough observations. These are combined into a new group, named "Combined Smaller ICC Groups," that can be statistically compared to every other group and also studied with respect to annual changes of transmission severity.

Table A.3: TADS Events and Hourly Event Probability by ICC

Initiating Cause Code	2009	2010	2011	2012	2013	2009–2013	Event Probability/Hour
Reliability Metrics	**1043**	**1054**	**1120**	**1042**	**908**	**5167**	**0.1179**
Human Error	291	305	291	307	280	1474	**0.0336**
Failed AC Circuit Equipment	257	277	306	261	248	1349	**0.0308**
Failed AC Substation Equipment	266	238	289	248	192	1233	**0.0281**
Failed Protection System Equipment	229	234	234	226	188	1111	**0.0254**
Lightning	789	741	822	852	814	4018	**0.0917**
Unknown	673	821	782	710	712	3698	**0.0844**
Weather Excluding Lightning	534	673	539	446	434	2626	**0.0599**
Foreign Interference	199	173	170	170	181	893	**0.0204**
Contamination	96	145	132	160	152	685	**0.0156**
Power System Condition	112	74	121	77	109	493	**0.0112**
Other	107	84	91	104	64	450	**0.0103**
Fire	92	84	63	106	130	475	**0.0108**
Combined Smaller ICC groups	**39**	**46**	**54**	**57**	**53**	**249**	**0.0057**
Vegetation	29	27	44	43	36	179	**0.0041**
Vandalism, Terrorism, or Malicious Acts	4	6	5	10	9	34	**0.0008**
Environmental	5	11	5	4	8	33	**0.0008**
Failed AC/DC Terminal Equipment	1	2	0	0	0	3	**0.0001**
All TADS events	**3705**	**3917**	**3934**	**3753**	**3557**	**18866**	**0.4305**
All with ICC assigned	**3684**	**3895**	**3894**	**3724**	**3557**	**18754**	**0.4279**

[98] For detailed definitions of TADS cause codes, please refer to: http://www.nerc.com/pa/RAPA/tads/Transmission Availability Data System Working Grou/TADS Definitions (Appendix 7).pdf, January 14, 2013, pp. 19-20.

Correlation between ICC and Transmission Severity

Figure A.3 shows the correlations between calculated transmission severity and the given ICC. To study a relationship between ICC and transmission severity of TADS events, the statistical significance of the correlation between transmission severity and the indicator function[99] of a given ICC was investigated.[100] A statistically significant positive or negative correlation between ICC and transmission severity could be determined by the test. A statistically significant positive correlation of ICC to transmission outage severity would indicate a greater likelihood that an event with this ICC would result in a higher transmission outage severity. A stark negative correlation would indicate the contrary; in this case, a lower transmission outage severity would be likely. If no significant correlation is found, it indicates the absence of a linear relationship between ICC and the transmission outage severity, and that the events with this ICC have an expected transmission severity similar to all other events from the database.

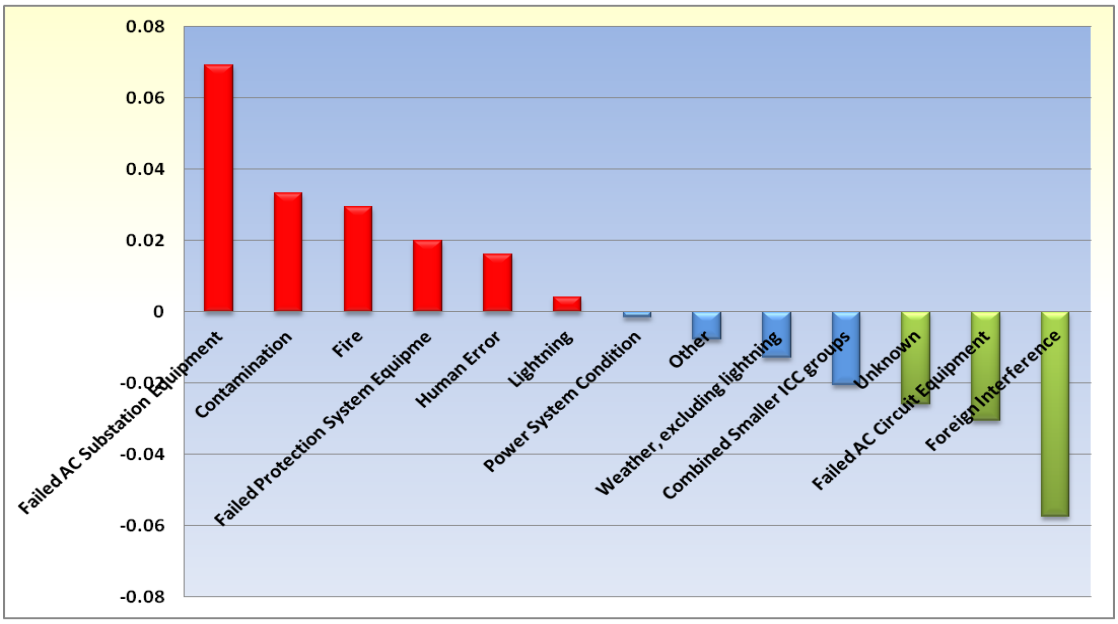


Figure A.3: Correlation between Augmented ICC and TS of TADS Events (2012–2013)

There were three key outcomes of all the tests. To begin, Failed AC Substation Equipment, Contamination, Fire, Reliability Metrics, Human Error, and Failed Protection System Equipment have statistically significant positive correlation with transmission severity. The expected severity of events with each of these ICCs is greater than the expected severity compared to other ICC events. Secondly, Foreign Interference, Failed AC Circuit Equipment, Smaller ICC Groups Combined, Unknown, and Weather Excluding Lightning have a statistically significant negative correlation with transmission severity. The expected severity of events initiated by these causes is smaller than the expected transmission severity of the remaining dataset. Finally, for each of the remaining groups (Power System Condition, Lighting, Other), the difference between transmission severity for the group and for its complement is not statistically significant.

Distribution of Transmission Severity by ICC

Next, the distribution of transmission severity for the entire dataset was studied separately for events with a given ICC. The transmission severity of the 2009–2013 dataset has a sample mean of 0.165 and the sample standard deviation of 0.108. The sample statistics for transmission severity by ICC are listed in Table A.4.

[99] The indicator function of a given ICC assigns value 1 to an event with this ICC and value 0 to the rest of the events.

[100] For each ICC, a null statistical hypothesis on zero correlation at significance level 0.05 was tested. If the test resulted in rejection of the hypothesis, it is concluded that a statistically significant positive or negative correlation between an ICC and transmission severity exists; the failure to reject the null hypothesis indicates no significant correlation between ICC and transmission severity.

The groups of events initiated by Failed AC Substation Equipment, Fire, and Failed Protection System Equipment not only have statistically[101] greater expected severity than the rest of the events, but the variance of transmission severity (and its standard deviation) for each of these groups is also statistically greater than the variance for the other events. The greater variance is an additional risk factor since it indicates more frequent occurrences of events with high transmission severity.

Table A.4 provides a column that indicates which other ICCs are statistically smaller than a given ICC referenced by the table's column 1 index. For example, transmission severity for Human Error (#5) is significantly smaller than for Failed AC Substation Equipment (#1), while Fire (#2) is not statistically significantly smaller than Failed AC Substation Equipment.

Table A.4: Distribution of Transmission Severity by ICC (2009–2013)

#	Initiating Cause Code	Average TS of Events with the ICC	Is Expected TS Statistically Significantly Bigger than for the Rest of the Events with ICC Assigned?	ICC with Statistically Significantly Smaller TS	Standard Deviation of TS
1	Failed AC Substation Equipment	0.191	Yes	3,4,5,6,7,8,9,10,11,12,13	0.135
2	Fire	0.183	Yes	5,6,7,8,9,10,11,12,13	0.131
3	Contamination	0.182	Yes	5,6,7,8,9,10,11,12,13	0.107
4	Failed Protection System Equipment	0.172	Yes	8,9,10,11,12,13	0.123
5	Human Error	0.169	Yes	8,10,11,12,13	0.102
6	Lightning	0.164	No	10,11,12,13	0.095
	All TADS events	**0.165**	**N/A**	**N/A**	**0.108**
	All with ICC assigned	**0.164**	**N/A**	**N/A**	**0.106**
7	Power System Condition	0.163	No	12,13	0.185
8	Weather Excluding Lightning	0.160	No	11,12,13	0.095
9	Other	0.158	No	13	0.216
1	Unknown	0.158	No	11,12,13	0.078
1	Failed AC Circuit Equipment	0.152	No	13	0.086
1	Combined Smaller ICC groups	0.144	No	none	0.132
1	Foreign Interference	0.136	No	none	0.065

[101] At significance level 0.05

Average Transmission Severity by ICC: Annual Changes

Year-over-year changes in calculated transmission severity by ICC were reviewed next. Figure A.4 shows changes in the average severity for each ICC and for the 2009–2013 dataset. The groups of ICC events are listed from left to right by descending average transmission severity for the five-year data. The largest average transmission severity over the five-year period was observed for events initiated by Failed AC Substation Equipment; the single-highest annual average transmission severity is observed for 2010 events initiated by Fire. NERC's investigation revealed that two wildfires[102] initiated the most severe events in this category.

It should be noted that for all ICC groups except Power System Condition, Combined Smaller ICC Groups, and Foreign Interference, the 2013 average transmission severity reduced compared with 2012; and for all groups except Power System Condition, it stayed below the five-year average transmission severity of the group.

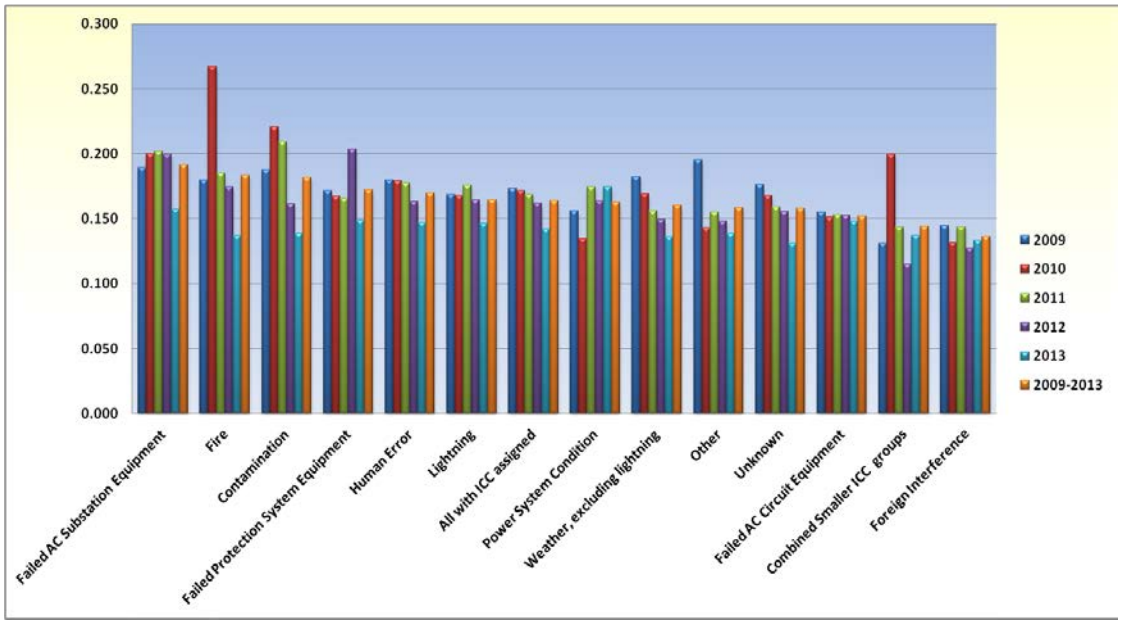


Figure A.4: Average Transmission Severity of TADS Events by ICC (2009–2013)

The following series of graphs shows changes in the average transmission severity by year for four groups of ICCs. For each group, the graph is accompanid by a list of statistically significant[103] changes (decreases and increases).

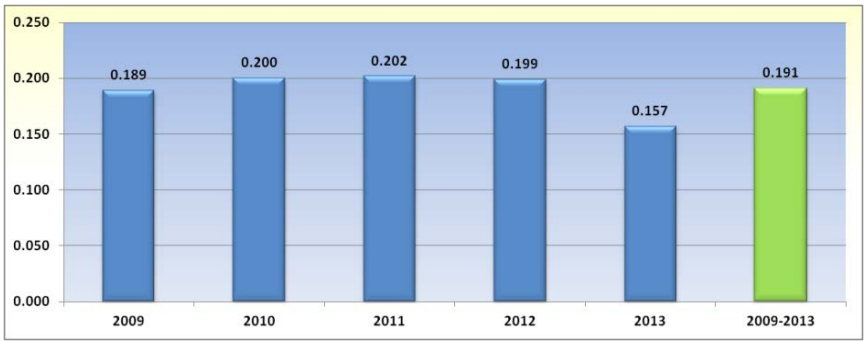


Figure A.5: Average Transmission Severity of Events Initiated by Failed AC Substation Equipment (2009–2013)

- Statistically significant year-over-year increases
  - none
- Statistically significant year-over-year decreases
  - 2009 vs. 2013
  - 2010 vs. 2013
  - 2011 vs. 2013
  - 2012 vs. 2013

[102] Québec wildfires June 22-23, 2010, and Sequoia National Forest fire in California, July 29-30, 2010

[103] This summary only lists changes that are statistically significant at the 0.05 level.

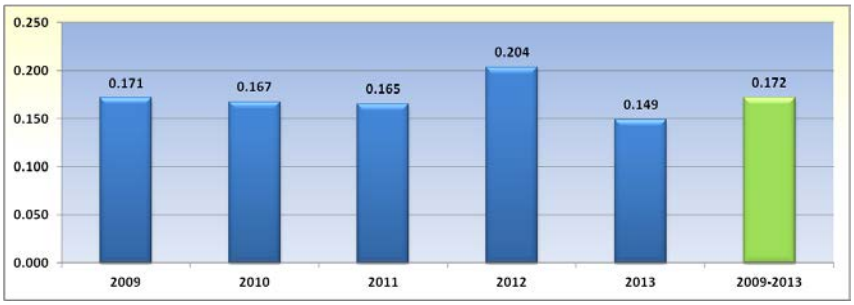


Figure A.6: Average Transmission Severity of Events Initiated b Failed Protection System Equipment (2009–2013)

- Statistically significant year-over-year increases
  - 2009 vs. 2012
  - 2010 vs. 2012
  - 2011 vs. 2012
- Statistically significant year-over-year decreases
  - 2012 vs. 2013

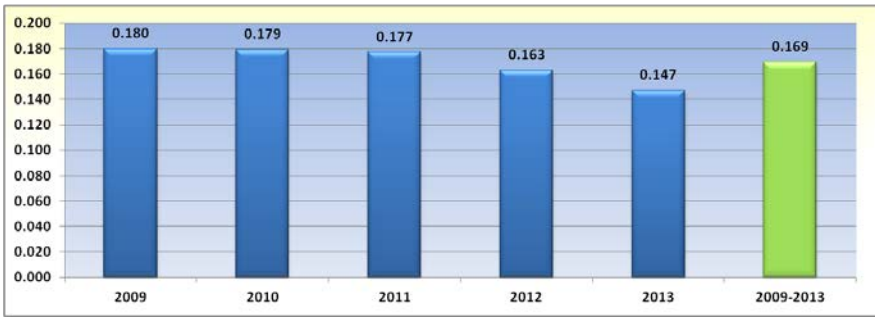


Figure A.7: Average Transmission Severity of Events Initiated by Human Error (2009–2013)

- Statistically significant year-over-year increases
  - none
- Statistically significant year-over-year decreases
  - 2009 vs. 2012
  - 2009 vs. 2013
  - 2010 vs. 2012
  - 2010 vs. 2013
  - 2011 vs. 2013

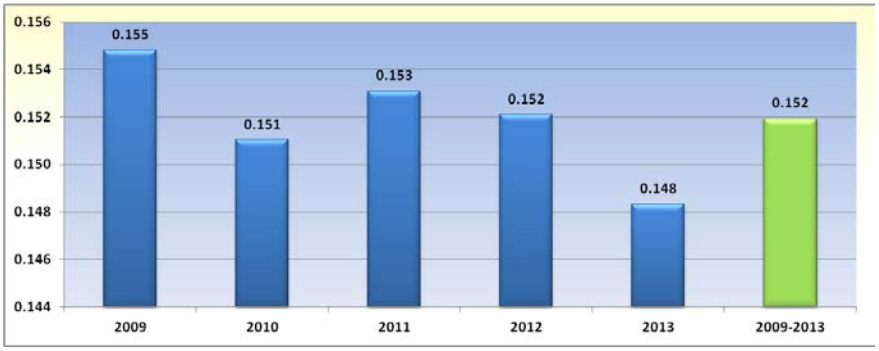


Figure A.8: Average Transmission Severity of Events Initiated by Failed AC Circuit Equipment (2009–2013)

- Statistically significant year-over-year increases
  - none
- Statistically significant year-over-year decreases
  - none

Finally, for the 2008–2012 set of TADS events, changes in the average transmission severity by year are as follows:

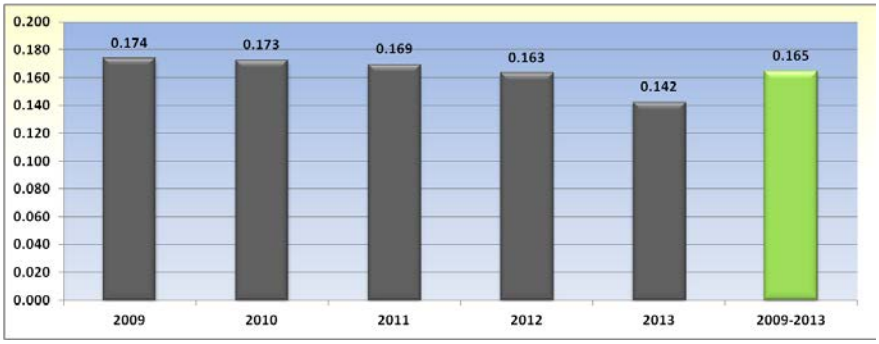


Figure A.9: Average Transmission Severity of TADS Events (2009–2013)

- Statistically significant year-over-year increases
  - none
- Statistically significant year-over-year decreases
  - 2009 vs. 2012
  - 2010 vs. 2012
  - 2010 vs. 2013
  - 2011 vs. 2012
  - 2011 vs. 2013
  - 2012 vs. 2013

Total (Combined) Transmission Severity by ICC: Annual Changes

Total annual transmission severity associated with each ICC by year (the sum of the transmission severity of all events from the group) is listed in Table A.5.

Table A.5: Annual Transmission Severity by ICC (2009–2013)

Group of TADS events	2009	2010	2011	2012	2013
Reliability Metrics	**181.7**	**183.2**	**195.4**	**185.1**	**136.1**
Human Error	52.3	54.7	51.5	50.0	41.2
Failed AC Circuit Equipment	39.8	41.8	46.8	39.7	36.8
Failed AC Substation Equipment	50.4	47.6	58.3	49.3	30.2
Failed Protection System Equipment	39.3	39.1	38.7	46.0	28.0
Lightning	132.7	124.4	144.5	139.8	119.1
Unknown	118.4	137.9	124.2	110.2	93.4
Weather Excluding Lightning	97.2	113.6	83.9	66.6	59.3
Foreign Interference	28.8	22.7	24.4	21.6	24.1
Contamination	18.0	32.0	27.6	25.8	21.0
Power System Condition	17.4	10.0	21.1	12.6	19.0
Fire	16.5	22.4	11.7	18.5	17.8
Other	20.9	12.0	14.1	15.4	8.9
Combined Smaller ICC Groups	**5.1**	**9.2**	**7.8**	**6.5**	**7.3**
All TADS Events	**643.8**	**675.8**	**665.7**	**612.4**	**506.0**
All with ICC Assigned	**636.8**	**667.5**	**654.6**	**602.1**	**506.0**

Figure A.10 shows changes in the total transmission severity of TADS events by year.

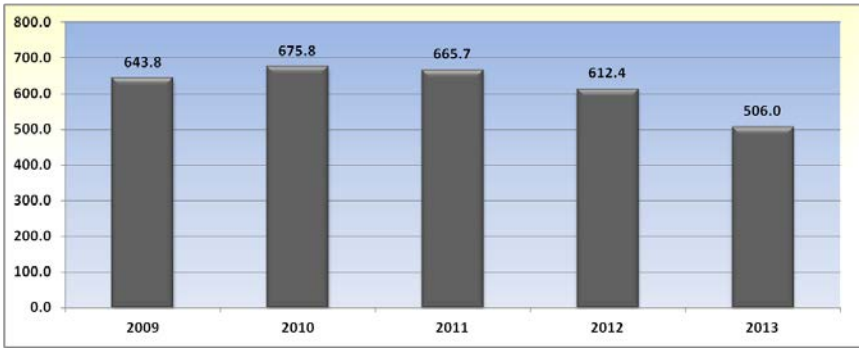


Figure A.10: Total Transmission Severity of TADS Events (2009–2013)

- Statistically significant year-over-year increases
  - none
- Statistically significant year-over-year decreases
  - 2010 vs. 2012
  - 2010 vs. 2013
  - 2011 vs. 2012
  - 2011 vs. 2013
  - 2012 vs. 2013

In particular, changes in the total transmission severity of events with a common ICC related to one of the ALR metrics are shown in Figure A.11.

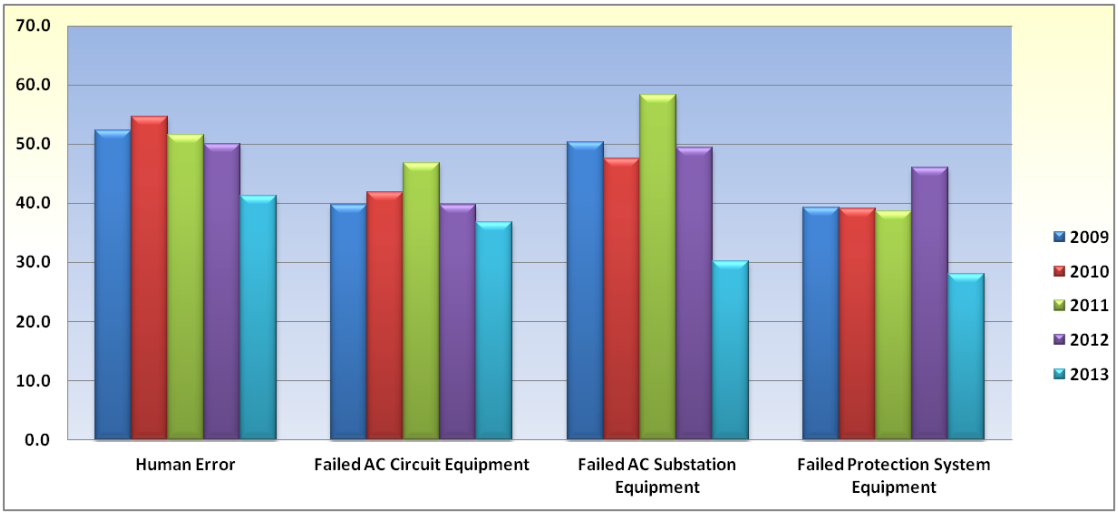


Figure A.11: Total Transmission Severity by Year

There were several statistically significant increases and decreases over time for ICCs related to Adequate Level of Reliability (ALR) metrics, as summarized below. For the annual total transmission severity of TADS events initiated by Human Error, there were:

- no statistically significant increases;
- statistically significant year-over-year decreases:
  - 2009 vs. 2013
  - 2010 vs. 2012
  - 2010 vs. 2013
  - 2011 vs. 2013

For the annual total transmission severity of TADS events initiated by Failed AC Circuit Equipment, there were:

- no statistically significant changes

For the annual total transmission severity of TADS events initiated by Failed AC Substation Equipment, there were:

- no statistically significant increases;
- statistically significant year-over-year decreases:
  - 2009 vs. 2013
  - 2010 vs. 2013
  - 2011 vs. 2013
  - 2012 vs. 2013

For the annual total transmission severity of TADS events initiated by Failed Protection System Equipment, there were:

- statistically significant year-over-year increases:
  - 2009 vs. 2012

- 2011 vs. 2012

- statistically significant year-over-year decreases:
  - 2012 vs. 2013.

Thus, all groups of TADS events from Reliability Metrics had a reduction in their total transmission severity in 2013 as compared with any other year from 2009 to 2012; moreover, many of these reductions were statistically significant.

Transmission Severity Risk and Relative Risk of TADS Events by ICC

The risk of each ICC group can be defined as the total transmission severity associated with this group; its relative risk is equal to the percentage of the group transmission severity in the 2009–2013 database. Equivalently, the risk of a given ICC per hour can be defined as the product of the probability that an event with this ICC initiates during an hour and the expected severity (impact) of an event from this group. For any ICC group, the relative risk per hour is the same as the relative risk for five years (or any other time period). Figure A.12 shows year-over-year changes in the relative risk of TADS events by ICC.

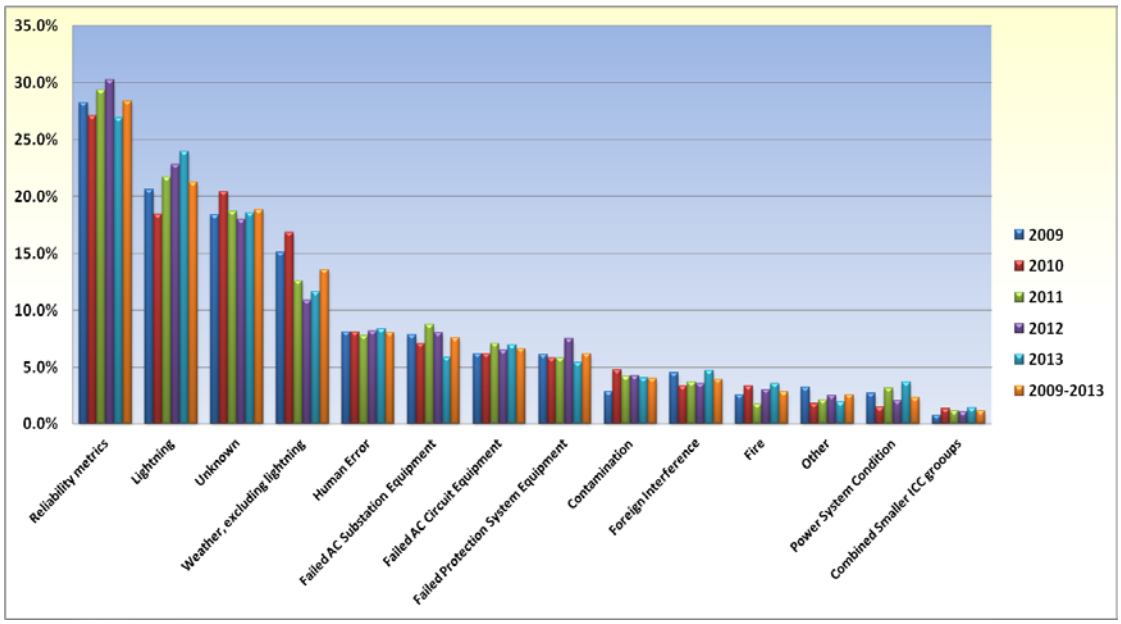


Figure A.12: Relative Transmission Severity Risk by ICC and Year

2012–2013 Study with Augmented Event Types

TOs provided transmission performance information using the NERC TADS process. The data used in these studies includes momentary and sustained automatic outages of ac transmission circuits (overhead and underground) that operate at voltages greater than or equal to 200 kV.

TADS event-type reporting was modified in 2012 to further distinguish normal clearing events from abnormal clearing events. To introduce the additional data into this study where this level of detail is not available for prior years, TADS events with protection system misoperations—event types 61 dependability[104] (failure to operate)

[104] Event Type 61 Dependability (failure to operate): one or more automatic outages with delayed fault clearing due to failure of a single protection system (primary or secondary backup) under either of these conditions:
- Failure to initiate the isolation of a faulted power system Element as designed, or within its designed operating time, or
- In the absence of a fault, failure to operate as intended within its designed operating time.

and 62 security[105] (unintended operation)—are included with ICCs as shown in Table A.6. The new ICCs developed are analogous to protection system misoperations, which are comprised of Failed Protection System Equipment (FPSE) and Human Error with event type 61 or 62 (HE and Type 61/62). Aggregate totals of 2012–2013 TADS events by augmented ICC are provided in Table A.6. Events initiated by Misoperations comprise 8.2 percent of all events and represent the fourth-largest group of events (after weather-related and Unknown ICCs.)

Table A.6: TADS Outage Events by Augmented ICC (2012-2013)

Initiating Cause Code	2012	2013	2012-2013
Lightning	852	813	1665
Unknown	710	712	1422
Weather Excluding Lightning	446	433	879
Misoperation: FPSE OR (HE AND Type 61/62)	321	281	602
Failed AC Circuit Equipment	261	248	509
Failed AC Substation Equipment	248	191	439
Human Error AND NOT(Type 61 OR Type 62)	212	191	403
Foreign Interference	170	181	351
Contamination	160	151	311
Fire	106	130	236
Power System Condition	77	109	186
Other	104	64	168
Vegetation	43	36	79
Vandalism, Terrorism, or Malicious Acts	10	9	19
Environmental	4	8	12
All with ICC assigned	**3724**	**3557**	**7281**
In TADS	**3753**	**3557**	**7310**

Human Error ICCs with event type 61 or 62 correspond to two misoperation causes:[106] incorrect setting/logic/design error or as-left personnel error. These ICCs also include Human Error events that occur during maintenance and testing activities that would not traditionally be classified as a misoperation. Historically, Human Error events during maintenance and testing that results in protection system activation have contributed to large disturbance events. Therefore, these events were included to capture this risk. After reclassifying 184 events that were initially identified as Human Performance but were reclassified as Misoperations, Human Error now accounts for 5.5 percent of all 2012–2013 TADS events.

[105] Event Type 62 Security (unintended operation): one or more automatic outages caused by improper operation (e.g., overtrip) of a protection system resulting in isolating one or more TADS elements it is not intended to isolate, either during a fault or in the absence of a fault.

[106] http://www.nerc.com/comm/PC/Performance%20Analysis%20Subcommittee%20PAS%20DL/Protection_System_Misoperation_Reporting_Template_Final.xlsx, January 16, 2013.

Figure A.13 shows the correlation between calculated transmission severity and each ICC. A red bar in Figure A.13 corresponds to an ICC that has a statistically significant positive correlation with transmission severity, a green bar corresponds to an ICC that has a statistically significant negative correlation, and a blue bar corresponds to an ICC that has a correlation that is not statistically significant. A statistically significant positive correlation of an ICC with a transmission outage severity would indicate a higher likelihood that an event with that ICC will result in a higher transmission outage severity. A statistically significant negative correlation indicates the contrary; in this case, a lower transmission outage severity would be likely. If a correlation is not statistically significant, this implies that a positive or negative correlation was very likely observed by a mere chance, and there is, in fact, no relationship between ICC and the transmission outage severity. The events with this ICC have an expected transmission severity similar to all other events from the database.

Failed AC Substation Equipment and Misoperations had the largest and most statistically significant positive correlation with 2012–2013 automatic transmission outage severity. In other words, TADS events initiated by these two causes tended to have higher transmission severity than other TADS events that occurred in 2012 and 2013.

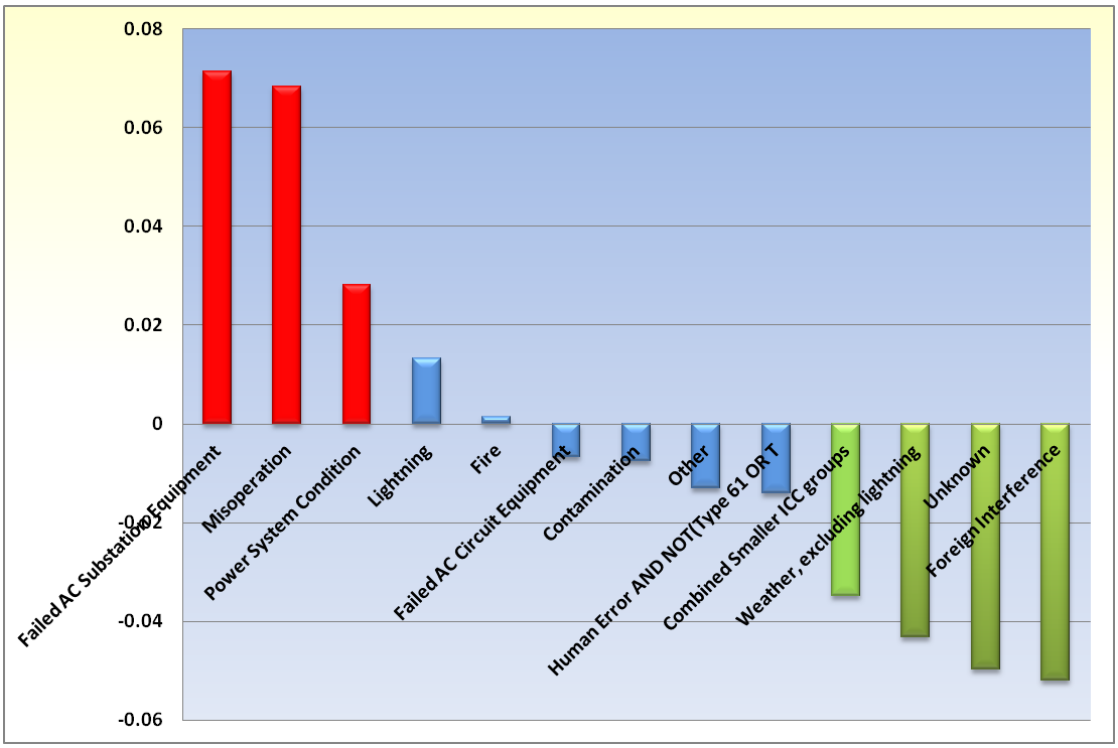


Figure A.13: Correlation between Augmented ICC and TS of TADS Events (2012–2013)

Relative risk of the 2012–2013 TADS events by augmented ICC is listed in Table A.7. The probability that an event from a given group initiated during a given hour is estimated from the frequency of the events of each type without taking into account the event duration. Excluding weather-related and Unknown events, events initiated by Misoperations and by Failed AC Substation Equipment had the largest shares in the total transmission severity and contributed 9.4 and 7.1 percent, respectively, to transmission severity relative risk.

Table A.7: Relative Risk by Augmented ICC (2012–2013)

Group of TADS events	Probability that an Event from a Group Starts during a Given Hour	Expected Impact (Expected Transmission Severity of an Event)	Risk Associated with a Group Per Hour	Relative Risk by Group (%)
Lightning	0.095	0.155	0.015	**23.1**
Unknown	0.081	0.143	0.012	**18.2**
Weather Excluding Lightning	0.050	0.143	0.007	**11.2**
Misoperation	0.034	0.175	0.006	**9.4**
Failed AC Substation Equipment	0.025	0.180	0.005	**7.1**
Failed AC Circuit Equipment	0.029	0.151	0.004	**6.9**
Human Error AND NOT(Type 61 OR Type 62)	0.023	0.150	0.003	**5.4**
Contamination	0.018	0.149	0.003	**4.2**
Foreign Interference	0.020	0.130	0.003	**4.1**
Fire	0.013	0.154	0.002	**3.2**
Power System Condition	0.011	0.170	0.002	**2.8**
Other	0.010	0.145	0.001	**2.2**
Combined Smaller ICC groups	**0.006**	**0.126**	**0.001**	**1.2**
All TADS events	**0.417**	**0.153**	**0.064**	**100.0**
All with ICC assigned	**0.415**	**0.152**	**0.063**	**99.1**

Since additional outage detail is available for two years, annual changes in transmission severity of the events initiated by Misoperations can now be studied. The analysis is provided in Table A.8. Statistical tests led to the conclusion that both the average transmission severity of these events and their total transmission severity statistically significantly decreased in 2013 versus 2012.

Table A.8: Relative Risk by Augmented ICC (2012–2013)

TADS events initiated by Misoperations	2012	2013
Average TS of an event	0.198	0.149
Total TS of the group	63.6	41.8

CDM Events: Definitions and Breakdown by ICC

As part of the analysis, a breakdown of ICCs was performed for TADS events containing Common- or Dependent-Mode (CDM) outages. These TADS events have more transmission severity than TADS events with a Single-Mode outage. TADS events were separated into two types: Single-Mode events and CDM events. A Single-Mode event is defined as a TADS event with a single-element outage. A CDM TADS event is a TADS event in which all outages have one of the modes (other than Single Mode) in Table A.9.

Table A.9: Outage Mode Codes

Outage Mode Code	Automatic Outage Description
Single Mode	A single-element outage that occurs independently of another automatic outage
Dependent Mode Initiating	A single-element outage that initiates at least one subsequent element automatic outage
Dependent Mode	An automatic outage of an element that occurred as a result of an initiating outage, whether the initiating outage was an element outage or a non-element outage
Common Mode	One of at least two automatic outages with the same ICC where the outages are not consequences of each other and occur nearly simultaneously
Common Mode Initiating	A common-mode outage that initiates one or more subsequent automatic outages

Some TADS events were entered as a combination of Single-Mode outages and other outage modes. These events were manually examined to determine if the event was Single-Mode or CDM. For some events, it was not possible to determine whether the event was Single-Mode or CDM, nor was it possible to tell the ICC for the event. These events, approximately 0.4 percent of all TADS events, were removed from the study.

Table A.10 lists CDM events by ICC in the 2009–2013 database and their percentages with respect to all TADS events with a given ICC. Similar to all TADS events, Lightning initiated the largest number of CDM events. CDM events initiated by Failed AC Substation Equipment comprise the second largest group, followed by Weather Excluding Lightning, and Human Error. Overall, 3,227 CDM events were defined, representing 17.1 percent of all TADS events from 2009 to 2013. Out of these, 3,136 are assigned to one of the 17 ICCs.

Almost all ICC groups of CDM events for five years have a sufficient sample size to be used in a statistical analysis, but the sample size is not enough to track statistically significant year-over-year changes in transmission severity. Four ICCs (Vegetation; Vandalism, Terrorism, or Malicious Acts; Environmental, and Failed AC/DC Terminal Equipment) must be combined to comprise a new group, Combined Smaller ICC Groups, that can be statistically compared to every other group.

Table A.10: CDM Events and Hourly Event Probability by ICC (2009–2013)

Initiating Cause Code	ALL TADS events	CDM events	CDM as % of ALL	Event Probability/Hour
Reliability Metrics	**5167**	**1249**	**24.2**	**0.0285**
Failed AC Substation Equipment	1233	444	36.0	0.0101
Failed Protection System Equipment	1111	296	26.6	0.0068
Human Error	1474	324	22.0	0.0074
Failed AC Circuit Equipment	1349	185	13.7	0.0042
Lightning	4018	559	13.9	0.0128
Weather Excluding Lightning	2626	334	12.7	0.0076
Unknown	3698	306	8.3	0.0070
Power System Condition	493	310	62.9	0.0071
Other	450	109	24.2	0.0025
Foreign Interference	893	97	10.9	0.0022
Fire	475	77	16.2	0.0018
Contamination	685	59	8.6	0.0013
Combined Smaller ICC groups	**249**	**36**	**14.5**	**0.0008**
Vegetation	179	14	7.8	0.0003
Environmental	33	11	33.3	0.0003
Failed AC/DC Terminal Equipment	3	3	100.0	0.0001
Vandalism, Terrorism, or Malicious	34	8	23.5	0.0002
All In TADS	**18866**	**3227**	**17.1**	**0.0736**
All with ICC assigned	**18754**	**3136**	**16.7**	**0.0716**

CDM Events: Correlation between ICC and Transmission Severity

To study a relationship between ICC and transmission severity of TADS events, the statistical significance of the correlation between transmission severity and the indicator function[107] of a given ICC was investigated.[108] A statistically significant positive or negative correlation between ICC and transmission severity could be determined by the test.

A red bar in Figure A.14 corresponds to an ICC that has a statistically significant positive correlation with transmission severity, a green bar corresponds to an ICC that has a statistically significant negative correlation, and a blue bar corresponds to an ICC is not statistically significant. A statistically significant positive correlation of initiating cause code with transmission outage severity would indicate a higher likelihood that an event with this ICC will result in a higher transmission outage severity. A statistically significant negative correlation indicates the contrary; in this case, a lower transmission outage severity would be likely. If a correlation is not statistically significant, this implies that a positive or negative correlation was very likely observed by a mere chance, and there is, in fact, no linear relationship between ICC and the transmission outage severity, and the events with this ICC have the expected transmission severity similar to all other events from the database.

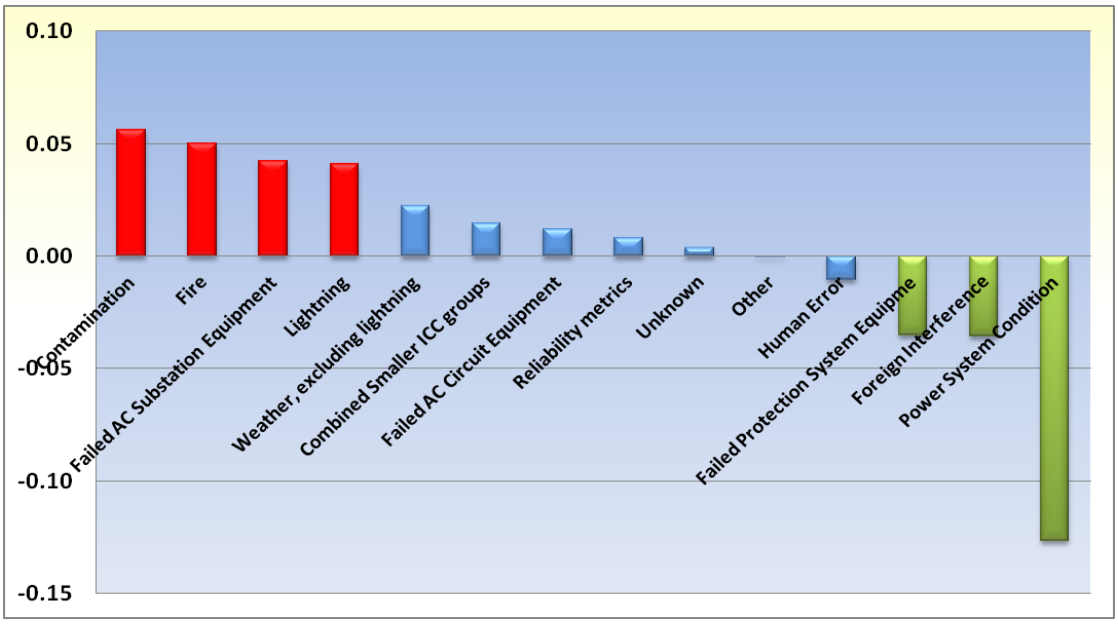


Figure A.14: Correlation between ICC and TS of TADS CDM Events (2009-2013)

Results of the correlation analysis are as follows:

- For the 2009–2013 CDM events, the Contamination ICC has the largest and most statistically significant positive correlation with transmission severity, followed by Fire and Failed AC Substation Equipment. Lightning also has a statistically significant positive correlation.
- Power System Condition, Foreign Interference, and Failed Protection System Equipment have a statistically significant negative correlation with transmission severity. CDM events initiated by either of these causes, on average, tend to have a smaller severity than events from the entire CDM dataset.

[107] The indicator function of a given ICC assigns value 1 to an event with this ICC and value 0 to the rest of the events.

[108] For each ICC, a null statistical hypothesis on zero correlation at significance level 0.05 was tested. If the test resulted in rejection of the hypothesis, it is concluded that a statistically significant positive or negative correlation between an ICC and transmission severity exists; the failure to reject the null hypothesis indicates no significant correlation between ICC and transmission severity.

CDM Events: Distribution of Transmission Severity by ICC

Next, the distribution of transmission severity for CDM events with a given ICC was studied. The transmission severity for CDM events has a sample mean of 0.244 and a sample standard deviation of 0.187. The sample statistics for transmission severity by ICC are listed in Table A.11. The CDM events initiated by Contamination have the largest average transmission severity of 0.317, followed by Fire and Failed AC Substation Equipment (with the expected transmission severity of 0.300, 0.261, respectively). The events initiated by Power System Condition have the smallest average severity of 0.170. Interestingly, the CDM events initiated by Contamination and Fire did not occur often, but upon occurrence resulted in significant transmission severity. Because CDM events typically have more outages per event than Single-Mode events, on average CDM events have higher transmission severity than TADS events.

Table A.11 provides a column that indicates which other ICCs are statistically smaller than a given ICC referenced by the table's column 1 index. For example, transmission severity for Unknown (#8) is statistically significantly smaller than Contamination (#1), while Fire (#2) is not statistically significantly smaller than Contamination.

Transmission Severity Risk and Relative Risk of CDM Events by ICC

If the transmission severity risk of each ICC group is simply the total transmission severity associated with the group, then its relative risk is equal to the percentage of the group transmission severity in the 2009–2013 dataset. Equivalently, the risk of a given ICC per hour can be defined as the product of the probability that an event with this ICC initiated during an hour and the expected severity, or impact, of an event from this group. Then, for any ICC group, the relative risk per hour is the same as the relative risk for five years or any other time period. Table A.11 lists relative risk by ICC with the ICC groups of CDM events in order from the largest relative risk to the smallest.

Table A.11: Evaluation of CDM Event ICC Contribution to Transmission Severity (2009–2013)

Group of TADS events	Probability that an Event from a Group Starts during a Given Hour	Expected Impact (Expected Transmission Severity of an Event)	Risk Associated with a Group Per Hour	Relative Risk by Group (%)
CDM Lightning	0.013	0.258	0.003	4.6
CDM Failed AC Substation Equipment	0.010	0.261	0.003	3.7
CDM Weather Excluding Lightning	0.008	0.253	0.002	2.7
CDM Human Error	0.007	0.236	0.002	2.5
CDM Unknown	0.007	0.244	0.002	2.4
CDM Failed Protection System Equipment	0.007	0.221	0.001	2.1
CDM Power System Condition	0.007	0.170	0.001	1.7
CDM Failed AC Circuit Equipment	0.004	0.250	0.001	1.5
CDM Other	0.002	0.241	0.001	0.8
CDM Fire	0.002	0.300	0.001	0.7
CDM Foreign Interference	0.002	0.204	0.000	0.6
CDM Contamination	0.001	0.317	0.000	0.6
CDM Combined Smaller ICC groups	0.001	0.257	0.000	0.3
All TADS events	**0.430**	**0.165**	**0.071**	**100.0**
All CDM events	**0.074**	**0.244**	**0.018**	**25.4**
All with ICC assigned	**0.072**	**0.241**	**0.017**	**24.4**

Appendix B – Statistical Analysis for ALR1-12 Metric

Interconnection Frequency Response: Time Trends

Eastern Interconnection

The time trend analysis uses the Eastern Interconnection frequency response (FR) datasets for 2009–2013. In this section, relationships between frequency response and the explanatory variable T (time: year, month, day, hour, minute, second) are studied.

Even though a linear trend line for the scatter plot connecting T and FR shown in Figure 1.5 has a negative slope at -0.07139, the linear regression is not statistically significant[109] and, on average, the Eastern Interconnection frequency response[110] has been stable from 2009 through 2013.

ERCOT Interconnection

The time trend analysis uses the ERCOT frequency response datasets for 2009–2013. In this section, the relationship is investigated between frequency response and the explanatory variable T, when a frequency response event happened.

There is a positive correlation of 0.23 between T and FR; further, the statistical test on the significance of the correlation (and the equivalent test of the significance of a linear regression) results in a rejection of the null hypothesis about zero correlation (p-value of both tests below 0.0001). This proves that it was very unlikely that the observed positive correlation occurred simply by chance. Moreover, a linear trend line for the scatter plot connecting T and FR shown in Figure 1.5 has a statistically significant positive slope (0.0000013), the linear regression is statistically significant, and on average, the ERCOT Interconnection frequency response increased from 2009 through 2013 at the average rate of 3.3 MW/.1 Hz.

Québec Interconnection

The time trend analysis uses the Québec Interconnection frequency response datasets for 2011–2013. The frequency response values represent the observed values of the analysis (response) variable FR of the Québec Interconnection frequency response. In this section, the relationship is investigated between frequency response and the explanatory variable T, when a frequency response event happened.

There is a positive correlation of 0.13 between T and FR; however, the statistical test on the significance of the correlation (and the equivalent test of the significance of a linear regression) fails to reject the null hypothesis about zero correlation at a standard significance level (p-value of the both tests is 0.23). This result leads to the conclusion that with high probability the positive correlation could occur simply by chance. It implies that even though a linear trend line for the scatter plot connecting T and FR shown in Figure 1.5 has a positive slope (0.00000104), the linear regression is not statistically significant, and on average, the Québec Interconnection frequency response has been stable from 2011 through 2013.

Western Interconnection

The time trend analysis uses the Western Interconnection frequency response datasets from 2009 through 2013. The frequency response values represent the observed values of the analysis (response) variable FR, the Western Interconnection frequency response. In this section, the relationship is investigated between FR and the explanatory variable T, when a frequency response event happened.

---

[109] The linear regression in http://www.nerc.com/docs/standards/dt/Field_Trial_Analysis-final_20120910.pdf recommended by Howard Ilian is completely different from the linear regression in Appendix B which is used for time trend analysis.

[110] There is a positive correlation of 0.0017 between T and FR; however, the statistical test on significance of the correlation (and the equivalent test of the significance of a linear regression) fails to reject the null hypothesis about zero correlation at a standard significance level (p-value of the both tests is 0.98). This implies the increase in the expected frequency response since 2009 could just be chance.

There is a negative correlation of -0.05 between T and FR; however, the statistical test on the significance of the correlation (and the equivalent test of the significance of a linear regression) fails to reject the null hypothesis about zero correlation at a standard significance level (p value of the both tests is 0.60). This result leads to the conclusion that the negative correlation could have occurred simply by chance. It implies that even though a linear trend line for the scatter plot connecting T and FR shown in Figure 1.5 has a negative slope (-0.000000435), the linear regression is not statistically significant, and on average, the Western Interconnection frequency response has been stable from 2009 through 2013.

For the Western Interconnection, the data for the years 2009 through 2010 are not very reliable. The value of B was calculated within the first 10 seconds in 2009 and 2010. The other reason the frequency response is much higher for these years is because the capacity of the unit—rather than the net MW loss to the interconnection—was reported. In recent years, such as from 2011 through 2013, better tools have been put in place to detect frequency events and their underlying causes. There are also more systematic procedures to document and verify these events.

Interconnection Frequency Response: Year-to-Year Changes

Eastern Interconnection

The time trend analysis uses the Eastern Interconnection frequency response datasets from 2009 through 2013. The sample statistics by year are listed in Table B.1. The last column lists the number of frequency response events that fell below the absolute IFRO.[111]

Table B.1: Sample Statistics for Eastern Interconnection

Year	Number of Values	Mean of Frequency Response	Std. Dev. of Frequency Response	Minimum	Maximum	Number of Events with FR below the IFRO=1014
2009-2013	**257**	**2308.3**	**603.0**	**698.7**	**4335.9**	**3**
2009	44	2258.4	522.5	1404.8	3625.0	0
2010	49	2335.7	697.6	1102.5	4335.9	0
2011	65	2467.8	593.7	1210.0	3815.2	0
2012	28	2314.3	523.6	1374.0	3921.4	0
2013	71	2171.9	596.5	698.7	3696.3	3

Next, Fisher's Least Significant Difference test is used to analyze all pair-wise changes in frequency response. These tests result in the conclusion that there was a statistically significant decrease of frequency response in 2013 compared with 2011, and there were no other statistically significant changes in the expected frequency response by year for the Eastern Interconnection.

[111] http://www.nerc.com/FilingsOrders/us/NERC Filings to FER DL/FR Annual Report 12-27-13 Final.pdf

ERCOT Interconnection

The time trend analysis uses the ERCOT Interconnection frequency response datasets from 2009 through 2013. The sample statistics by year are listed in Table B.2. The last column lists the number of frequency response events that fell below the absolute IFRO.

Table B.2: Sample Statistics for ERCOT Interconnection

Year	Number of Values	Mean of Frequency Response	Std. Dev. of Frequency Response	Minimum	Maximum	Number of events with FR below the IFRO=413
2009-2013	**298**	**612.2**	**240.8**	**228.0**	**2552.8**	**34**
2009	51	595.2	185.0	263.5	1299.1	5
2010	67	609.7	164.8	367.6	1152.5	3
2011	65	509.6	131.3	228.0	993.0	15
2012	63	571.2	191.9	290.4	1417.9	9
2013	52	809.8	383.2	378.7	2552.8	2

Next, Fisher's Least Significant Difference test is applied to analyze all pair-wise changes in frequency response. These tests find four statistically significant improvements in the expected frequency response (between 2009 and 2013, between 2010 and 2013, between 2011 and 2013, and between 2012 and 2013).

Several factors contributed to the frequency response performance in the ERCOT Interconnection during the years in which the frequency response did not meet the recommended IFRO (2011 and 2012).

- ERCOT has a small hydro fleet that suffered significantly due to the extreme drought of 2011. There was some relief in 2012, but not in the geographical area of these hydro facilities. Additionally, the owners of the facilities have changed the facilities' operation. Prior to the ERCOT nodal market implementation in December 2010, many of these facilities were operated as frequency responsive reserves. They were on-line in synchronous condenser mode and ramped to full output in about 20 seconds anytime frequency dropped to 59.900 Hz or below, providing 50 to 240 MW of primary frequency response (during the first 20 seconds of a disturbance). Since early 2011, this service has been discontinued.
- There was a drop in natural gas prices and a change in dispatch. The price change caused many of the large coal generators to shut down, and frequency response from these generators had been excellent. The combined-cycle facilities that replaced these units had difficulty getting frequency response to work consistently and correctly. Since the fall of 2012, frequency response from combined-cycle facilities has improved, due to TRE's efforts to work with these generators to improve their performance.
- Another contributing factor was the continued increase in wind generation in ERCOT that typically operates at maximum output. Without margin in the up direction, the interconnection only benefits by curtailing wind generators during high-frequency excursions from these generators. When low-frequency excursions occur, the wind generators cannot provide additional output to increase interconnection frequency.

Québec Interconnection

The time trend analysis uses the Québec Interconnection frequency response datasets for the years 2011 through 2013. The sample statistics by year are listed in Table B.3. The last column lists the number of frequency response events that fell below the absolute IFRO.**Error! Bookmark not defined.**

Table B.3: Sample Statistics for Québec Interconnection

Year	Number of Values	Mean of Frequency Response	Std. Dev. of Frequency Response	Minimum	Maximum	Number of Events with FR below the IFRO=180
2011–2013	**85**	**575.3**	**202.9**	**214.7**	**1228.0**	**0**
2011	20	499.1	153.6	214.7	829.9	0
2012	28	592.7	212.4	305.9	1202.1	0
2013	37	603.3	213.3	250.9	1227.8	0

Next, Fisher's Least Significant Difference test is applied to analyze all pair-wise changes in frequency response. These tests result in the conclusion that there are no statistically significant changes in the expected frequency response by year for Québec Interconnection.

Western Interconnection

The time trend analysis uses the Western Interconnection frequency response datasets for 2009–2013. The sample statistics are listed by year in Table B.4. The last column lists the number of frequency response events that fell below the absolute IFRO.**Error! Bookmark not defined.**

Table B.4: Sample Statistics for Western Interconnection

Year	Number of Values	Mean of Frequency Response	Std. Dev. of Frequency Response	Minimum	Maximum	Number of Events with FR below the IFRO=949
2009–2013	**119**	**1514.0**	**422.9**	**816.7**	**3125.0**	**3**
2009	25	1513.6	295.7	1000.0	2027.0	0
2010	29	1572.2	512.3	816.7	3125.0	2
2011	25	1496.5	391.9	1078.6	2894.6	0
2012	12	1466.8	557.2	997.0	3123.5	0
2013	28	1491.2	404.3	821.9	2851.0	1

It is impossible to statistically analyze pair-wise annual changes in the Western Interconnection frequency response due to small sample sizes for each year.

Explanatory Variables for Frequency Response and Multiple Regression

Explanatory Variables

In the *2012 State of Reliability* report, Key Finding #2 proposed further work to see if specific indicators could be tied to severity of frequency deviation events. For each interconnection, the following set of six variables is included as explanatory variables (regressors) in the multiple regression models that describe the interconnection frequency response. These variables are not pair-wise uncorrelated, and some pairs are strongly correlated; however, all are included as candidates to avoid the loss of an important contributor to the frequency response variability. Model selection methods help ensure the removal of highly correlated regressors and run multicollinearity diagnostics (variance inflation diagnostic) for a multiple regression model selected.

Summer (Indicator Function) – Defined as 1 for frequency response events that occur from June through August and 0 otherwise.

Winter (Indicator Function) – Defined as 1 for frequency response events that occur from December through February and 0 otherwise.
High Pre-Disturbance Frequency (Indicator Function) – Defined as 1 for frequency response events with pre-disturbance frequency (point A)>60 Hz and 0 otherwise.
On-peak Hours (Indicator Function) – Defined as 1 for frequency response events that occurred during on-peak hours and 0 otherwise. On-peak hours are designated as follows: Monday to Saturday from 0700 to 2200 (Central Time) excluding six holidays: New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, and Christmas Day.
Time – A moment in time (year, month, day, hour, minute, second) when a frequency response event happened. Time is measured in seconds elapsed between midnight of January 1, 1960 (the time origin for the date format in SAS), and the time of a corresponding frequency response event. This is used to determine trends over the study period.
Interconnection Load Level – Measured in megawatts. For the Eastern Interconnection, the data are unavailable for the 2013 events; thus, the multivariate statistical analysis for them involves 2009–2012 data only (186 observations for the Eastern Interconnection). For the ERCOT and Western Interconnections, the analysis covers the five-year data, and for the Québec Interconnection, the 2011–2013 data.

Table B.5 lists the ranks of statistically significant variables of interconnection frequency response for each interconnection. "Positive" indicates positive correlation, "negative" indicates negative correlation, and a dash indicates no statistically significant linear relation. If the initial pre-disturbance frequency is higher than 60 Hz, it is more likely that governor actions will be delayed because of the time it takes for the frequency to drop to the upper dead-band setting.

Table B.5: Observation Summary

Explanatory Valuable	Western	Eastern	ERCOT	Québec
Summer	-	-	-	-
Winter	-	-	-	2 (positive)
High Pre-disturbance	1 (negative)	2 (negative)	1 (negative)	-
On-peak hours	-	-	-	3 (positive)
Time	-	-	2 (positive)	-
Load Level	-	1 (positive)	-	1 (positive)

Eastern Interconnection: Correlation Analysis and Multivariate Model

Descriptive statistics for the six explanatory variables and the Eastern Interconnection frequency response are listed in Table B.6.

Table B.6: Descriptive Statistics

Variable	N	Mean	Std Dev	Minimum	Maximum
Time	186	-	-	1/1/2009	12/31/2012
Interconnection Load	186	343,170	63,792	217,666	541,565
On-Peak Hours	186	0.640	0.481	0	1
A>60	186	0.505	0.501	0	1
Winter	186	0.161	0.369	0	1
Summer	186	0	0	0	1
FR	186	2360	599	1103	4336

The correlation and a single regression analysis result in the hierarchy of the explanatory variables for the Eastern Interconnection frequency response shown in Table B.7. The value of a coefficient of determination R^2 indicates

the percentage in variability of frequency response that can be explained by variability of the corresponding explanatory variable. Out of the six parameters, interconnection load has the biggest impact on frequency response, followed by the indicator of high pre-disturbance frequency. Interconnection load is positively correlated with frequency response (they increase or decrease together, on average), while high pre-disturbance frequency is negatively correlated with frequency response. The events with A>60 Hz have smaller frequency response than the events with A≤60 Hz. The other four variables do not have a statistically significant[112] linear relationship with frequency response.

Table B.7: Correlation and Regression Analysis

Explanatory Variable	Correlation with FR	Statistically Significant (Yes/No)	Coefficient of Determination of Single Regression (If SS)
Interconnection Load	0.38	Yes	14.4%
A>60	-0.24	Yes	6.0%
On-Peak hours	0.11	No	N/A
Time	0.10	No	N/A
Winter	-0.09	No	N/A
Summer	0.06	No	N/A

Both step-wise selection and backward elimination algorithms[113] result in a multiple regression model that connects the Eastern Interconnection frequency response with the following significant[114] regressors: interconnection load and high pre-disturbance frequency (the other four variables are not selected or were eliminated). The models' coefficients are listed in Table B.8.

Table B.8: Coefficients of Multiple Model

Variable	DF	Parameter Estimate	Standard Error	t-value	p-value	Variance Inflation Value
Intercept	1	1272.19	218.21	5.83	<.0001	0
Interconnection Load	1	0.0036	0.00	5.86	<.0001	1.00067
A>60	1	-304.10	78.60	-3.87	0.0002	1.00067

The adjusted coefficient of multiple determination of the model is 20.0 percent; the model is statistically significant ($p<0.0001$). The random error has a zero mean and the sample deviation σ of 536 MW/.1 Hz. Variance inflation factors for the regressors do not exceed 1.0007, which confirms an acceptable level of multicollinearity that does not affect a general applicability of the model. Frequency responses in the Eastern Interconnection are higher due to the large number of disturbances in the dataset in which frequency changes were greater than the generator dead-bands. Also, in earlier studies, the gross output of the unit trip was reported, rather than the net generation[115] megawatt loss to the interconnection.

[112] At significance level 0.1

[113] For step-wise regression algorithm and Backward Elimination algorithm see D. C. Montgomery and G. C. Runger. Applied Statistics and Probability for Engineers. Fifth Edition. 2011. John Wiley & Sons. Pp. 499-501.

[114] Regressors in the final model have p-values not exceeding 0.1.

[115] There could be a coincident loss of load also.

ERCOT: Correlation Analysis and Multivariate Model

Descriptive statistics for the six explanatory variables and the ERCOT Interconnection frequency response are listed in Table B.9.

Table B.9: Descriptive Statistics

Variable	N	Mean	Std Dev	Minimum	Maximum
Winter	298	0.305	0.461	0	1
Summer	298	0.252	0.435	0	1
Date	298	-	-	1/1/2009	12/31/2013
A>60	298	0.440	0.497	0	1
On-Peak Hours	298	0.609	0.489	0	1
Interconnection Load	298	38,791	9,745	22,243	64,744
FR	298	612.16	240.75	228.04	2552.75

The correlation and a single regression analysis result in the hierarchy of the explanatory variables for the ERCOT Interconnection frequency response shown in Table B.10.

Table B.10: Correlation and Regression Analysis

Explanatory Variable	Correlation with FR	Statistically Significant (Yes/No)	Coefficient of Determination of Single Regression (If SS)
A>60	-0.31	Yes	9.4%
Time	0.23	Yes	5.3%
Winter	0.07	No	N/A
On-Peak Hours	0.07	No	N/A
Summer	0.04	No	N/A
Interconnection Load	0.02	No	N/A

Out of the six parameters, the indicator of high pre-disturbance frequency has the biggest impact on frequency response, followed by time. High pre-disturbance frequency is negatively correlated with frequency response (the events with A>60 Hz have smaller frequency response than the events with A≤60 Hz, and time is positively correlated with frequency response (on average, frequency response increases with time). The other four variables do not have a statistically significant[116] linear relationship with frequency response.

Finally, both step-wise selection algorithm and backward elimination algorithm result in a multiple regression model that connects the ERCOT Interconnection frequency response with high pre-disturbance frequency and time (the other four variables are not selected or were eliminated[117]) as regressors. The coefficients of the multiple models are listed in Table B.11.

Table B.11: Coefficients of Multiple Model

Variable	DF	Parameter Estimate	Standard Error	t-value	p-value	Variance Inflation Value
Intercept	1	-1377.45	484.53	-2.84	0.0048	0
Time	1	0.00000126	0.00000030	4.24	<.0001	1.00002
A>60	1	-147.89	26.15	-5.66	<.0001	1.00002

The adjusted coefficient of multiple determination of the model is 14.0 percent; the model is statistically significant ($p<0.0001$). The random error has a zero mean and the sample deviation σ of 224 MW/.1 Hz. Variance

[116] At significance level 0.1

[117] Regressors in the final model have p-values not exceeding 0.1.

inflation factors for the regressors do not exceed 1.00002, which confirms an acceptable level of multicollinearity that does not affect a general applicability of the model.

Québec: Correlation Analysis and Multivariate Model

Descriptive statistics for the six explanatory variables and the Québec Interconnection frequency response are in Table B.12.

Table B.12: Descriptive Statistics

Variable	N	Mean	Std Dev	Minimum	Maximum
Winter	85	0.188	0.393	0	1
Summer	85	0.541	0.501	0	1
A>60	85	0.471	0.502	0	1
Time	85	-	-	1/1/2011	12/31/2013
On-Peak Hours	85	0.647	0.481	0	1
Interconnection Load	85	21,635	4,593	14,330	35,140
FR	85	575.30	202.88	214.74	1228

The correlation and a single regression analysis result in the hierarchy of the explanatory variables for the Québec Interconnection frequency response shown in Table B.13.

Table B.13: Correlation and Regression Analysis

Explanatory Variable	Correlation with FR	Statistically Significant (Yes/No)	Coefficient of Determination of Single Regression (If SS)
Interconnection Load	0.28	Yes	7.6%
Winter	0.26	Yes	6.7%
On peak Hours	0.18	Yes	3.3%
Time	0.13	No	N/A
Summer	-0.10	No	N/A
A>60	-0.08	No	N/A

Out of the six parameters, interconnection load has the biggest impact on frequency response, followed by the indicators of winter and on-peak hours. Interconnection load, winter, and on-peak hours are positively and statistically significantly[118] correlated with frequency response (the winter events have higher frequency response than other events; the on-peak hour events have higher frequency response than the off-peak hour events; and, finally, the events with higher interconnection load have larger frequency response). The other three variables do not have a statistically significant linear relationship with frequency response.

Finally, both step-wise selection algorithm and backward elimination algorithm result in a single regression model that connects the Québec Interconnection frequency response with interconnection load (the other five variables are not selected or were eliminated[119]). The coefficients of the single model are in Table B.14.

Table B.14: Coefficients of Single Model

Variable	DF	Parameter Estimate	Standard Error	t-value	p-value	Variance Inflation Value
Intercept	1	312.1	103.06	3.03	0.0033	0.00
Interconnection Load	1	0.0122	0.00466	2.61	0.0107	1.00

[118] At significance level 0.1

[119] Regressors in the final model have p-values not exceeding 0.1.

The model's adjusted coefficient of determination is 6.5 percent; the model is statistically significant (p=0.01). The random error has a zero mean and the sample deviation σ of 196 MW/.1 Hz. Since the multiple models for the Québec Interconnection frequency response are reduced to a single model, no multicollinearity diagnostics are needed.

The main reason that winter events have a better frequency response is because winter is the peak usage season in the Québec Interconnection. More generator units are on-line; therefore, there is more inertia in the system, so it is more robust in responding to frequency changes in the winter.

Western Interconnection: Correlation Analysis and Multivariate Model

Descriptive statistics for the six explanatory variables and the Western Interconnection frequency response are listed in Table B.15.

Table B.15: Descriptive Statistics

Variable	N	Mean	Std Dev	Minimum	Maximum
Winter	119	0.218	0.415	0	1
Summer	119	0.378	0.487	0	1
Time	119	-	-	1/1/2009	12/31/2013
A>60	119	0.395	0.491	0	1
Interconnection Load	119	92553	17424	60188	143637
On-Peak Hours	119	0.597	0.493	0	1
FR	119	1514	422.9	816.7	3125.0

The correlation and a single regression analysis result in the hierarchy of the explanatory variables for the Western Interconnection frequency response shown in Table B.16.

Table B.16: Correlation and Regression Analysis

Explanatory Variable	Correlation with FR	Statistically Significant (Yes/No)	Coefficient of Determination of Single Regression (If SS)
A>60	-0.312	Yes	9.7%
Winter	-0.099	No	N/A
Interconnection Load	0.089	No	N/A
Summer	0.084	No	N/A
Time	-0.048	No	N/A
On-Peak Hours	0.024	No	N/A

Out of the six parameters, the indicator of high pre-disturbance frequency has the biggest impact on frequency response. The indicator is negatively and statistically significantly correlated with frequency response (the events with pre-disturbance frequency greater than 60 Hz have smaller frequency response on average). The other five variables are not statistically significantly[120] correlated with frequency response.

[120] At significance level 0.1

Finally, both step-wise selection algorithm and backward elimination algorithm result in a single regression model that connects the Western Interconnection frequency response with one regressor, the indicator of high pre-disturbance frequency (the other five variables are not selected or were eliminated[121]). The coefficients of the single model are listed in Table B.17.

Table B.17: Coefficients of Single Model

Variable	DF	Parameter Estimate	Standard Error	t-value	p-value	Variance Inflation Value
Intercept	1	1620.4	47.56	34.07	<.0001	0.00
A>60	1	-268.7	75.68	-3.55	0.0006	1.00

[121] Regressors in the final model have p-values not exceeding 0.1.

Appendix C – Statistical Summary of SRI$_{bps}$ Assessment

The PAS has investigated the SRI$_{bps}$ performance for 2008–2013 as well as a year-by-year comparison. From this analysis it concluded that 2011 performance was the best SRI$_{bps}$ on record, as measured by its mean and standard deviation, in spite of the relatively large standard deviation (whose outliers included the September 8, 2011 load shed event, in addition to the February 2, 2011 cold weather load loss event). It also determined that 2009 and 2013 were the next best performance years, followed by 2010, 2012, and 2008. These values are shown in Table C.1 below.

Table C.1: Descriptive Statistics of Annual SRI $_{bps}$

Year	N	SRI $_{bps}$	
		Mean	Std Dev
2008	366	1.801	0.674
2009	365	1.664	0.528
2010	365	1.742	0.611
2011	365	1.504	1.041
2012	366	1.785	0.813
2013	365	1.670	0.600

This ranking is further visible in Figure C.1 below. It can be observed that if outlier performance were taken as a larger input to ranking the year's results, 2011 and 2012 would be considered poorer performance years, while 2013 and 2009 would be rated as the best performance years.

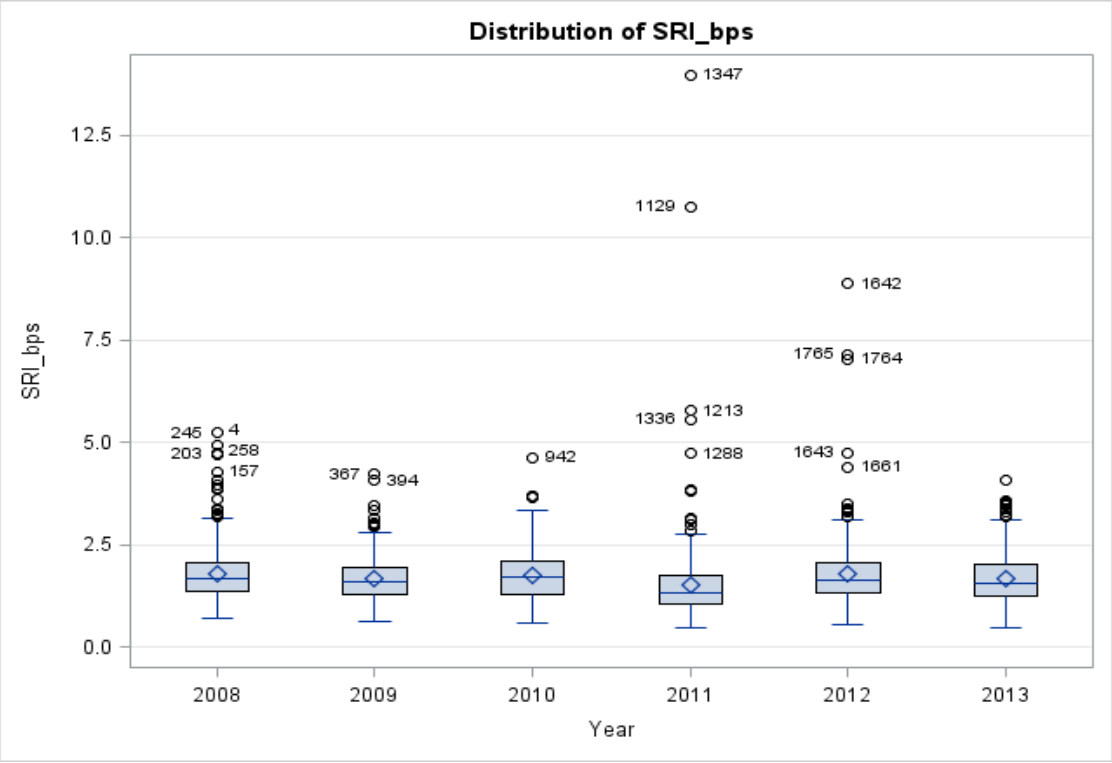


Figure C.1: Boxplot of Annual SRI$_{bps}$

Finally, the performance of each year compared to every other year is depicted in Table C.2 below; if no reference to statistical significance is made within the table, it is assumed to be statistically significant.[122]

Table C.2: Pair-wise Comparison of Annual SRI_{bps}

	Compared to Year					
Base Year	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**
2008		2009 Better	2010 Better, but not Statistically Significant	2011 Better	2012 Better, but not Statistically Significant	2013 Better
2009			2009 Better, but not Statistically Significant	2011 Better	2009 Better	Approximately Equal
2010				2011 Better	2012 Better, but not Statistically Significant	2013 Better, but not Statistically Significant
2011					2011 Better	2011 Better
2012						2013 Better
2013						

The second analysis performed was an assessment of the distribution. Performance is most closely represented as a log-normal distribution; however, 2011 and 2012 do not fit that distribution.

Table C.3: SRI_{bps} Parameters for Fitted Log-normal Distribution

Parameter	Symbol	2008 Estimate	2009 Estimate	2010 Estimate	2011 Estimate	2012 Estimate	2013 Estimate	2008–2013 Estimate
Minimum p-value*	P	**0.205**	**>0.50**	**0.082**	**0.009**	**0.007**	**>0.250**	**0.001**
Fit to Log-normal		Good	Very good	Poor	Not fitted	Not fitted	Good	Not fitted
Threshold	Theta	0.389	0.059	-0.196			-0.491	
Scale	Zeta	0.247	0.422	0.613			0.734	
Shape	Sigma	0.440	0.319	0.312			0.273	
Mean		**1.799**	**1.664**	**1.743**			**1.670**	
Std Dev		**0.651**	**0.525**	**0.620**			**0.601**	

[122] At significance level 0.05.

In Figure C.2 below is the histogram for 2013 SRI_{bps}, which did conform to a log-normal distribution.

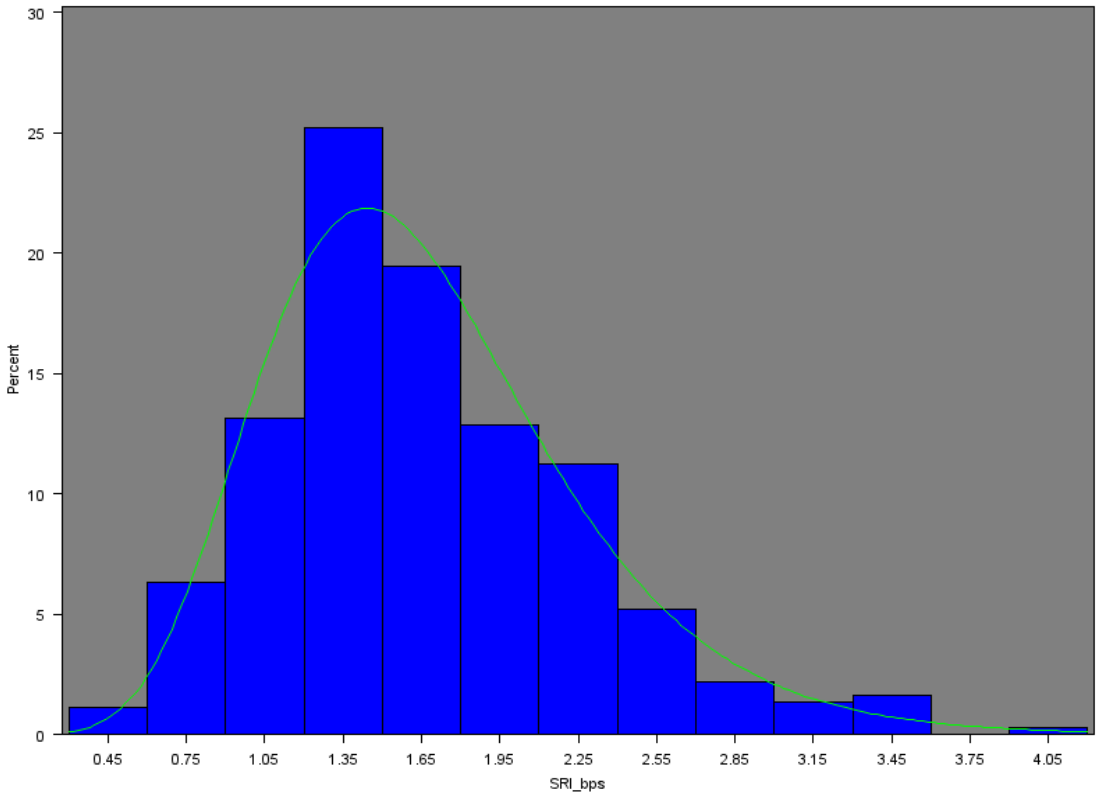


Figure C.2: Histogram for SRI_{bps} for 2013

In Figure C.3 below, the trend of performance is shown over the six-year history. It is notable that the trend of performance over this period is improving, which is very close to statistically significant;[123] statistical significance means that the changes observed are real changes and are not due to random variations in the data.

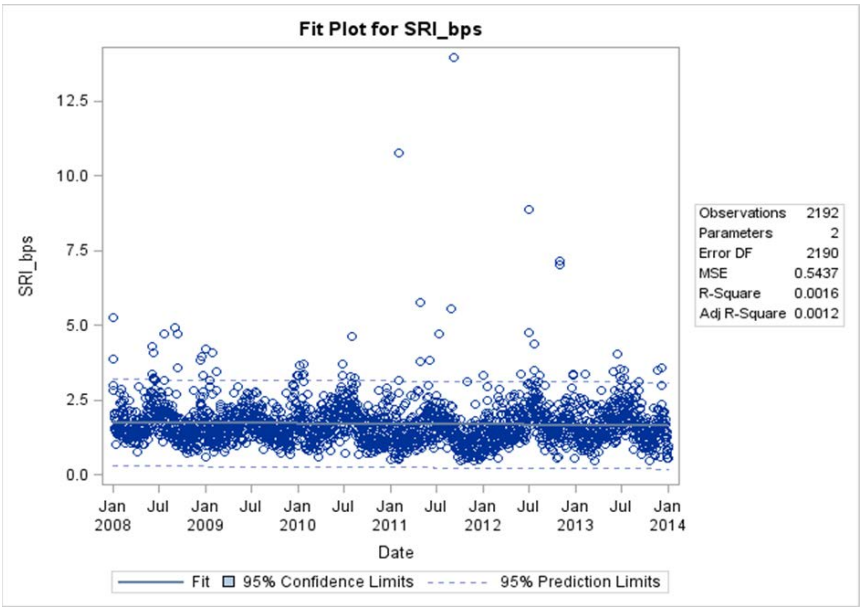


Figure C.3: Fit Plot for SRI_{bps} 2008–2013

[123] Significance of the linear regression describing the time trend is P=0.06.

Appendix D – Abbreviations Used in This Report

Acronym	Description
ALR	Adequate Level of Reliability
BES	Bulk Electric System
BPS	Bulk Power System
CDM	Common/Dependent Mode
EEA	Energy Emergency Alert
ERO	Electric Reliability Organization
ERCOT	Electric Reliability Council of Texas
FERC	Federal Energy Regulatory Commission
FRCC	Florida Reliability Coordinating Council
ICC	Initiating Cause Code
IROL	Interconnection Reliability Operating Limit
ISO	Independent System Operator
ISO-NE	ISO New England
KCMI	Key Compliance Monitoring Index
MRO	Midwest Reliability Organization
NERC	North American Electric Reliability Corporation
NPCC	Northeast Power Coordinating Council
NYISO	New York Independent Service Operator
PAS	Performance Analysis Subcommittee
PSMTF	Protection System Misoperation Task Force
RC	Reliability Coordinator
RE	Regional Entities
RF	ReliabilityFirst
RSG	Reserve-Sharing Group
SERC	SERC Reliability Corporation
SNL	Sandia National Laboratories
SOL	System Operating Limit
SPS	Special Protection Schemes
SPCS	System Protection and Control Subcommittee
SPP	Southwest Power Pool
SRI	Severity Risk Index
TADS	Transmission Availability Data System
TADSWG	Transmission Availability Data System Working Group
TO	Transmission Owner
TRE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Contributions

Acknowledgements

NERC would like to express its appreciation to the many people who provided technical support and identified areas for improvement.

NERC Industry Groups

Table 1 lists the NERC industry group contributors.

Table 1: NERC Group Acknowledgements

Group	Officers
Planning Committee Reviewers	John Feit, Public Service Commission of Wisconsin David Jacobsen, Manitoba Hydro Dale Burmester, American Transmission Company, LLC
Performance Analysis Subcommittee	Chair: Melinda Montgomery, Entergy Vice Chair: Heide Caswell, PacifiCorp
Demand Response Availability Data System Working Group	Chair: Bob Collins, TRE Vice Chair: Mike Jaeger, ISO-NE
Events Analysis Subcommittee	Chair: Sam Holeman, Duke Energy Vice Chair: Hassan Hamdar, FRCC
Generation Availability Data System Working Group	Chair: Gary Brinkworth, TVA Vice Chair: Leeth DePriest, Southern Company
Transmission Availability Data System Working Group	Chair: Jake Langthorn, Oklahoma Gas and Electric Co. Vice Chair: Jeff Schaller, Hydro One Networks, Inc.
Resources Subcommittee	Chair: Don Badley, Northwest Power Pool Corp. Vice Chair: Gerald Beckerle, Ameren Services
Operating Reliability Subcommittee	Chair: Joel Wise, TVA Vice Chair: Eric Senkowicz, FRCC
Frequency Working Group	Chair: Sydney Niemeyer, NRG Energy
Operating Committee	Chair: Tom Bowe, PJM Interconnection, LLC Vice Chair: James D. Castle, Duke Energy
Planning Committee	Chair: Ben Crisp, SERC Reliability Corporation Vice Chair: Ben Crisp, SERC Reliability Corporation
Reliability Assessment Subcommittee	Chair: Vince Ordax, FRCC Vice Chair: Layne Brown, WECC
System Protection and Control Subcommittee	Chair: William J. Miller, Exelon Corporation Vice Chair: Philip B. Winston, Southern Company
Protection System Misoperations Task Force	Chair: John Seidel, Midwest Reliability Organization
Spare Equipment Database Working Group	Chair: Dale Burmester, American Transmission Company, LLC Vice Chair: Puesh Kumar, APPA
Compliance and Certification Committee	Chair: Terry Bilke, Midwest ISO, Inc. Vice Chair: Patricia E. Metro, National Rural Electric Cooperative Association

Regional Entity Staff

Table 2 provides a list of the Regional Entity staff that provided data and content review.

Table 2: Contributing Regional Entity Staff

Name	Regional Entity
Vince Ordax	FRCC
John Seidel	MRO
Phil Fedora	NPCC
Paul Kure	RF
John Johnson	SERC
Alan Wahlstrom and Deborah Currie	SPP
Bob Collins	TRE
Matthew Elkins	WECC

NERC Staff

Table 3 provides a list of the NERC staff who contributed to this report.

Table 3: NERC Staff

Name	Title	E-mail Address
Thomas Burgess	Vice President and Director, Reliability Assessment and Performance Analysis	thomas.burgess@nerc.net
Howard Gugel	Director of Reliability Risk Analysis	howard.gugel@nerc.net
Naved Khan	Engineer, Reliability Performance Analysis	naved.khan@nerc.net
Svetlana Ekisheva	Senior Statistician, Reliability Assessment and Performance Analysis	svetlana.ekisheva@nerc.net
Matthew Varghese	Senior Performance Analysis Engineer	matthew.varghese@nerc.net
Elsa Prince	Engineer, Reliability Performance Analysis	elsa.prince@nerc.net
Andrew Slone	Engineer, Reliability Performance Analysis	andrew.slone@nerc.net
Lee Thaubald	Data Analyst Performance Analysis	lee.thaubald@nerc.net
Michelle Marx	Administrative Assistant	michelle.marx@nerc.net
Ben McMillan	Risk Analysis Engineer	ben.mcmillan@nerc.net
James Merlo	Associate Director of Human Performance	james.merlo@nerc.net
Robert W. Cummings	Director of Reliability Initiatives and System Analysis	bob.cummings@nerc.net
Rich Bauer	Senior Reliability Specialist	rich.bauer@nerc.net
Margaret Pate	Reliability Risk Control Program Liaison	margaret.pate@nerc.net

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
Valerie.Agnew@nerc.net

For questions about this form or for assistance in completing the form, call Valerie Agnew at 404-446-2566.

NERC welcomes suggestions for improving the reliability of the Bulk-Power System through improved Reliability Standards. Please use this form to submit your proposal for a new NERC Reliability Standard or a revision to an existing standard.

Request to propose a new or a revision to a Reliability Standard			
Proposed Project Number and Name	Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems)		
Proposed Project Purpose:	Revise NERC Glossary of Terms definition: Special Protection System (SPS) Revise SPS-related Reliability Standards		
Date Submitted:	02/12/2014		
SAR Requester Information			
Name:	Al McMeekin		
Organization:	NERC		
Telephone:	404-446-9675	E-mail:	Al.McMeekin@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard ☒ Revision to existing Standard		☒ Withdrawal of existing Standard ☐ Urgent Action	

SAR Information
Industry Need (What is the industry problem this request is trying to solve?):
The existing NERC Glossary of Terms definition for a Special Protection System (SPS) or, as used in the Western Interconnection, a Remedial Action Scheme (RAS), lacks the clarity and specificity necessary for consistent identification and classification of protection schemes as SPS or RAS across the eight NERC Regions, leading to inconsistent application of the related NERC Reliability Standards. In FERC Order No. 693 (dated March 16, 2007), the Commission identified three of the SPS-related ~~standards~~Reliability Standards (PRC-012-0, PRC-013-0, and PRC-014-0) as fill-in-the-blank standards because they are applicable to the Regional Reliability Organizations (RROs). Consequently, the Commission did not approve or remand them, rendering them neither mandatory nor enforceable. This project also addresses, in part, four recommendations related to identification and coordination of SPS from the joint FERC-NERC inquiry of the September 2011 Southwest Blackout Event. NOTE: Detailed information is included in the NERC Planning Committee report "Special Protection Systems (SPS) and Remedial Action Schemes (RAS): Assessment of Definition, Regional Practices, and Application of Related Standards" Revision 0.1 – April 2013.
Purpose or Goal (How does this request propose to address the problem described above?):
1) Establish a definition of an SPS or RAS that provides the specificity needed to consistently identify and classify protection schemes as SPS or RAS across all eight NERC Regions, thereby promoting the consistent application of the NERC Reliability Standards related to SPS. 2) Correct the applicability of the NERC Reliability Standards related to SPS/RAS by assigning responsibilities to the specific users, owners, and operators of the Bulk-Power System rather than the RROs. 3) Develop continent-wide standards to address all aspects of SPS/RAS, including but not limited to, the: • planning, coordination, and design of SPS/RAS, • review, assessment, and documentation of SPS/RAS, • operational considerations for monitoring, status notification, and response to failures, • analysis of SPS/RAS operations, and defining and reporting of SPS/RAS misoperations, • testing of SPS/RAS, and maintenance of any non-protection system components used ~~in SPS~~.

SAR Information
Identify the Objectives of the proposed standard's requirements (What specific reliability deliverables are required to achieve the goal?):
Successful implementation of a modified ~~SPS~~ definition ~~and~~for an SPS/RAS, with the revised SPS ~~standards~~/RAS-related Reliability Standards will improve Bulk-Power System reliability by providing continent-wide consistency in the identification and classification of SPS or RAS, and by promoting the consistent application of ~~NERC~~the related Reliability Standards ~~related to SPS~~.
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The project will develop a revised definition of SPS or RAS, as well as ~~standards~~revise the NERC Reliability Standards that address the: • review of new or modified SPS/RAS, • annual assessments of SPS/RAS in transmission planning studies, • periodic comprehensive SPS/RAS assessments, • analysis and reporting of SPS/RAS misoperations, • maintenance, testing and operational aspects of SPS/RAS.
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
The SDT will revise the definition of SPS/RAS to provide the clarity and specificity necessary for consistent identification and classification of protection schemes as SPS ~~or~~ /RAS across the eight NERC Regions. The SDT will revise or retire the six existing SPS ~~standards~~/RAS-related Reliability Standards: • PRC-012-0 Special Protection System Review Procedure • PRC-013-0 Special Protection System Database • PRC-014-0 Special Protection System Assessment • PRC-015-0 Special Protection System ~~data~~Data and Documentation • PRC-016-0.1 Special Protection System Misoperations • PRC-017-0 Special Protection System Maintenance and Testing

SAR Information
The SDT will correct the applicability in PRC-012-0, PRC-013-0, and PRC-014-0 by assigning the requirements to the specific users, owners, and operators of the ~~bulk power system~~Bulk Power System. The SDT will combine appropriate requirements from PRC-012-0, PRC-013-0, PRC-014-0, PRC-015-0, PRC-016-0.1, and PRC-~~015~~017-0 into ~~a~~one or more Reliability Standard~~-~~(s). The new standard(s) will provide specific requirements for: • review of new or modified SPS/RAS; • annual assessments of SPS/RAS in transmission planning studies; • periodic comprehensive SPS/RAS assessments; • design of SPS~~;~~/RAS; • operations and misoperations; • maintenance and testing of SPS/RAS; and • maintenance and testing of non-Protection System components used in SPS/RAS; and • coordination of SPS/RAS with other SPS/RAS, UFLS, UVLS, and Protection Systems. Due to the significant difference between Protection Systems and SPS, the subject of SPS misoperation is not addressed in the revision of Reliability Standard PRC-004. This SDT will develop a definition for SPS/RAS misoperation and revise PRC-016-0.1. The new Reliability Standard will provide specific requirements for the analysis of SPS operations and reporting of SPS misoperations. The SDT will address the complexity of maintaining and testing SPS, as well as the maintenance and testing of non-Protection System components used in SPS in a Reliability Standard. ~~-~~This SDT will coordinate with the PRC-005-4 SDT to prevent any overlaps or gaps in coverage. The SDT also will consider operational considerations for monitoring, status notification, and response to failures of SPS/RAS; and, if necessary, modify other related standards. The SDT will retire requirements that are administrative in nature that are not necessary for reliability of the Bulk-Power System, or that are superseded by other requirements; i.e., the new Reliability Standards will qualify as steady-state. No market interface impacts are anticipated.

Reliability Functions		
The Standard will Apply to the Following Functions (Check each one that applies.)		
☐	~~Regional Reliability Organization~~	~~Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.~~
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☐	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☒	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☒	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.

Reliability Functions		
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☐	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles		
Applicable Reliability Principles (Check all that apply).		
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.	
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.	
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.	
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.	
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.	
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.	
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.	
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.	
Does the proposed Standard comply with all of the following Market Interface Principles?		Enter (yes/no)
	1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
	2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes

Reliability and Market Interface Principles	
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

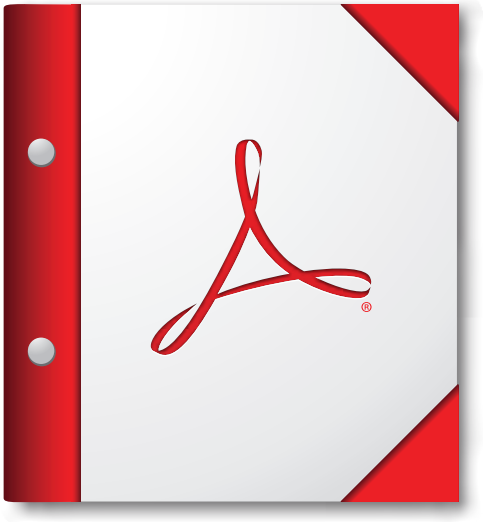
Related Standards	
Standard No.	Explanation
IRO-005-3.1a	The SDT may decide not to change this standard, but the SDT should keep the standard in mind since it contains potentially overlapping requirements.
PRC-001-1.1	The SDT may decide not to change this standard, but the SDT should keep the standard in mind since it contains potentially overlapping requirements.
PRC-005-2	The SDT may decide not to change this standard, or subsequently approved versions, but the SDT should keep the standard in mind to avoid any gaps or overlap between this standard and PRC-017-1.
PRC-010-1	The SDT may adjust the definition of Special Protection System to include centrally-controlled undervoltage-based load shedding or exclude UVLS Programs.
CIP-002, CIP-003, CIP-004, CIP-005, CIP-006 CIP-007, CIP-008, CIP-009, CIP-010 CIP-011, EOP-004, FAC-010, FAC-011, IRO-005, IRO-014, MOD-029, MOD-030, NUC-001, PRC-001, PRC-004-WECC, PRC-005, PRC-006, PRC-012, PRC-013, PRC-014,	The SDT will review all current standards that include the term SPS or RAS to ensure the modified term and definition are congruent.

Related Standards	
PRC-015, PRC-016, PRC-017, PRC-020, PRC-021, PRC-023, PRC-024, PRC-025, TOP-005, TPL-001, TPL-002, TPL-003, TPL-004; NERC Glossary of Terms: Special Protection System, Remedial Action Scheme; WECC Regional Term: Dependability-Based Misoperation, WECC Regional Term: Functionally Equivalent RAS, WECC Regional Term: Security-Based Misoperation	

Related SARs	
~~SAR ID~~Project	Explanation
Project 2008-02 – Undervoltage Load Shedding	The UVLSSDT is recommending that Project 2010-05.2 – Special Protection Systems adjust the definition of Special Protection System to include centrally-controlled undervoltage-based load shedding or exclude UVLS Programs.

Related Standards	

Regional Variances	
Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
RFC	
SERC	
SPP	
WECC	Communicate recommended changes to Regional Reliability Standard PRC-004-WECC-1, regional criteria PRC-(012 through 014)-WECC-CRT-2, and PRC-013 RAS Reporting Template; or, if necessary, incorporate a regional variance in the NERC Reliability Standards developed by this project. All changes to any WECC standards and documents will be coordinated with WECC.



For the best experience, open this PDF portfolio in Acrobat X or Adobe Reader X, or later.

Get Adobe Reader Now!

NPCC, Inc.

NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

June 13, 2014

Members, Reliability Coordinating Committee
and
Members, Task Force on Coordination of Operation
Members, Task Force on Coordination of Planning
Members, Task Force on Infrastructure Security and Technology
Members, Task Force on System Protection
Members, Task Force on System Studies

Re: Minutes of the February 26, 2014 RCC Meeting

Sir / Madam:

Attached are the minutes of the February 26, 2014 meeting of the NPCC Reliability Coordinating Committee, as approved at the June 4, 2014 meeting.

Sincerely,

Phil Fedora

Philip A. Fedora
Assistant Vice President-Reliability Services

cc: NPCC Staff

NORTHEAST POWER COORDINATING COUNCIL
Reliability Coordinating Committee Minutes
February 26, 2014

Mr. Briggs called the meeting of the Reliability Coordinating Committee (RCC), held at the New York Times Square Residence Inn by the Marriott to order at 10:00 am.

Attendance

Officers of the Reliability Coordinating Committee

Alden Briggs, Chair	New Brunswick Power Corporation
Michael Schiavone, Co-Vice Chair	National Grid USA
Brian Evans-Mongeon, Co-Vice Chair	Utility Services, Inc.

Sector 1 - Transmission Owners

Central Hudson Gas & Electric Corp.	(proxy to James McCloskey)
Central Maine Power Company	David Conroy (Alternate)
Consolidated Edison Company of New York, Inc.	Mike Forte
Long Island Power Authority	(proxy to Anie Philip – via phone)
National Grid USA	Michael Schiavone
New Brunswick Power Corporation	(proxy to Alden Briggs)
New York Power Authority	(proxy to Randy Crissman)
New York State Electric & Gas Corp.	Ray Kinney
Northeast Utilities	Brad Bentley
Nova Scotia Power Incorporated	(via written proxy)
Rochester Gas & Electric Corporation	John Allen (Alternate - via phone)
The United Illuminating Company	Robert Pelligrini Jonathan Appelbaum (via phone)
Vermont Transco	(via written proxy)

Sector 2 – Reliability Coordinators

Hydro-Québec TransÉnergie	Pierre Paquet
Independent Electricity System Operator	Barbara Constantinescu
ISO-New England, Inc.	Mike Henderson
New Brunswick Power Corporation	Alden Briggs
New York Independent System Operator	Dana Walters (Alternate)

Sector 3 – Transmission Dependent Utilities, Distribution Companies and Load Serving Entities

Hydro-Québec Distribution	Stephane Dufrense (via phone)
New York Power Authority	(proxy to Randy Crissman)
Long Island Power Authority	Anie Philip (Alternate – via phone)
Northeast Utilities	Dwayne Basler

Sector 4 Generation Owners

Dominion Energy Marking, Inc.	Mike Garton (via phone)
Dynegy, Inc.	(via written proxy)
Entergy Nuclear Northeast	Tom Czerniewski (via phone)
Long Island Power Authority	(proxy to Anie Philip – via phone)
New York Power Authority	Randy Crissman
NextEra Energy Resources	(via written proxy)
Northeast Utilities	(proxy to Dwayne Basler)

Sector 5 – Marketers, Brokers, and Aggregators

Constellation Energy Commodities Group	(via written proxy)
HQ Energy Marketing Inc.	(via written proxy)
HQ Energy Services (US) Inc.	(via written proxy)
Long Island Power Authority	(proxy to Anie Philip – via phone)
New York Power Authority	(proxy to Randy Crissman)
PPL EnergyPlus, LLC	Elizabeth Davis (Alternate - via phone)
Utility Services	Brian Evans-Mongeon

Sector 6 – State and provincial Regulatory and/or Governmental Authorities

New York Power Authority	(proxy to Randy Crissman)
New York State Department of Public Service	Ed Schrom (Alternate)

Sector 7 – Sub-Regional Reliability Councils, Customers, other Regional Entities and Interested Entities

New York State Reliability Council, LLC	Roger Clayton (via phone)

NPCC Staff

Gerry Dunbar	Manager of Reliability Criteria Requirements
Phil Fedora	Assistant Vice President, Reliability Services
Brian Hogue	Information Systems & Security Management
Stanley Kopman	Assistant Vice President of Compliance Registration & Enforcement
Quoc Le	Manager, System Planning and Protection
Jennifer Mattiello	Vice President & Chief Operating Officer
John Mosier, Jr.	Assistant Vice President of System Operations
Scott Neid	Manager, Compliance Program Development
Andrey Oks (via phone)	Manager, Reliability Performance Criteria

Frantz Roc	Manager, Information Technologies
Paul Roman	Manager, Operations Planning
Ralph Rufrano	Manager, Event Analysis
Edward Schwerdt	President & Chief Executive Officer

Guests

Paul DiFilippo	Chair, Task Force on System Protection
Marc Dusseault	Chair, Task Force on Coordination of Planning
Gregory Goodrich	Chair, Task Force on Infrastructure Security & Technology
Dean Latulipe (via phone)	Chair, SS-38 Working Group
Jim McCloskey	Central Hudson Gas & Electric
John Norden	Chair, Task Force on Coordination of Operation
Isen Widjaja (via phone)	Chair, Load Modeling Working Group
Raey Yohannes (via phone)	Entergy Services, Inc.

Quorum Statement

Mr. Fedora indicated that a quorum had been achieved, by member attendance, proxy or alternate designation. He also noted having received the following written proxies:

Sector 1 – Transmission Owners
Paul Casey – Nova Scotia Power Incorporated
Paul Renaud – Vermont Electric Power Company, Inc.

Sector 4 – Generator Owners
Allen D. Schriver - NextEra Energy Resources
James Watson – Dynegy, Inc.

Sector 5 – Marketers, Brokers, and Aggregators
Glenn McCartney - Constellation Energy Commodities Group, Inc.
Yannick Vennes – HQ Energy Marketing Inc.
Louis Guilbault - HQ Energy Services (US) Inc.

Antitrust Guidelines for NPCC Meetings

Mr. Fedora reviewed the NPCC Antitrust Guidelines in the Agenda package, and suggested contacting NPCC Inc.'s Secretary, Andrianne S. Payson, at (212) 424-8218 for further information.

President & CEO Report

Mr. Schwerdt reported on the following items:

Bulk Electric System Definition
Following a 74% affirmative vote from the industry ballot body and a unanimous approval by the NERC Board of Trustees during their November 21, 2013 teleconference meeting, NERC filed the revised BES Definition with FERC on December 13, 2013 with a request for expedited action. Timely approval by FERC is necessary for an orderly implementation in the U.S. of the revised definition effective July 1, 2014.

In anticipation of that implementation, work on BES Exception Process ERO-wide IT tool has continued, addressing some technical issues identified during the end-to-end testing by NERC and Regional staffs. Guidelines for evaluating BES exception requests and guidelines for reviewing self-determined notifications have been developed to both enhance the efficiency of the processes and to support consistency between the Regional Entities. Reference documentation for stakeholder users is under development and currently out for industry comment. Last week's RSC meeting included a review of the current draft document. Finally, stakeholder training regarding the implementation of the definition and use of the BES tool is being scheduled, including a session in conjunction with the May 2014 NPCC Compliance and Standards Workshop being held in Cooperstown, New York.

ERO Enterprise 2014-2017 Strategic Plan
The NERC Board of Trustees at its February 6, 2014 meeting approved the ERO Enterprise Strategic Plan for 2014 through 2017 as it was modified based on discussions at the previous day's Member Representatives Committee meeting. The five Enterprise-wide Goals can be summarized as follows:

- ✓ Goal 1 – Develop clear, reasonable and sound mandatory standards that are practical to implement and cost effective
- ✓ Goal 2 – Implement risk-based registration, compliance and enforcement that holds industry accountable for violations
- ✓ Goal 3 – Support a culture of compliance that addresses reliability risks and leverages the industry's internal controls
- ✓ Goal 4 - Identify and prioritize risks and consistently analyze
- ✓ events and system performance
- ✓ Goal 5 – Operate a collaborative enterprise with improved efficiencies and cost effectiveness

2015 Business Plan and Budget
NERC and the eight Regional Entities are currently working on establishing shared business plan and budget assumptions to support the development of a more collaborative ERO Enterprise plan for the 2015 Business Cycle. NPCC will be providing an initial draft of its 2015 Business Plan and Budget to the NPCC Finance and Audit Committee in

mid-April, with a review by the full Board scheduled for their April 29, 2014 meeting. NERC is looking to post Draft 1 of its 2015 Business Plan and Budget, along with all of the Regional Entity BP&Bs by mid-May. A presentation to the RCC on the NPCC BP&B is scheduled for the June RCC meeting, with final NPCC Board approval expected in late June.

Chair Report

Meeting Agenda

Mr. Briggs said he had received no changes to the meeting Agenda as provided in the Agenda package.

The RCC then approved the Agenda.

Events Analysis "Lessons Learned" Template

Mr. Briggs refereed to the Events Analysis "Lessons Learned" Template provided in the Agenda package. He stated that comments received from the RCC review of the template have been incorporated.

Common Task Force Statement of Purpose

Mr. Briggs indicated that the Task Force Chairs have agreed to common wording for their respective Task Force's Statement of Purpose; the Task Forces will be presenting their revised Task Force Scopes for approval at the June 2014 RCC meeting.

Approved 2014-2015 RCC Work Plan

Mr. Briggs explained that at their January 29, 2014 meeting, the NPCC Board approved the 2014-2015 RCC Work Plan, adding the highlighted words "to the extent possible, are conducted in an efficient and cost-effective manner," as shown in the Agenda package.

Consent Agenda

The Reliability Coordinating Committee unanimously approved the following Consent Agenda items (all written proxies in favor, with three abstentions: Sector 5, Marketers, Brokers, and Aggregators - Glen McCartney, Constellation Energy Commodities Group, Inc., Louis Guilbault, HQ Energy Services (US) Inc., and Yannick Vennes, HQ Energy Marketing Inc.):

September11, 2013 Meeting Minutes

The Draft-For-Approval Minutes of the December 3, 2013 Reliability Coordinating Committee were approved, with corrections noted.

RCC Membership Changes

The following changes to RCC Membership were approved:

Sector 1, Transmission Owners

- ✓ Mr. James McCloskey of Central Hudson Gas & Electric Corporation succeeds Mr. Thomas C. Duffy, as the member.

Task Force Roster Changes

The following changes to Task Force and Working Group memberships were approved:

Task Force on Coordination of Operation

- ✓ Mr. Robert Reinmuller succeeds Mr. Paul Tremblay as a member, both of Hydro One, Inc.
- ✓ Mr. Tony O'Hara succeeds Mr. Alden Briggs as a member, both of New Brunswick Power Corporation.

CO-1 Control Performance Working Group

- ✓ Mr. David Devereaux to represent the Ontario Independent Electric System Operator as an alternate.
- ✓ Mr. Ed Rappold to represent ISO-New England as an alternate.

CO-2 Working Group on System Operator Training

- ✓ Ms. Diane Leferriere of HQ TransEnergie succeeds Mr. Stephen George of ISO New England, Inc. as Chair.
- ✓ Mr. Eduardo Sanchez to replace Mr. Stephen George as the ISO-New England, Inc. as member.
- ✓ Mr. Keith Harris of New York Independent System Operator to serve as Vice Chair.

CO-12 System Operator Training Working Group

- ✓ Mr. Michael Courchesne to replace Mr. Yan Beachamp as the CO-12 Chairman.
- ✓ Ms. Candida D'Costa to replace John Medal as the IESO alternate representative.

SS-38 Inter-Area Dynamic Analysis Working Group

- ✓ Mr. Emeka Ojukwu will represent New York Independent System Operator as a member. Mr. Tao has retired.

SS-38 Load Modeling Ad Hoc Working Group

- ✓ Mr. Daniele D'Aquila succeeds Mr. Tao as member.

Interim Review of Resource Adequacy

Approved as provided in the Agenda package. Mr. Bentley noted corrections to his transmittal letters.

2013 NPCC SPS List, BPS List, UVLS Program List, Major Projects List, and DCT Exclusions List

Approved as referenced in the Agenda package.

A-10 Implementation Plan Update

Approved as provided in the Agenda package.

Chicopee Alternative UFLS Plan

Approved as provided in the Agenda package.

Reliability Coordinating Committee Actions

NPCC 2013 Long Range Adequacy Overview

Mr. Fedora explained that this study evaluated, on a consistent basis, the long range adequacy of NPCC and neighboring Regions' plans to meet their Loss of Load Expectation (LOLE) planning criteria through a multi-area probabilistic assessment for the period from 2014 to 2018, based on the reported NERC 2013 Long Term Reliability Assessment data.

Mr. Dusseault added that the Task Force on Coordination of Planning discussed and approved the overview at their February 5, 2014, meeting, and requested RCC approval.

The RCC then approved the NPCC 2013 Long Range Adequacy Overview as provided in the Agenda (all written proxies in favor, with two abstentions: Sector 5, Marketers, Brokers, and Aggregators - Louis Guilbault, HQ Energy Services (US) Inc., and Yannick Vennes, HQ Energy Marketing Inc.).

Mr. Henderson indicated he would be contacting Mr. Fedora suggesting some editorial changes following the meeting.

2014 NPCC Summer Reliability Assessment

Mr. Roman presented the preliminary results of the "*2014 NPCC Summer Reliability Assessment*" provided in the Agenda package. He explained that the NPCC CO-12 Seasonal Assessment Working Group focused on the assessment of reliability within NPCC for the 2014 Summer Operating Period.

Mr. Fedora then provided the CP-8 Working Group's multi-area probabilistic reliability assessment regarding the estimated use of operating procedures designed to mitigate resource shortages for the same period. He also provided the RCC with the preliminary weather projection for the 2014 summer period.

In response to a question, Mr. Fedora indicated that the assessment also compares last year's actual experience with that estimated in the previous year's (2013) assessment.

The schedule for RCC review and Task Force approvals was discussed; public release of the assessment will be provided at a May 1, 2014 Media Event.

Status Reports

Mr. Briggs referred the RCC to the materials provided in the Agenda package; the RCC discussed the following Agenda items:

NPCC Regional Standards Committee (RSC) Report

Mr. Dunbar highlighted the materials described in the Agenda package; he indicated that the pace of NERC Standard development activity has been very aggressive this year, and that this high level of activity is expected to continue going forward in 2014. He then highlighted the following activities:

- ✓ approval of the NPCC Regional Standard Processes Manual;
- ✓ development of the continent wide Disturbance Monitoring Standard PRC-002-02, and the related Cost Effective Analysis Process; and,
- ✓ development of the continent-wide Cost Effective Analysis Process.

NPCC Reliability Directory Status Report

Mr. Dunbar referred the RCC to the materials provided in the Agenda package.

NPCC Compliance Committee

Mr. Kopman provided a brief summary of the materials provided in the Agenda package, and provided a highlight of aspects of the RAI Pilot Program. Mr. Schwerdt added that transitioning toward the uniform ERO-wide Self-Certification schedule described in the Agenda package will provide greater consistency and lessen the burden for those registered in more than one Region.

SS-38 Working Group Update

Mr. Widjaja stated that the SS-38 Load Modeling Working Group continues to make progress on the load modeling study effort, and reviewed the materials provided in the Agenda package.

Mr. Latulipe indicated that the SS-38 Working Group on Inter-Area Dynamic Analysis continues to make good progress on the UFLS Adequacy Assessment Study. He reported that the S-38 Working Group has mostly completed the work on identification of islands to be studied by performing coherent generation analysis including the use multiple methods of forming islands. Results of the work completed by each Area are being documented; during the first Quarter of 2014, all Areas are expected to complete the preliminary assessment of the NPCC UFLS program. Sensitivity analysis will be conducted during this summer.

TFCO/TFCP Phase 2 revision of Directory No. 1

Mr. Dunbar reported that the CP-11 /CO-7 Working Group have reviewed the revision of Directory No. 1 through a series of weekly WebEx meetings in 2013 and posted the draft of the Directory for Open Process review on December 11, 2013; the review concluded on January 25, 2014.

The CP-11/CO-7 Working Group has reconvened and will be considering any resultant revision of Directory No. 1 to address the comments received.

TFIST Cyber Update

Mr. Goodrich highlighted the following items provided in the Agenda package:

- ✓ an update on CIP Version 5;
- ✓ FERC Order 791; and,
- ✓ NERC Project: 2014-2 - CIP Version 5 Revisions Standard Drafting Team activities.

The RCC discussed substation relay communication with respect to the level of protection to be assigned under CIP-002-5.

TFSP Update

Mr. DiFilippo referred the RCC to the materials provided in the Agenda package regarding the SP-7 Working Group's review of Protection Systems Misoperations and the BPS Risk Reduction Implementation Status Report.

2013-2014 Task Force Work Plan Progress

The Chairs of the NPCC Task Forces provided a brief summary of their respective 2013-2014 Task Force Work Plan Progress reports provided in the Agenda package.

NPCC Reliability Assessment Program (NRAP) Highlights Report

Mr. Fedora indicated that the '*NPCC Reliability Assessment Program Highlights Report*' has been updated as of February 21, 2014 and is posted on the NPCC website.

NERC Agenda Items

Operating Committee (OC)

Mr. Mosier reviewed the following March 2014 NERC Operating Committee Agenda items:

- ✓ continued monitoring of the implementation of the Operating Reliability Coordination Agreement;
- ✓ review of the Geomagnetic Disturbance Planning Guide; and,
- ✓ the transition of NERCnet to the Eastern Interconnection Data Sharing Network.

Planning Committee (PC)

Mr. Fedora reviewed the following March 2014 NERC Planning Committee Agenda items:

- ✓ roundtable discussion of identified strategic Regional issues to help the Planning Committee prioritize its work activities moving forward;
- ✓ formation of the Essential Reliability Services Task Force;
- ✓ Integration of Variable Generation Task Force follow-up activities; and,
- ✓ approval of a revised metric for ALR1-4 – one that better reflects the loss of supply from BPS generation/transmission events rather than from distribution level events.

Critical Infrastructure Protection Committee (CIPC)

Mr. Hogue reported that there were no voting items on the March 2014 NERC Critical Infrastructure Committee Agenda; the previously identified Cyber Security issues will be discussed.

Informational Items

Mr. Briggs referred the RCC to the materials included in the Agenda package. The following Informational Items were discussed at the meeting:

Executive Order and Presidential Policy Directive 21/NIPP/NIST Update

Mr. Goodrich provided an update of the information provided in the Agenda package regarding the National Infrastructure Protection Plan and the 2014 NIST Framework for Improving Critical Infrastructure Cybersecurity. He explained that the Integrated Task Force will continue on information sharing, research and development with a focus on public and private sector partnership. The re-alignment within US Government agencies impacted Sector Specific that spawned updates to the Electric Sub-sector Coordinating Council.

Cyber-Physical Security Update

Mr. Goodrich provided an overview of the material provided in the Agenda package. He stated the GridEx II report is expected to be released soon, and described plans for GridEx III in 2015.

White House Quadrennial Energy Review

Mr. Goodrich referred the RCC to the materials in the Agenda package regarding the Presidential Memorandum that established a Quadrennial Energy Review.

Definition of the Bulk Electric System

Mr. Fedora described the recent activities related to the revised definition of the Bulk Electric System (BES). They included posting of guidance documents and other supporting materials on the NERC Bulk Electric System Definition, Notification, and Exception Process Project Web Page.

He also reminded the RCC of the BES related sessions scheduled for the Spring NPCC Compliance and Standards Workshop. A pre-Workshop training session is scheduled for explaining how to submit BES Self-Determined Notifications and BES Exception Requests through the BESNet application.

Events Analysis Program – Overview and Status

Mr. Rufrano provided a status and overview of the Events Analysis program provided in the Agenda package.

July 3rd Quebec Event

Mr. Paquet provided a brief overview of the July 3, 2013 Quebec event. He indicated that Quebec is in the process of providing the NPCC Task Forces detailed presentations of the event and Quebec's Action Plan to address the lessons learned. He stated that a Final Report summarizing the event and any corresponding NPCC Task Force recommendations are expected to be presented at the June 2014 RCC meeting.

Eastern Interconnection Frequency Response Activities

Mr. Briggs referred the RCC to the materials in the Agenda package.

Other Matters

Mr. Briggs noted the announced retirement of Ms. Constantinescu from the IESO and recognized her contributions. She responded that she was grateful to be provided the opportunity to work with the RCC over the years. The RCC wished her the very best in her future plans.

The RCC meeting was then adjourned.

Next RCC Meeting Date	Location
June 4, 2014	New York Times Square Residence Inn by the Marriott

Distribution of Approved Minutes

NPCC Full & General Member Representatives and Alternates
Members, NPCC Board of Directors
Members, NPCC Reliability Coordinating Committee
Members, NPCC Public Information Committee
Members, NPCC Compliance Committee
Members, NPCC Regional Standards Committee
Members, NPCC Task Force on Coordination of Operation
Members, NPCC Task Force on Coordination of Planning
Members, NPCC Task Force on Infrastructure Security and Technology
Members, NPCC Task Force on System Protection
Members, NPCC Task Force on System Studies
NPCC Officers
NPCC Staff
Andrew J. Fawbush, Esq.
Andrianne S. Payson, Esq.
and
Federal Energy Regulatory Commission – Mike Bardee, David O'Connor, Juan Villar

La Régie de L'Énergie – Daniel Soulier
Ontario Energy Board – Peter Fraser
United States Department of Energy – David Meyer
New Brunswick Department of Energy and Mines – David Sallows
Nova Scotia Utility & Review Board – S. Bruce Outhouse, Q.C.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2007-11 Disturbance Monitoring

Requested Approvals

- PRC-002-2 Disturbance Monitoring and Reporting Requirements

Requested Retirements

- PRC-002-1 Define Regional Disturbance Monitoring and Reporting Requirements
- PRC-018-1 Disturbance Monitoring Equipment Installation and Data Reporting

Prerequisite Approvals

- None

Applicable Entities

- Planning Coordinator
- Reliability Coordinator
- Transmission Owner
- Generator Owner

Revisions to Defined Terms in the NERC Glossary

~~The standard drafting team proposes the following new definitions:~~	
~~Dynamic Disturbance Recording (DDR)~~	~~The recording of time sequenced data for dynamic power system characteristics such as power swings, frequency variations, and abnormal voltage problems.~~
~~Fault Recording (FR)~~	~~The recording of time sequenced waveform data for short circuits or failure of Elements resulting in abnormal voltage(s) and /or current(s).~~
~~Sequence of Events Recording (SOER)~~	~~The recording of time sequenced data for change in status of Elements, which may include protection and control devices.~~

Background

The Implementation Plan reflects consideration of the following:

1. This standard reflects the need for data, rather than equipment, with the understanding that the data is collected from Disturbance Monitoring Equipment distributed across the BES~~system~~.
2. A significant amount of s~~S~~equence of ~~E~~sevents ~~R~~recording (SER), f~~F~~ault r~~R~~ecording (FR), and d~~D~~ynamic d~~D~~isturbance r~~R~~ecording (DDR) equipment already exists on the BES. The monitoring~~location~~ requirements in this standard align with industry practices ~~for locating this equipment~~. Therefore, many existing recordings can~~-~~ satisfy the Requirements and Implementation Plan put forth.
3. Fault MVA data is readily available or calculable by the Transmission Owners for the BES buses ~~locations~~ they own. Therefore, six (6) months is adequate time for generating the list of BES bus locations following the methodology described in Attachment 1 (Requirement R1).
4. Responsible Entities have the relevant data and information pertaining to the BES Elements requiring DDR~~ynamic Disturbance Recording~~ and six (6) months is adequate time for working with any affected Entities and generating the list of BES Elements.
5. The nine (9) month time period for ~~R2, R7, and~~ R124 includes the six (6) month implementation for R1, and R56 ~~(refer to 3, and 4 preceding), and a three (3) month additional time period to make notifications.~~ The nine (9) months for R124 implementation is reasonable for the contents of that requirement. ~~All requirements pertaining to possible implementation of equipment are referenced to notification of the list of bus locations or Elements to account for any delays in the process of location and Element selection.~~
6. A total percentage (%) of BES buses ~~locations~~ and BES Elements established in Requirements R1 and R56 respectively, are used in the Implementation Plan since these lists are explicitly created and readily available. It is expected that many locations will become compliant with incremental changes to recording.
7. A graduated approach to implementation recognizes that progress will be made while attempting to minimize any potential significant impact to the Entities. ~~The timelines put forth allow for inertial delays in implementing new equipment or technologies (e.g. developing new standards and processes, testing and energization, and project management).~~
8. Implementation of disturbance monitoring following changes to the system are addressed ~~by referencing the Implementation Plan to the time of notification following reassessment. Changes to disturbance monitoring are only required for identified bus locations or Elements~~ following reassessment of the lists as per Requirement R1~~, Part 1.2~~ and Requirement R56~~, Part 6.2~~.

9. Implementing SOER, FR, and DDR may require scheduled outages for both Transmission Owners and Generator Owners. Generator Owners may have outage cycles of 24 months or more depending on the type and characteristics of the generating units or plant. Meanwhile, Transmission Owners will have more Elements requiring SOER, FR, and DDR and may have to schedule outages across the system. The Implementation Plan takes this into account for scheduling outages.
10. An Entity owning only one (1) identified bus location, Element, or generating unit is allowed four (4) years for implementation to accommodate normal outage schedules.
11. The Implementation Plan accounts for any increase in requests to vendors for this technology or equipment that could impact implementation timelines for the respective Entities.

General Considerations

Each Transmission Owner and Generator Owner shall maintain the ability to provide Disturbance Monitoring data using current methods until the entity meets the requirements of PRC-002-2 in accordance with this Implementation plan. As required in PRC-018-1 Disturbance Monitoring Equipment Installed and Data Reporting, Requirement R1, Parts 1.1 and 1.2, it is expected that the Transmission Owner and Generator Owner will have those functionalities in regards to their current Disturbance Data.

Effective Date

The standard shall become effective on the first day of the first calendar quarter six (6) months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter six (6) months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Standard(s) for Retirement

PRC-002-1 Midnight of the day immediately prior to the Effective Date of PRC-002-2 in the particular jurisdiction in which the new standard is becoming effective.

Each Transmission Owner, and Generator Owner shall maintain documentation to demonstrate compliance with PRC-018-1 until that entity meets the requirements of PRC-002-2 in accordance with this Implementation Plan. Standard PRC-018-1 shall remain effective throughout the phased implementation period of PRC-002-2 and shall be applicable to an entity's Disturbance Monitoring and Reporting activities not yet transitioned to PRC-002-2. PRC-018-1 will be retired following full implementation of PRC-002-2 as noted below.

PRC-018-1 Midnight of the day immediately prior to six (6) years after the Effective Date of PRC-002-2 in the particular jurisdiction in which the new standard is becoming effective.

~~**Implementation Plan for Definitions**~~

~~Entities shall use these definitions when implementing any requirement in this standard that references one of the definitions.~~

Implementation Plan for PRC-002-2 Requirements R1 and R5~~6~~:

Entities shall be 100% compliant on the first day of the first calendar quarter six (6) months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is six (6) months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Implementation Plan for PRC-002-2 Requirement~~s R2, R7, and~~ R1~~2~~4~~~~:

Entities shall be 100% compliant on the first day of the first calendar quarter nine (9) months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is nine (9) ~~-~~months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Implementation Plan for PRC-002-2 Requirements R2, R3, R4, R5, R6~~8~~, R7~~9~~, R8~~10~~, R9~~11~~, R10~~12~~ and R11~~13~~:

Entities shall be at least 50% compliant within four (4) years of the Effective Date of PRC-002-2 and fully compliant within six (6) years of the Effective Date.

Entities that own only one (1) identified BES bus , BES Element, or generating unit shall be fully compliant within six (6) years of the Effective Date.

~~Entities shall be compliant with the initial list of BES bus locations in Requirement R1 and list of Elements in Requirement R6 within the following:~~

- ~~Following governmental authority or as otherwise provided for in jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect,~~
  - ~~At least 25% compliant within two (2) years following notification of the list~~
  - ~~At least 50% compliant within three (3) years following notification of the list~~

- ~~100% compliant within four (4) years following notification of the list~~

- ~~**Note**: Entities that own only one (1) identified BES bus location, Element, or generating unit shall be 100% compliant within four (4) years following notification of the list.~~

- ~~Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is forty-eight (48) months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction,~~

Entities shall be 100% compliant with a reassessed list from Requirement R1~~, Part 1.2~~ or R5~~6, Part 5~~6.2 within three (3) years following notification of the list.

Conforming Changes to Other Standards

Where conflicts between the continent-wide standard PRC-002-2 and a regional standard exist, entities should comply with PRC-002-2. Conflicts will be addressed in the regional standards development process.

- The following conflicts PRC-002-2 Requirement R3 stipulates data must be captured by fault recording to determine electrical quantities. PRC-002-NPCC-01 Requirement R3 stipulates the recording of those quantities.
- PRC-002-2 Requirement R5 stipulates the capture of dynamic disturbance recording data for HVDC. PRC-002-NPCC-01 does specify HVDC.

PRC-002-2 Requirement R8 recognizes dynamic disturbance recording that is not continuous. PRC-002-NPCC-01 addresses dynamic disturbance recorders installed after the standard was approved have to be continuous.

Implementation Plan Summary											
Requirement	Entity	Identify bus locations/ Elements	Notification	SOE	FR	DDR	Time Sync	5 Year Assessment	Other	Percent Compliant	Following compliance instructions noted for each requirement above:
R1	TO	X	X	X	X			X		100	Six (6) months
R2	TO		X							100	Nine (9) months
R23	TO/GO			X						25	Two (2) years
										50	Three (3) years
										100	Four (4) years
R34	TO/GO				X					25	Two (2) years
										50	Three (3) years
										100	Four (4) years
R45	TO/GO				X					25	Two (2) years
										50	Three (3) years
										100	Four (4) years
R56	RE (PC or RC)	X	X			X		X		100	Six (6) months
R7	RE (PC or RC)		X							100	Nine (9) months
R68	RE (PC or RC)TO					X				25	Two (2) years
										50	Three (3) years
										100	Four (4) years
R79	TGO					X				25	Two (2) years
										50	Three (3) years
										100	Four (4) years
R810	TO/GO					X				25	Two (2) years
										50	Three (3) years
										100	Four (4) years
R911	TO/GO					X				25	Two (2) years
										50	Three (3) years
										100	Four (4) years
R102	TO/GO						X			25	Two (2) years
										50	Three (3) years
										100	Four (4) years
R113	TO/GO								X	25	Two (2) years
										50	Three (3) years
										100	Four (4) years
R124	TO/GO								X	100	Nine (9) months

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2007-11 Disturbance Monitoring

VRF and VSL Justifications

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in PRC-002-2 – Disturbance Monitoring and Reporting Requirements.

Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined by the ERO Sanctions Guidelines.

The Disturbance Monitoring and Reporting Requirements Standard Drafting Team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project:

NERC Criteria –VRFs

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

FERC VRF Guidelines

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

The Commission seeks to ensure that Violation Risk Factors assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System.

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

Guideline (3) – Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) –Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

VRF and VSL Justifications – PRC-002-2, R1	
Proposed VRF	**Lower**
NERC VRF Discussion	R1 is a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** R1 establishes the list of Sequence of Events Recordings and Fault Recordings that is consistent with FERC guideline G1, Recommendation 12 of the Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has parts that are of equal importance; only one VRF was assigned so there is no conflict.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This requirement calls for establishing a list of BES bus locations for Sequence of Events Recording and Fault Recording using the selection procedure in Attachment 1. The team could not identify other continent-wide reliability standards of the same nature.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to establish the list of BES bus locations for Sequence of Events Recording and Fault Recording could not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1 contains only one objective which is to establish a list of BES bus locations for Sequence of Events Recording and Fault Recording and to review the list every 5 calendar years. Since the requirement has only one objective, only one VRF was assigned.

VRF and VSL Justifications – PRC-002-2, R1	
Proposed Lower VSL	The Transmission Owner identified the BES buses as directed by Requirement R1 for more than 80% but less than 100% of the required BES buses. OR The Transmission Owner assessed the BES buses as directed by Requirement R1 but was late by 30 calendar days or less. OR The Transmission Owner as directed by Requirement R1 was late in notifying the other owners by 10 calendar days or less. ~~The Transmission Owner identified the bus locations as directed by Requirement R1, Part 1.1 for more than 80% but less than 100% of the required bus locations.~~ ~~OR~~ ~~The Transmission Owner assessed the bus locations as directed by Requirement R1, Part 1.2 but was late by 30 calendar days or less.~~
Proposed Moderate VSL	The Transmission Owner identified the BES buses as directed by Requirement R1 for more than 70% but less than or equal to 80% of the required BES buses. OR The Transmission Owner assessed the BES buses as directed by Requirement R1 but was late by greater than 30 calendar days and less than or equal to 60 calendar days. OR The Transmission Owner as directed by Requirement R1 was late in notifying the other owners by greater than 10 calendar days but less than or equal to 20 calendar days.~~The Transmission Owner identified the bus locations as directed by Requirement R1, Part 1.1 for more than 70% but less than or equal to 80% of the required bus locations.~~ ~~OR~~ ~~The Transmission Owner assessed the bus locations as directed by Requirement R1, Part 1.2 but was late by greater than 30 calendar days and less than or equal to 60 calendar days.~~

VRF and VSL Justifications – PRC-002-2, R1	
Proposed High VSL	The Transmission Owner identified the BES buses as directed by Requirement R1 for more than 60% but less than or equal to 70% of the required BES buses. OR The Transmission Owner assessed the BES buses as directed by Requirement R1 but was late by greater than 60 calendar days and less than or equal to 90 calendar days. OR The Transmission Owner as directed by Requirement R1 was late in notifying the other owners by greater than 20 calendar days but less than or equal to 30 calendar days.~~The Transmission Owner identified the bus locations as directed by Requirement R1, Part 1.1 for more than 60% but less than or equal to 70% of the required bus locations.~~ ~~OR~~ ~~The Transmission Owner assessed the bus locations as directed by Requirement R1, Part 1.2 but was late by greater than 60 calendar days and less than or equal to 90 calendar days.~~
Proposed Severe VSL	The Transmission Owner identified the BES buses as directed by Requirement R1for less than or equal to 60% of the required BES buses. OR The Transmission Owner assessed the BES buses as directed by Requirement R1but was late by greater than 90 calendar days. OR The Transmission Owner as directed by Requirement R1 was late in notifying one or more other owners by greater than 30 calendar days. ~~The Transmission Owner identified the bus locations as directed by Requirement R1, Part 1.1 for less than or equal to 60% of the required bus locations.~~ ~~OR~~ ~~The Transmission Owner assessed the bus locations as directed by Requirement R1, Part 1.2 but was late by greater than 90 calendar days.~~

VRF and VSL Justifications – PRC-002-2, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	PRC-002-2 differs from PRC-002-1 (not enforceable) and PRC-018-1 (enforceable and will be retired upon approval of PRC-002-2) in that PRC-002-2 deals with Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording in order to adequately capture data for events analysis; and not equipment as referenced in the PRC-002-1 and PRC-018-1. Therefore, the VSL's cannot be compared between PRC-002-2 and PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.

VRF and VSL Justifications – PRC-002-2, R1	
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Non CIP
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Non CIP

~~VRF and VSL Justifications – PRC-002-2, R2~~	
~~**Proposed VRF**~~	~~**Lower**~~
~~NERC VRF Discussion~~	~~R2 is a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES.~~
~~FERC VRF G1 Discussion~~	~~**Guideline 1- Consistency w/ Blackout Report**~~ ~~R2 requires the Transmission Owner to notify the other affected owners to provide Sequence of Events Recordings and Fault Recordings at bus locations selected in Requirement R1. This is consistent with FERC guideline G1, Recommendation 12 of the Blackout Report.~~
~~FERC VRF G2 Discussion~~	~~**Guideline 2- Consistency within a Reliability Standard**~~ ~~This requirement does not have parts.~~
~~FERC VRF G3 Discussion~~	~~**Guideline 3- Consistency among Reliability Standards**~~ ~~This requirement calls for notifying the other affected owners to~~

VRF and VSL Justifications – PRC-002-2, R2	
	provide Sequence of Events Recordings and Fault Recordings at bus locations selected in Requirement R1. The team could not identify other continent-wide reliability standards of the same nature.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to notify the owners of BES bus locations for Sequence of Events Recording and Fault Recording selected in R1 could not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective which is to notify the owners of BES bus locations for Sequence of Events Recording and Fault Recording selected in R1.
Proposed Lower VSL	The Transmission Owner as directed by Requirement R2 was late in notifying the owners by 10 calendar days or less.
Proposed Moderate VSL	The Transmission Owner as directed by Requirement R2 was late in notifying the owners by greater than 10 calendar days but less than or equal to 20 calendar days.
Proposed High VSL	The Transmission Owner as directed by Requirement R2 was late in notifying the owners by greater than 20 calendar days but less than or equal to 30 calendar days.
Proposed Severe VSL	The Transmission Owner as directed by Requirement R2 was late in notifying one or more owners by greater than 30 calendar days.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	PRC-002-2 differs from PRC-002-1 (not enforceable) and PRC-018-1 (enforceable and will be retired upon approval of PRC-002-2) in that PRC-002-2 deals with Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording in order to adequately capture data for events analysis; and not equipment as referenced in the PRC-002-1 and PRC-018-1. Therefore, the VSL's cannot be compared between PRC-002-2 and PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2	Guideline 2a:

VRF and VSL Justifications — PRC-002-2, R2	
Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The VSL assignment is for R2 is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Non CIP
FERC VSL G6 VSLs for cyber security requirements containing	Non CIP

~~VRF and VSL Justifications – PRC-002-2, R2~~	
~~interdependent tasks of documentation and implementation should account for their interdependence~~	

VRF and VSL Justifications – PRC-002-2, R2~~3~~	
Proposed VRF	**Lower**
NERC VRF Discussion	R2~~3~~ is a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state of capability of the BES, or the ability to effectively monitor, control, or restore the BES.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** R2~~3~~ provides criteria for Sequence of Events Recording which falls under Recommendation 12 of the Blackout Report and is consistent with FERC guideline G1.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** This requirement does not have parts.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This requirement establishes criteria for Sequence of Events Recording selected in R1, Attachment 1. The team could not identify other continent-wide reliability standards of the same nature.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to establish criteria for Sequence of Events Recording could not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2~~3~~ contains only one objective which is to establish criteria for Sequence of Events Recording. Since the requirement has only one objective, only one VRF was assigned.

VRF and VSL Justifications – PRC-002-2, R2~~3~~	
Proposed Lower VSL	Each Transmission or Generator Owner as directed by Requirement R2 had more than 75% but less than 100% of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the bus locations as per Requirement R2.~~Each Transmission or Generator Owner as directed by Requirement R3 implemented more than 75% but less than 100% of the total Sequence of Events Recording for circuit breaker position (open/close) for each of the circuit breakers at the bus locations established in Requirement R1.~~
Proposed Moderate VSL	Each Transmission or Generator Owner as directed by Requirement R2 had more than 50% but less than or equal to 75% of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the bus locations as per Requirement R2.~~Each Transmission or Generator Owner as directed by Requirement R3 implemented more than 50% but less than or equal to 75% of the total Sequence of Events Recording for circuit breaker position (open/close) for each of the circuit breakers at the bus locations established in Requirement R1.~~
Proposed High VSL	Each Transmission or Generator Owner as directed by Requirement R2 had more than 10% but less than or equal to 50% of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the bus locations as per Requirement R2.~~Each Transmission or Generator Owner as directed by Requirement R3 implemented more than 10% but less than or equal to 50% of the total Sequence of Events Recording for circuit breaker position (open/close) for each of the circuit breakers at the bus locations established in Requirement R1.~~
Proposed Severe VSL	Each Transmission or Generator Owner as directed by Requirement R2 had from 0% but less than or equal to 10% of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the bus locations as per Requirement R2.~~Each Transmission or Generator Owner as directed by Requirement R3 implemented from 0% but less than or equal to 10% of the total Sequence of Events Recording for circuit breaker position (open/close) for each of the circuit breakers at the bus locations established in Requirement R1.~~
FERC VSL G1	PRC-002-2 differs from PRC-002-1 (not enforceable) and PRC-018-1

VRF and VSL Justifications – PRC-002-2, R2~~3~~	
Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	(enforceable and will be retired upon approval of PRC-002-2) in that PRC-002-2 deals with Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording in order to adequately capture data for events analysis; and not equipment as referenced in the PRC-002-1 and PRC-018-1. Therefore, the VSL's cannot be compared between PRC-002-2 and PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R2~~3~~ is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5	Non CIP

VRF and VSL Justifications – PRC-002-2, R23	
Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Non CIP

VRF and VSL Justifications – PRC-002-2, R34	
Proposed VRF	**Lower**
NERC VRF Discussion	R34 is a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state of capability of the BES, or the ability to effectively monitor, control, or restore the BES.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** R43 provides criteria for Fault Recordings which falls under Recommendation 12 of the Blackout Report and is consistent with FERC guideline G1.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has parts that are of equal importance; only one VRF was assigned so there is no conflict.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This requirement establishes criteria for Fault Recording selected in R1, Attachment 1. The team could not identify other continent-wide reliability standards of the same nature.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to establish criteria for Fault Recording could not directly affect

VRF and VSL Justifications – PRC-002-2, R3~~4~~	
	the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R3~~4~~ contains only one objective which is to establish criteria for Fault Recording. Since the requirement has only one objective, only one VRF was assigned.
Proposed Lower VSL	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 75% but less than 100% of the total set of required electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities per each Element.~~The Transmission Owner or Generator Owner implemented Fault Recording as directed by Requirement R4, Parts 4.1 and 4.2 that covers more than 75% but less than 100% of the total set of required electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities per each Element.~~
Proposed Moderate VSL	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 50% but less than or equal to 75% of the total set of required electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities per each Element.~~The Transmission Owner or Generator Owner implemented Fault Recording as directed by Requirement R4, Parts 4.1 and 4.2 that covers more than 50% but less than or equal to 75% of the total set of required electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities per each Element.~~
Proposed High VSL	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 10% but less than or equal to 50% of the total set of required electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities per each Element.~~The Transmission Owner or Generator Owner implemented Fault Recording as directed by Requirement R4, Parts 4.1 and 4.2 that~~

VRF and VSL Justifications – PRC-002-2, R3~~4~~	
	~~covers more than 10% but less than or equal to 50% of the total set of required electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities per each Element.~~
Proposed Severe VSL	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 0% but less than or equal to 10% of the total set of required electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities per each Element.~~The Transmission Owner or Generator Owner implemented Fault Recording as directed by Requirement R4, Parts 4.1 and 4.2 that covers more than 0% but less than or equal to 10% of the total set of required electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities per each Element.~~
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	PRC-002-2 differs from PRC-002-1 (not enforceable) and PRC-018-1 (enforceable and will be retired upon approval of PRC-002-2) in that PRC-002-2 deals with Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording in order to adequately capture data for events analysis; and not equipment as referenced in the PRC-002-1 and PRC-018-1. Therefore, the VSL's cannot be compared between PRC-002-2 and PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments	Guideline 2a: The VSL assignment is for R4 is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – PRC-002-2, R3~~4~~	
that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Non CIP
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Non CIP

VRF and VSL Justifications – PRC-002-2, R4~~5~~

VRF and VSL Justifications – PRC-002-2, R4~~5~~	
Proposed VRF	**Lower**
NERC VRF Discussion	R4~~5~~ is a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state of capability of the BES, or the ability to effectively monitor, control, or restore the BES.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** R4~~5~~ provides criteria for Fault Recordings which falls under Recommendation 12 of the Blackout Report and is consistent with FERC guideline G1.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has parts that are of equal importance; only one VRF was assigned so there is no conflict.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This requirement establishes criteria for Fault Recordings selected in R1, Attachment 1. The team could not identify other continent-wide reliability standards of the same nature.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to establish criteria for Fault Recording could not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R4~~5~~ contains only one objective which is to establish criteria for Fault Recording. Since the requirement has only one objective, only one VRF was assigned.
Proposed Lower VSL	The Transmission Owner or Generator Owner had FR data that meets more than 75% but less than 100% of the total recording properties as specified in Requirement R4.~~The Transmission Owner or Generator Owner implemented Fault Recording that meets more than 75% but less than 100% of the total recording properties as specified in Requirement R5.~~
Proposed Moderate VSL	The Transmission Owner or Generator Owner had FR data that meets

VRF and VSL Justifications – PRC-002-2, R4~~5~~	
	more than 50% but less than or equal to 75% of the total recording properties as specified in Requirement R4.~~The Transmission Owner or Generator Owner implemented Fault Recording that meets more than 50% but less than or equal to 75% of the total recording properties as specified in Requirement R5.~~
Proposed High VSL	The Transmission Owner or Generator Owner had FR data that meets more than 10% but less than or equal to 50% of the total recording properties as specified in Requirement R4.~~The Transmission Owner or Generator Owner implemented Fault Recording that meets more than 10% but less than or equal to 50% of the total recording properties as specified in Requirement R5.~~
Proposed Severe VSL	The Transmission Owner or Generator Owner had FR data that meets more than 0% but less than or equal to 10% of the total recording properties as specified in Requirement R4.~~The Transmission Owner or Generator Owner implemented Fault Recording that meets more than 0% but less than or equal to 10% of the total recording properties as specified in Requirement R5.~~
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	PRC-002-2 differs from PRC-002-1 (not enforceable) and PRC-018-1 (enforceable and will be retired upon approval of PRC-002-2) in that PRC-002-2 deals with Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording in order to adequately capture data for events analysis; and not equipment as referenced in the PRC-002-1 and PRC-018-1. Therefore, the VSL's cannot be compared between PRC-002-2 and PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is	Guideline 2a: The VSL assignment is for R5 is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – PRC-002-2, R4~~5~~	
Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Non CIP
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Non CIP

VRF and VSL Justifications – PRC-002-2, R~~6~~5	
Proposed VRF	**Lower**
NERC VRF Discussion	R5~~6~~ is a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state of capability of the BES, or the ability to effectively monitor, control, or restore the BES.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** R~~6~~5 establishes the list of Dynamic Disturbance Recordings that is consistent with FERC guideline G1, Recommendation 12 of the Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has parts that are of equal importance; only one VRF was assigned so there is no conflict.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This requirement calls for identifying BES Elements for Dynamic Disturbance Recording. The team could not identify other continent-wide reliability standards of the same nature.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to identify BES Elements for Dynamic Disturbance Recording could not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R5~~6~~ contains only one objective which identifies BES Elements within specified criteria and to review the list every 5 calendar years. Since the requirement has only one objective, only one VRF was assigned.
Proposed Lower VSL	The Responsible Entity accurately identified the Elements for DDR as directed by Requirement R5 for more than 80% but less than 100% of the required Elements. OR

VRF and VSL Justifications – PRC-002-2, R~~6~~5	
	The Responsible Entity assessed the Elements for DDR as directed by Requirement R5 but was late by 30 calendar days or less. OR The Responsible Entity as directed by Requirement R5 was late in notifying the owners by 10 calendar days or less. ~~The Responsible Entity accurately identified the Elements for DDR as directed by Requirement R6, Part 6.1 for more than 80% but less than 100% of the required Elements.~~ ~~OR~~ ~~The Responsible Entity assessed the Elements for DDR as directed by Requirement R6, Part 6.2 but was late by 30 calendar days or less.~~
Proposed Moderate VSL	The Responsible Entity accurately identified the Elements for DDR as directed by Requirement R5 for more than 70% but less than or equal to 80% of the required Elements. OR The Responsible Entity assessed the Elements for DDR as directed by Requirement R5 but was late by greater than 30 calendar days and less than or equal to 60 calendar days. OR The Responsible Entity as directed by Requirement R5 was late in notifying the owners by greater than 10 calendar days but less than or equal to 20 calendar days.~~The Responsible Entity accurately identified the Elements for DDR as directed by Requirement R6, Part 6.1 for more than 70% but less than or equal to 80% of the required Elements.~~ ~~OR~~ ~~The Responsible Entity assessed the Elements for DDR as directed by Requirement R6, Part 6.2 but was late by greater than 30 calendar days and less than or equal to 60 calendar days.~~
Proposed High VSL	The Responsible Entity accurately identified the Elements for DDR as directed by Requirement R5 for more than 60% but less than or equal to 70% of the required Elements. OR

VRF and VSL Justifications – PRC-002-2, R~~6~~5	
	The Responsible Entity assessed the Elements for DDR as directed by Requirement R5 but was late by greater than 60 calendar days and less than or equal to 90 calendar days. OR The Responsible Entity as directed by Requirement R5 was late in notifying the owners by greater than 20 calendar days but less than or equal to 30 calendar days.~~The Responsible Entity accurately identified the Elements for DDR as directed by Requirement R6, Part 6.1 for more than 60% but less than or equal to 70% of the required Elements.~~ ~~OR~~ ~~The Responsible Entity assessed the Elements for DDR as directed by Requirement R6, Part 6.2 but was late by greater than 60 calendar days and less than or equal to 90 calendar days.~~
Proposed Severe VSL	The Responsible Entity accurately identified the Elements for DDR as directed by Requirement R5 for less than or equal to 60% of the required Elements. OR The Responsible Entity assessed the Elements for DDR as directed by Requirement R5 but was late by greater than 90 calendar days. OR The Responsible Entity as directed by Requirement R5 was late in notifying one or more owners by greater than 30 calendar days.~~The Responsible Entity accurately identified the Elements for DDR as directed by Requirement R6, Part 6.1 for less than or equal to 60% of the required Elements.~~ ~~OR~~ ~~The Responsible Entity assessed the Elements for DDR as directed by Requirement R6, Part 6.2 but was late by greater than 90 calendar days.~~
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended	PRC-002-2 differs from PRC-002-1 (not enforceable) and PRC-018-1 (enforceable and will be retired upon approval of PRC-002-2) in that PRC-002-2 deals with Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording in order to adequately capture

VRF and VSL Justifications – PRC-002-2, R~~6~~5	
Consequence of Lowering the Current Level of Compliance	data for events analysis; and not equipment as referenced in the PRC-002-1 and PRC-018-1. Therefore, the VSL's cannot be compared between PRC-002-2 and PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R5~~6~~ is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer	Non CIP

VRF and VSL Justifications – PRC-002-2, R~~6~~5	
network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Non CIP

~~VRF and VSL Justifications – PRC-002-2, R7~~	
~~**Proposed VRF**~~	~~**Lower**~~
~~NERC VRF Discussion~~	~~R7 is a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state of capability of the BES, or the ability to effectively monitor, control, or restore the BES.~~
~~FERC VRF G1 Discussion~~	~~**Guideline 1- Consistency w/ Blackout Report**~~ ~~R7 requires the Responsible Entity to notify the owners to provide Dynamic Disturbance Recordings for Elements selected in R6. This is consistent with FERC guideline G1, Recommendation 12 of the Blackout Report.~~
~~FERC VRF G2 Discussion~~	~~**Guideline 2- Consistency within a Reliability Standard**~~ ~~This requirement does not have parts.~~
~~FERC VRF G3 Discussion~~	~~**Guideline 3- Consistency among Reliability Standards**~~ ~~This requirement calls for the Responsible Entity to notify the owners of the Elements for Dynamic Disturbance Recording selected in R6.~~ ~~The team could not identify other continent-wide reliability standards~~

VRF and VSL Justifications – PRC-002-2, R7	
	of the same nature.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to notify the owners of the Elements selected for Dynamic Disturbance Recording in R6 could not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R7 contains only one objective which is to notify the owners of BES Elements selected for Dynamic Disturbance Recording selected in R6.
Proposed Lower VSL	The Responsible Entity as directed by Requirement R7 was late in notifying the owners by 10 calendar days or less.
Proposed Moderate VSL	The Responsible Entity as directed by Requirement R7 was late in notifying the owners by greater than 10 calendar days but less than or equal to 20 calendar days.
Proposed High VSL	The Responsible Entity as directed by Requirement R7 was late in notifying the owners by greater than 20 calendar days but less than or equal to 30 calendar days.
Proposed Severe VSL	The Responsible Entity as directed by Requirement R7 was late in notifying one or more owners by greater than 30 calendar days.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	PRC-002-2 differs from PRC-002-1 (not enforceable) and PRC-018-1 (enforceable and will be retired upon approval of PRC-002-2) in that PRC-002-2 deals with Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording in order to adequately capture data for events analysis; and not equipment as referenced in the PRC-002-1 and PRC-018-1. Therefore, the VSL's cannot be compared between PRC-002-2 and PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level	Guideline 2a: The VSL assignment is for R7 is not binary.

VRF and VSL Justifications — PRC-002-2, R7	
Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Non CIP
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	Non CIP

~~VRF and VSL Justifications – PRC-002-2, R7~~	
~~documentation and implementation should account for their interdependence~~	

VRF and VSL Justifications – PRC-002-2, R~~6~~8	
Proposed VRF	**Lower**
NERC VRF Discussion	R~~6~~8 is a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state of capability of the BES, or the ability to effectively monitor, control, or restore the BES.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** R~~6~~8 provides criteria for Dynamic Disturbance Recordings which falls under Recommendation 12 of the Blackout Report and is consistent with FERC guideline G1.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has parts that are of equal importance; only one VRF was assigned so there is no conflict.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This requirement establishes criteria for Dynamic Disturbance Recording selected in R~~5~~6. The team could not identify other continent-wide reliability standards of the same nature.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to establish criteria for Dynamic Disturbance Recording could not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar

VRF and VSL Justifications – PRC-002-2, R6~~8~~	
	requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R6 contains only one objective which is to establish criteria for Dynamic Disturbance Recording. Since the requirement has only one objective, only one VRF was assigned.
Proposed Lower VSL	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 that covered more than 75% but less than 100% of the total required electrical quantities for all applicable BES Elements.~~The Transmission Owner implemented DDR as directed by Requirement R8, Parts 8.1 and 8.4 that covers more than 75% but less than 100% of the total required electrical quantities for all applicable BES Elements.~~
Proposed Moderate VSL	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 for more than 50% but less than or equal to 75% of the total required electrical quantities for all applicable BES Elements.~~The Transmission Owner implemented DDR as directed by Requirement R8, Parts 8.1 through 8.4 for more than 50% but less than or equal to 75% of the total required electrical quantities for all applicable BES Elements.~~
Proposed High VSL	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 for more than 0% but less than or equal to 50% of the total required electrical quantities for all applicable BES Elements.~~The Transmission Owner implemented DDR as directed by Requirement R8, Parts 8.1 through 8.4 for more than 0% but less than or equal to 50% of the total required electrical quantities for all applicable BES Elements.~~
Proposed Severe VSL	The Transmission Owner failed to have DDR data as directed by Requirement R6, Parts 6.1 through 6.4.~~The Transmission Owner failed to implement DDR as directed by Parts 8.1 through 8.4.~~
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering	PRC-002-2 differs from PRC-002-1 (not enforceable) and PRC-018-1 (enforceable and will be retired upon approval of PRC-002-2) in that PRC-002-2 deals with Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording in order to adequately capture data for events analysis; and not equipment as referenced in the PRC-002-1 and PRC-018-1. Therefore, the VSL's cannot be compared

VRF and VSL Justifications – PRC-002-2, R6~~8~~	
the Current Level of Compliance	between PRC-002-2 and PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R8 is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic,	Non CIP

VRF and VSL Justifications – PRC-002-2, R6~~8~~	
should apply binary VSLs	
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Non CIP

VRF and VSL Justifications – PRC-002-2, R7~~9~~	
Proposed VRF	**Lower**
NERC VRF Discussion	R7~~9~~ is a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state of capability of the BES, or the ability to effectively monitor, control, or restore the BES.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** R7~~9~~ provides criteria for Dynamic Disturbance Recordings which falls under Recommendation 12 of the Blackout Report and is consistent with FERC guideline G1.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has parts that are of equal importance; only one VRF was assigned so there is no conflict.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This requirement establishes criteria for Dynamic Disturbance Recording selected in R6. The team could not identify other continent-wide reliability standards of the same nature.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to establish criteria for Dynamic Disturbance Recording could

VRF and VSL Justifications – PRC-002-2, R7~~9~~	
	not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R7~~9~~ contains only one objective which is to establish criteria for Dynamic Disturbance Recording. Since the requirement has only one objective, only one VRF was assigned.
Proposed Lower VSL	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 that covers more than 75% but less than 100% of the total required electrical quantities for all applicable BES Elements.~~The Generator Owner implemented DDR as directed by Requirement R9, Parts 9.1 through 9.4 that covers more than 75% but less than 100% of the total required electrical quantities for all applicable BES Elements.~~
Proposed Moderate VSL	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 for more than 50% but less than or equal to 75% of the total required electrical quantities for all applicable BES Elements.~~The Generator Owner implemented DDR as directed by Requirement R9, Parts 9.1 through 9.4 for more than 50% but less than or equal to 75% of the total required electrical quantities for all applicable BES Elements.~~
Proposed High VSL	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 for more than 0% but less than or equal to 50% of the total required electrical quantities for all applicable BES Elements.~~The Generator Owner implemented DDR as directed by Requirement R9, Parts 9.1 through 9.4 for more than 0% but less than or equal to 50% of the total required electrical quantities for all applicable BES Elements.~~
Proposed Severe VSL	The Generator Owner failed to have DDR data as directed by Requirement R7, Parts 7.1 through 7.4.~~The Generator Owner failed to implement DDR as directed by Requirement R9, Parts 9.1 through 9.4.~~

VRF and VSL Justifications – PRC-002-2, R7~~9~~	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	PRC-002-2 differs from PRC-002-1 (not enforceable) and PRC-018-1 (enforceable and will be retired upon approval of PRC-002-2) in that PRC-002-2 deals with Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording in order to adequately capture data for events analysis; and not equipment as referenced in the PRC-002-1 and PRC-018-1. Therefore, the VSL's cannot be compared between PRC-002-2 and PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R7~~9~~ is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.

VRF and VSL Justifications – PRC-002-2, R7~~9~~	
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Non CIP
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Non CIP

VRF and VSL Justifications – PRC-002-2, R8~~10~~	
Proposed VRF	**Lower**
NERC VRF Discussion	R8~~10~~ is a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state of capability of the BES, or the ability to effectively monitor, control, or restore the BES.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** R8~~10~~ provides criteria for Dynamic Disturbance Recordings which falls under Recommendation 12 of the Blackout Report and is consistent with FERC guideline G1.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has parts that are of equal importance; only one VRF was assigned so there is no conflict.

VRF and VSL Justifications – PRC-002-2, R8~~10~~	
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This requirement establishes the need for continuous data recording and storage for Dynamic Disturbance Recordings established in R6. The team could not identify other continent-wide reliability standards of the same nature.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to establish continuous data recording and storage for Dynamic Disturbance Recordings established in R5~~6~~ could not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R8~~10~~ contains only one objective to establish continuous data recording and storage for Dynamic Disturbance Recordings established in R6. Since the requirement has only one objective, only one VRF was assigned.
Proposed Lower VSL	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed in Requirement R8, for more than 75% but less than 100% of the Elements they own as determined in Requirement R5.~~The Transmission Owner or Generator Owner implemented continuous or non-continuous DDR, as directed in Requirement R10, for more than 75% but less than 100% of the Elements they own as determined in Requirement R6.~~
Proposed Moderate VSL	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed in Requirement R8, for more than 50% but less than or equal to 75% of the Elements they own as determined in Requirement R5.~~The Transmission Owner or Generator Owner implemented continuous or non-continuous DDR, as directed in Requirement R10, for more than 50% but less than or equal to 75% of the Elements they own as determined in Requirement R6.~~
Proposed High VSL	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed in Requirement R8, for more than 0% but less than or equal to 50% of the Elements they own as

VRF and VSL Justifications – PRC-002-2, R8~~10~~	
	determined in Requirement R5.~~The Transmission Owner or Generator Owner implemented continuous or non-continuous DDR, as directed in Requirement R10, for more than 0% but less than or equal to 50% of the Elements they own as determined in Requirement R6.~~
Proposed Severe VSL	The Transmission Owner or Generator Owner failed to have continuous or non-continuous DDR data, as directed in Requirement R8, for the Elements they own as determined in Requirement R5.~~The Transmission Owner or Generator Owner failed to implement continuous or non-continuous DDR, as directed in Requirement R10, for the Elements they own as determined in Requirement R6.~~
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	PRC-002-2 differs from PRC-002-1 (not enforceable) and PRC-018-1 (enforceable and will be retired upon approval of PRC-002-2) in that PRC-002-2 deals with Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording in order to adequately capture data for events analysis; and not equipment as referenced in the PRC-002-1 and PRC-018-1. Therefore, the VSL's cannot be compared between PRC-002-2 and PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R8~~10~~ is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the

VRF and VSL Justifications – PRC-002-2, R8~~10~~	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Non CIP
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Non CIP

VRF and VSL Justifications – PRC-002-2, R9~~11~~	
Proposed VRF	**Lower**
NERC VRF Discussion	R9~~11~~ is a requirement in a long-term planning time frame that, if

VRF and VSL Justifications – PRC-002-2, R9~~11~~	
	violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state of capability of the BES, or the ability to effectively monitor, control, or restore the BES.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** R9~~11~~ provides criteria for Dynamic Disturbance Recordings which falls under Recommendation 12 of the Blackout Report and is consistent with FERC guideline G1.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has parts that are of equal importance; only one VRF was assigned so there is no conflict.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This requirement established technical specifications for Dynamic Disturbance Recording selected in R6. The team could not identify other continent-wide reliability standards of the same nature.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to establish technical specifications for Dynamic Disturbance Recording selected in R6 could not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R9~~11~~ contains only one objective which is to establish technical specifications for Dynamic Disturbance Recording selected in R6. Since the requirement has only one objective, only one VRF was assigned.
Proposed Lower VSL	The Transmission Owner or Generator Owner had DDR data that meets more than 75% but less than 100% of the total recording properties as specified in Requirement R9.~~The Transmission Owner or Generator Owner implemented Dynamic Disturbance Recording that meets more than 75% but less than 100% of the total recording properties as specified in Requirement R11.~~
Proposed Moderate VSL	The Transmission Owner or Generator Owner had DDR data that meets more than 50% but less than or equal to 75% of the total recording

VRF and VSL Justifications – PRC-002-2, R9~~11~~	
	properties as specified in Requirement R9.~~The Transmission Owner or Generator Owner implemented Dynamic Disturbance Recording that meets more than 50% but less than or equal to 75% of the total recording properties as specified in Requirement R11.~~
Proposed High VSL	The Transmission Owner or Generator Owner had DDR data that meets more than 10% but less than or equal to 50% of the total recording properties as specified in Requirement R9.~~The Transmission Owner or Generator Owner implemented Dynamic Disturbance Recording that meets more than 10% but less than or equal to 50% of the total recording properties as specified in Requirement R11.~~
Proposed Severe VSL	The Transmission Owner or Generator Owner had DDR data that meets more than 1% but less than or equal to 10% of the total recording properties as specified in Requirement R9.~~The Transmission Owner or Generator Owner implemented Dynamic Disturbance Recording that meets more than 1% but less than or equal to 10% of the total recording properties as specified in Requirement R11.~~
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	PRC-002-2 differs from PRC-002-1 (not enforceable) and PRC-018-1 (enforceable and will be retired upon approval of PRC-002-2) in that PRC-002-2 deals with Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording in order to adequately capture data for events analysis; and not equipment as referenced in the PRC-002-1 and PRC-018-1. Therefore, the VSL's cannot be compared between PRC-002-2 and PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is	Guideline 2a: The VSL assignment is for R9~~11~~ is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – PRC-002-2, R9~~11~~	
Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	**Guideline 3- Consistency among Reliability Standards** This requirement established technical specifications for Dynamic Disturbance Recording selected in R5. The team could not identify other continent-wide reliability standards of the same nature.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Non CIP
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Non CIP

VRF and VSL Justifications – PRC-002-2, R10~~12~~	
Proposed VRF	**Lower**
NERC VRF Discussion	R10~~2~~ is a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state of capability of the BES, or the ability to effectively monitor, control, or restore the BES.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** R10~~2~~ requires time synchronization of Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording data which falls under Recommendation 12 of the Blackout Report and is consistent with FERC guideline G1.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** This requirement does not have parts.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This requirement calls for time synchronization for Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording data for locations established in R1 and R5~~6~~. The team could not identify other continent-wide reliability standards of the same nature.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failures to time synchronize Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording data could not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R10~~2~~ contains only one objective which is to time synchronize Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording data. Since the requirement has only one objective, only one VRF was assigned.
Proposed Lower VSL	The Transmission Owner or Generator Owner had time synchronization for SER, FR, and DDR data for more than 90% but less than 100% of the bus locations as per Requirements R1 and

VRF and VSL Justifications – PRC-002-2, R10~~12~~	
	Elements as per Requirement R5 as directed by Requirement R10. ~~The Transmission Owner or Generator Owner implemented time synchronization for Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording for more than 90% but less than 100% of the bus locations established in Requirements R1 and Elements established in Requirement R6 as directed by Requirement R12.~~
Proposed Moderate VSL	The Transmission Owner or Generator Owner had time synchronization for SER, FR, and DDR data for more than 80% but less than or equal to 90% of the bus locations as per Requirements R1 and Elements as per Requirement R5 as directed by Requirement R10. ~~The Transmission Owner or Generator Owner implemented time synchronization for Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording for more than 80% but less than or equal to 90% of the bus locations established in Requirements R1 and Elements established in Requirement R6 as directed by Requirement R12.~~
Proposed High VSL	The Transmission Owner or Generator Owner had time synchronization for SER, FR, and DDR data for more than 70% but less than or equal to 80% of the bus locations as per Requirements R1 and Elements as per Requirement R5 as directed by Requirement R10. ~~The Transmission Owner or Generator Owner implemented time synchronization for Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording for more than 70% but less than or equal to 80% of the bus locations established in Requirements R1 and Elements established in Requirement R6 as directed by Requirement R12.~~
Proposed Severe VSL	The Transmission Owner or Generator Owner failed to have time synchronization for SER, FR, and DDR data for less than or equal to 70% of the bus locations as per Requirements R1 and Elements as per Requirement R5 as directed by Requirement R10. ~~The Transmission Owner or Generator Owner failed to implement time synchronization for Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording for less than 70% of the bus locations established in Requirements R1 and Elements established in~~

VRF and VSL Justifications – PRC-002-2, R10~~12~~	
	~~Requirement R6 as directed by Requirement R12.~~
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL's provide a broader compliance range than the associated VSL's in PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R10~~2~~ is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.

VRF and VSL Justifications – PRC-002-2, R10~~12~~	
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Non CIP
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Non CIP

VRF and VSL Justifications – PRC-002-2, R1~~3~~	
Proposed VRF	**Lower**
NERC VRF Discussion	R1~~3~~ is administrative in nature and a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state of capability of the BES, or the ability to effectively monitor, control, or restore the BES.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** R1~~3~~ provides criteria around timelines for providing the data and the data format. This is consistent with FERC guideline G1.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has parts that are of equal importance; only one VRF was assigned so there is no conflict.

VRF and VSL Justifications – PRC-002-2, R1~~3~~	
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This requirement sets the criteria on providing Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording data for locations selected in R1 and Elements established in R5~~6~~.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to provide Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording data for locations selected in R1 and Elements established in R5~~6~~ could not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1~~3~~ contains only one objective which is to provide Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording data within the specified criteria. Since the requirement has only one objective, only one VRF was assigned.
Proposed Lower VSL	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 provided the requested data more than 30 calendar days but less than 40 calendar days from the request. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Part 113.2 provided more than 90% but less than 100% of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided more than 90% but less than 100% in the proper data format. ~~The Transmission Owner or Generator Owner as directed by Requirement R13, Part 13.1 provided the requested data more than 30 calendar days but less than 40 calendar days from the request.~~ ~~OR~~ ~~The Transmission Owner or Generator Owner as directed by Requirement R13, Part 13.2 provided more than 90% but less than~~

VRF and VSL Justifications – PRC-002-2, R1~~3~~	
	~~100% of the requested data.~~ ~~OR~~ ~~The Transmission Owner or Generator Owner as directed by Requirement R13, Parts 13.3 through 13.5 provided more than 90% but less than 100% in the proper data format.~~
Proposed Moderate VSL	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 provided the requested data more than 40 calendar days but less than or equal to 50 calendar days from the request. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.2 provided more than 80% but less than or equal to 90% of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided more than 80% but less than or equal to 90% in the proper data format. ~~The Transmission Owner or Generator Owner as directed by Requirement R13, Part 13.1 provided the requested data more than 40 calendar days but less than or equal to 50 calendar days from the request.~~ ~~OR~~ ~~The Transmission Owner or Generator Owner as directed by Requirement R13, Part 13.2 provided more than 80% but less than or equal to 90% of the requested data.~~ ~~OR~~ ~~The Transmission Owner or Generator Owner as directed by Requirement R13, Parts 13.3 through 13.5 provided more than 80% but less than or equal to 90% in the proper data format.~~
Proposed High VSL	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 provided the requested data more than 50 calendar days but less than or equal to 60 calendar days from the request. OR

VRF and VSL Justifications – PRC-002-2, R1~~3~~	
	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.2 provided more than 70% but less than or equal to 80% of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided more than 70% but less than or equal to 80% in the proper data format. ~~The Transmission Owner or Generator Owner as directed by Requirement R13, Part 13.1 provided the requested data more than 50 calendar days but less than or equal to 60 calendar days from the request.~~ ~~OR~~ ~~The Transmission Owner or Generator Owner as directed by Requirement R13, Part 13.2 provided more than 70% but less than or equal to 80% of the requested data.~~ ~~OR~~ ~~The Transmission Owner or Generator Owner as directed by Requirement R13, Parts 13.3 through 13.5 provided more than 70% but less than or equal to 80% in the proper data format.~~
Proposed Severe VSL	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 failed to provide the requested data more than 60 calendar days from the request. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.2 failed to provide less than or equal to 70% of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided less than or equal to 70% in the proper data format.~~The Transmission Owner or Generator Owner as directed by Requirement R13, Part 13.1 failed to provide the requested data more than 60 calendar days from the request.~~

VRF and VSL Justifications – PRC-002-2, R1~~3~~	
	~~OR~~ ~~The Transmission Owner or Generator Owner as directed by Requirement R13, Part 13.2 failed to provide less than or equal to 70% of the requested data.~~ ~~OR~~ ~~The Transmission Owner or Generator Owner as directed by Requirement R13, Parts 13.3 through 13.5 provided less than or equal to 70% in the proper data format.~~
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL's provide a broader compliance range than the associated VSL's in PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1~~3~~ is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VRF and VSL Justifications – PRC-002-2, R1~~3~~	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Non CIP
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Non CIP

VRF and VSL Justifications – PRC-002-2, R1~~2~~4	
Proposed VRF	**Lower**
NERC VRF Discussion	R1~~2~~4 is a requirement in a long-term planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state of capability of the BES, or the ability to

VRF and VSL Justifications – PRC-002-2, R1~~2~~4	
	effectively monitor, control, or restore the BES.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** R1~~2~~4 provides criteria around the availability of Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording data.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** This requirement does not have parts.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This requirement sets the criteria around the availability of Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording data.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** Failure to follow the criteria around the availability of Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording data could not directly affect the electrical state or capability of the BES, or the ability to effectively monitor and control the BES. Violation of the requirement will not lead to bulk electric system instability, separation, or cascading failures. The VRF for this requirement is "Lower" which is consistent with NERC guidelines for similar requirements.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1~~2~~4 contains only one objective which is to establish criteria around the availability of Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording data. Since the requirement has only one objective, only one VRF was assigned.
Proposed Lower VSL	The Transmission Owner or Generator Owner as directed by Requirement R12 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 90 calendar days but less than 100 calendar days after discovery of the failure. ~~The Transmission Owner or Generator Owner as directed by Requirement R14 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 90 calendar days but less than 100 calendar days after discovery of the failure.~~
Proposed Moderate VSL	The Transmission Owner or Generator Owner as directed by Requirement R12 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 100 calendar days but less than or equal to 110 calendar days after discovery of the failure. ~~The~~

VRF and VSL Justifications – PRC-002-2, R124	
	~~Transmission Owner or Generator Owner as directed by Requirement R14 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 100 calendar days but less than or equal to 110 calendar days after discovery of the failure.~~
Proposed High VSL	The Transmission Owner or Generator Owner as directed by Requirement R12 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 110 calendar days but less than or equal to 120 calendar days after discovery of the failure. ~~The Transmission Owner or Generator Owner as directed by Requirement R14 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 110 calendar days but less than or equal to 120 calendar days after discovery of the failure.~~
Proposed Severe VSL	The Transmission Owner or Generator Owner as directed by Requirement R12 failed to report a failure and provide a Corrective Action Plan to the Regional Entity more than 120 calendar days after discovery of the failure. ~~The Transmission Owner or Generator Owner as directed by Requirement R14 failed to report a failure and provide a Corrective Action Plan to the Regional Entity more than 120 calendar days after discovery of the failure.~~
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	PRC-002-2 differs from PRC-002-1 (not enforceable) and PRC-018-1 (enforceable and will be retired upon approval of PRC-002-2) in that PRC-002-2 deals with Sequence of Events Recording, Fault Recording, and Dynamic Disturbance Recording in order to adequately capture data for events analysis; and not equipment as referenced in the PRC-002-1 and PRC-018-1. Therefore, the VSL's cannot be compared between PRC-002-2 and PRC-018-1. The VSL's for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level	Guideline 2a: The VSL assignment is for R124 is not binary. Guideline 2b: The propose VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – PRC-002-2, R1~~2~~4	
Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Non CIP
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Non CIP

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. Nominations for the SAR Drafting Team members were solicited February 26 – March 9, 2007.
2. The SAR was posted for a 30-day comment period March 22 – April 20, 2007.
3. Nominations for the Disturbance Monitoring Standard Drafting Team (~~SDT~~DMSDT) for Project 2007-11 Disturbance Monitoring were solicited June 12 – 25, 2007.
4. The project was placed into informal development the fall of 2010.
5. The project was placed into formal development January 2013.
6. Nominations for two additional ~~SDT~~DMSDT members were solicited April 12 – 25, 2013.
7. Three additional ~~SDT~~DMSDT members were added May 22, 2013.
8. Industry webinar was held May 22, 2013.
9. Industry technical conferences were held July 30 - 31, 2013 and August 6 - 7, 2013.
10. The draft standard was posted for a 45-day concurrent comment and ballot period November 1 – December 16, 2013.

Description of Current Draft

This is the second draft of the proposed standard and is being posted for stakeholder comments and additional ballot. This draft includes the modifications based on comments submitted by stakeholders

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with a 10-day Ballot	May 2014
Final Ballot	July 2014
BOT Adoption	August 2014

Effective Dates

The standard shall become effective on the first day of the first calendar quarter six (6) months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter six (6) months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

~~See PRC-002-2~~

Implementation Plan.

Implementation Plan for PRC-002-2 Requirements R1 and R5:

Entities shall be 100% compliant on the first day of the first calendar quarter six (6) months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is six (6) months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Implementation Plan for PRC-002-2 Requirement R12:

Entities shall be 100% compliant on the first day of the first calendar quarter nine (9) months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is nine (9) months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Implementation Plan for PRC-002-2 Requirements R2, R3, R4, R6, R7, R8, R9, R10, R11:

Entities shall be at least 50% compliant within four (4) years of the Effective Date of PRC-002-2 and fully compliant within six (6) years of the Effective Date.

Entities that own only one (1) identified BES bus location, Element, or generating unit shall be fully compliant within six (6) years of the Effective Date.

- **Note**: Entities that own only one (1) identified BES bus, BES Element, or generating unit and are notified by an entity shall be 100% compliant within four (4) years following notification.

Entities shall be 100% compliant with a reassessed list from Requirement R1or R5 within three (3) years following notification of the list.

Version History

Version	Date	Action	Change Tracking
2.0	TBD	Effective Date	New

DRAFT

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the NERC Glossary of Terms (Glossary) used in Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

DRAFT

When this standard has received ballot approval, the ~~text boxes~~Rationale Boxes will be moved to the ~~Application~~ Guidelines and technical Basis Section of the Standard.

A. Introduction

1. Title: Disturbance Monitoring and Reporting Requirements

2. Number: PRC-002-2

3. Purpose: To have adequate data available to facilitate event analysis of Bulk Electric System (BES) disturbances.

~~3.~~4. Applicability:

Functional Entities:

4.1 The Responsible Entity is:

~~3.1.1~~4.1.1 Eastern Interconnection – Planning Coordinator

4.1.2 ~~–~~ERCOT – Planning Coordinator or Reliability Coordinator

4.1.3 Western Interconnection – Reliability Coordinator

4.2 Transmission Owner

4.3 Generator Owner

Rationale for Functional Entities:

The Responsible Entity – the Planning Coordinator or Reliability Coordinator, as applicable in each Interconnection – has the best wide-area view of the BES and is most suited to be responsible for determining the Elements for which dynamic disturbance recording (DDR) data is required. The Transmission Owners and Generator Owners will have the responsibility for ensuring that adequate data is available for those Elements selected.

BES buses where sequence of events recording (SER) and fault recording (FR) data is required are best selected by Transmission Owners because they have the required tools, information, and working knowledge of their systems to determine these buses. The Transmission Owners and Generator Owners that own BES Elements on those BES buses will have the responsibility for ensuring that adequate data is available.

~~Rationale for Functional Entities:~~

~~The Responsible Entity – the Planning Coordinator or Reliability Coordinator, as applicable in each Interconnection – has the best wide-area view of the BES and is most suited to be responsible for determining the Elements for which Dynamic Disturbance Recorder (DDR) data is required. The Transmission Owners and Generator Owners will have the responsibility for ensuring that adequate data is available for those Elements selected.~~

~~BES Buses where Fault Recorder (FR) and Sequence of Events Recorder (SOER) data is required are best selected by Transmission Owners because they have the required tools, information, and working knowledge of their systems to determine these buses. The Transmission Owners and Generator Owners will have the responsibility for ensuring that adequate data is available.~~

B. Requirements and Measures

R1. Each Transmission Owner shall identify BES buses for which sequence of events ~~recorder~~recording (SER) and fault ~~recorder~~recording (FR) data is required by using the methodology in PRC-002-2, Attachment 1, notify ~~within 90 calendar days~~ other owners~~, if any,~~ of BES Elements connected to those BES buses~~,~~ , if any, within 90 calendar days that those BES Elements may require SER data and/or FR data, and reevaluate the identified BES buses at least once every five calendar years. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

DRAFT

M1. The Transmission Owner has a dated (electronic or ~~hardcopy~~hard copy) list of BES buses for which SER and FR data are required, identified in accordance with Attachment 1, ~~assessed~~and evidence that the bus identification has been reevaluated within the required interval. The Transmission Owner will also have dated (electronic or ~~hardcopy~~hard copy) evidence that it notified other owners in accordance with Requirement R1.

Rationale for R1:

Analysis and reconstruction of BES events requires SER and FR data from key BES buses. Requirement R1 directs a uniform methodology to identify these BES buses. Review of actual BES short circuit data received from the industry in response to the DMSDT's data request (June 5, 2013 through July 5, 2013) illuminated a strong correlation between the available short circuit MVA at a transmission bus and its relative size and importance to the BES based on (i) its voltage level, (ii) the number of transmission lines and other Elements connected to the bus, and (iii) the number and size of generating units connected to the bus. BES buses with a large short circuit MVA level are BES Elements that have a significant effect on system reliability and performance. Conversely, BES buses with very low short circuit MVA levels seldom cause large cascading system events, so SER and FR data from these BES Elements are not as significant. After analyzing and reviewing the collected data submittals from across the continent, the threshold MVA values were chosen to provide sufficient data for event analysis using engineering and operational judgment. Concerns have existed that the defined methodology for bus selection will overly concentrate data to selected BES buses. Repeated testing of the Attachment 1 methodology has demonstrated the proper distribution of SER and FR data collection.

For the purpose of PRC-002-2, there are a minimum number of BES buses for which SER and FR data are required, based on the short circuit level. With these concepts and the objective being sufficient recording coverage for event analysis, the DMSDT developed the procedure in Attachment 1 that utilizes the maximum available calculated three phase short circuit MVA. This methodology ensures comparable and sufficient coverage for SER and FR data regardless of variations in the size and system topology of Transmission Owners across all Interconnections. Additionally, this methodology provides a degree of flexibility for the use of judgment in the selection process to ensure sufficient distribution.

BES buses where SER and FR data are required are best selected by Transmission Owners because they have the required tools, information, and working knowledge of their systems to determine these buses. SER and FR data will include generating resource contributions to an event. DDR data better shows generator response to disturbances.

Each Transmission Owner must reevaluate the list of BES buses every five calendar years to address system changes.

Since there may be multiple owners of equipment that comprise a BES bus, the notification required in R1 is necessary to ensure all owners are notified.

A 90 calendar day notification deadline provides adequate time for the Transmission Owner to make the appropriate determination and notification.

~~Rationale for R1:~~

~~SER and FR data are not required from every location on the BES to conduct adequate analysis of a BES event; SER and FR from key locations on the BES will suffice. Requirement R1 directs a uniform methodology to select these locations.~~

~~Review of actual BES short circuit data received from the industry in response to the DMSDT's June 5, 2013 through July 5, 2013 data request illuminated a strong correlation between the available short circuit MVA at a transmission bus and its relative size and importance to the BES based on (i) its voltage level, (ii) the number of transmission lines and other Elements connected to the bus, and (iii) the number and size of generating units connected to the bus. Buses with a large short circuit MVA level Elements that have a significant effect on system reliability and performance. Conversely, buses with very low short circuit MVA level seldom cause large cascading system events, so FR and SER typically are not as significant. After analyzing and reviewing the collected data submittals from across the continent, the threshold MVA values were chosen to provide sufficient data for event analysis using engineering and operational judgment. Concerns have existed that the defined methodology for bus selection will overly concentrate data to selected locations. Repeated testing of the Attachment 1 methodology has demonstrated the proper distribution of SER and FR data collection.~~

~~For the purpose of PRC-002-2, there are a minimum number of buses for which FR and SER are required based on the short circuit level, With these concepts and the objective being sufficient recording coverage for event analysis, the SDT developed a procedure included in Attachment 1, that utilizes the maximum available calculated three phase short circuit MVA. This methodology ensures comparable and sufficient coverage for FR and SER data regardless of variations in size and system strength of Transmission Owners across all the Interconnections. Additionally, this methodology provides a degree of flexibility for the use of judgment in the selection process.~~

~~BES buses where FR and SER data is required are best selected by Transmission Owners because they have the required tools, information, and working knowledge of their systems to determine these buses. SER and FR data will reflect generating resource contributions to an event. DDR data better shows generator response to disturbances.~~

~~Each Transmission Owner must reevaluate the list of buses every five calendar years to address system changes such. Since there may be multiple owners of equipment that comprise a bus, the notification required in R1 is necessary to ensure all owners are notified.~~

~~To ensure effective and timely post event analysis, it is important to have continuity of SER and FR, with sufficient data from bus locations across the BES. Of the BES bus locations determined in Requirement R1, there may be locations where the Transmission Owner of the bus location does not own all the Elements. This requirement ensures that all necessary BES Elements at a selected bus location have SOER and FR data available by requiring the Transmission Owner of that bus location to notify the other owners of their respective BES Elements that they require SER and FR per this standard. A 90 calendar day notification deadline provides adequate time for the Transmission Owner to make the appropriate determination and notification.~~

R2. Each Transmission Owner and Generator Owner shall have SER data for circuit breaker position (open/close) for each circuit breaker they own connected directly to the BES buses identified ~~per~~in Requirement R1 and associated with the BES Elements at those BES buses identified ~~per~~in Requirement R1. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M2. The Transmission Owner or Generator Owner has evidence (electronic or ~~hardcopy~~hard copy) of SER data for circuit breaker position as specified in Requirement R2. Evidence may include, but is not limited to: (1) documents describing the device interconnections and configurations which can include a single design standard as representative for common installations; or (2) actual data recordings.

Rationale for R2:

The intent is to capture SER data (opening/closing) for the circuit breakers that can interrupt the current flow through each BES Element connected to a BES bus. Change of state of circuit breaker position, time stamped according to Requirement R10 to a common clock, provides the basis for assembling the detailed sequence of events timeline of a power system disturbance. Other status monitoring indications can be used for devices other than circuit breakers.

~~Rationale for R3:~~

~~The intent is to capture SER data (opening/closing) for the circuit breakers that can interrupt the current flow through each BES Element connected to a BES bus. Change of state of circuit breaker position, timestamped, as per Requirement R10 to a common clock, provides the basis for assembling the detailed sequence of events timeline of a power system disturbance.~~

R3. Each Transmission Owner and Generator Owner shall have the following FR data to determine the following electrical quantities ~~at~~for each of the BES Elements they own connected to the BES buses identified ~~per~~in Requirement R1: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

3.1 Phase-to-neutral voltages for each phase of each specified ~~line or~~ BES bus.

3.2 Each phase current and the residual or neutral current for the following BES Elements:

3.2.1~~.~~ Transformers that have a low-side operating voltage of 100kV or above.

3.~~2.~~2.2 Transmission lines.

M3. ~~**M3.**~~ The Transmission Owner or Generator Owner has evidence (electronic or ~~hardcopy~~hard copy) of FR data is sufficient to determine electrical quantities as specified in Requirement R3. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations including a single design standard as a representation for common installations; or (2) actual data recordings or derivations.

~~Rationale for R4:~~

~~The required electrical quantities may either be directly measured or derived if sufficient FR data is captured (e.g. residual or neutral current if the phase currents are directly measured). In order to cover all possible fault types, all phase-to-neutral voltages are required to be determinable for each BES Bus identified in Requirement R1. Phase current and residual current are required to distinguish between phase faults and ground faults. It also facilitates determination of the fault location and cause of relay operation. For transformers (Part 3.2.1), the data may be from either the high side or the low side of the transformer.~~

Rationale for R3:

The required electrical quantities may either be directly measured or derivable if sufficient FR data is captured (e.g. residual or neutral current if the phase currents are directly measured). In order to cover all possible fault types, all phase-to-neutral voltages are required to be determinable for each BES bus identified in Requirement R1. BES bus voltage data is adequate for system disturbance analysis. Phase current and residual current are required to distinguish between phase faults and ground faults. It also facilitates determination of the fault location and cause of relay operation. For transformers (Part 3.2.1), the data may be from either the high-side or the low-side of the transformer.

R4. Each Transmission Owner and Generator Owner shall have FR data as specified in Requirement R3 that meets the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

4.1 A single record or multiple records that include:

- ~~—~~ A pre-trigger record length of at least two cycles and a post-trigger record length of at least 30 cycles for the same trigger point~~.~~, or
- ~~—~~ At least two cycles of the pre-trigger data, the first three cycles of the ~~fault~~post-trigger data, and the final cycle of the fault as seen by the fault recorder.

4.2~~.~~ A minimum recording rate of 16 samples per cycle.

4.3~~.~~ Trigger settings for at least the following:

4.3.1. Neutral (residual) overcurrent.

4.3.2. Phase undervoltage or overcurrent.

M4. The Transmission Owner or Generator Owner has evidence (electronic or hardcopyhard copy) that FR data meets Requirement R5R4. Evidence may include, but is not limited to: (1) device specification (R4, Part 4.2) and configuration (R4, Parts 4.1 and 4.3), or (2) actual data recordings or derivations.

Rationale for R4:

Time-stamped pre- and post-trigger fault data aid in the analysis of power system operations and determination if operation were as designed. System faults generally persist for a short time period, approximately 1 to 50 cycles; thus, a 50 cycle post trigger minimum record length is adequate. Multiple records allow for legacy microprocessor relays which, when time synchronized, are capable of providing adequate fault data but not capable of providing fault data in a single record with 50 contiguous cycles post-trigger.

A minimum recording rate of 16 samples per cycle (960 Hz) is required to get sufficient point-on-wave data for recreating accurate fault conditions.

Rationale for R4:

Time stamped pre- and post-trigger fault data aid in the analysis of power system operations and determination if operations were as designed. System faults generally persist for a short time period, thus, a 30 cycle post-trigger minimum record length is adequate. Multiple records allow for legacy microprocessor relays which, when time synchronized, are capable of providing adequate fault data but not capable of providing fault data in a single record with 30 contiguous cycles post-trigger.

A minimum recording rate of 16 samples per cycle (960 Hz) is required to get sufficient point on wave data for recreating accurate fault conditions.

R5. Each Responsible Entity (Planning Coordinator or Reliability Coordinator, as applicable) shall identify BES Elements for which dynamic disturbance recorderrecording (DDR) data is required, notify within 90 calendar days other owners, if any, of BES Elements connected to those BES buses, if any, within 90 calendar days, that those BES Elements may require DDR data, and reevaluate the identified buses at least once every five calendar years. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

5.1. The BES Elements shall include the following:

5.1.1. Generating resource(s) with:

- **5.1.1.1.** Gross individual nameplate rating greater than or equal to 500 MVA., or
- **5.1.1.2** Gross individual nameplate rating greater than or equal to 300 MVA where the gross plant/facility aggregate nameplate rating is greater than or equal to 1000MVA. 1000 MVA.

5.1.2. Any one BES Element associated with major transmission interfaces, as defined by the Responsible Entity. Selection of major transmission interfaces should consider the following guidelines:

- Stability related interfaces or other significant Flowgates in the NERC Book of Flowgates for the Eastern Interconnection, or
- Transfer Paths in the Western Interconnection Path Rating Catalog, or
- Voltage stability limited transfer paths or load serving area, or
- Interfaces between Balancing Authority Areas, or
- Areas of significant congestion, thermal violation history, or relatively low Available Transfer Capability (ATC)).

5.1.3. Each terminal of a high- voltage direct current (HVDC) circuit with nameplate rating greater than or equal to 300 MVA, on the alternating current (AC) portion of the converter.

5.1.4. One or more BES Elements associated with Interconnection Reliability Operating Limits. (IROLs).

5.1.5. Any one BES Element within a major voltage sensitive area with an in-service undervoltage load shedding (UVLS) program.

5.2. The BES Elements shall include a minimum of:

5.2.1 One BES Element.

5.2.2 One additional BES Element perfor each additional 3,000 MW of its historical peak system Demand.

DRAFT

M5. The Responsible Entity has a dated (electronic or ~~hardcopy~~hard copy) list of BES Elements for DDR data, identified in accordance with Requirement R5, assessed within the required interval, dated evidence (electronic or ~~hardcopy~~hard copy) of notification to each Transmission Owner or Generator Owner of Elements identified in Requirement R5. Evidence may include, but is not limited to: letters, emails, electronic files, or hard copy records demonstrating transmittal of information.

Rationale for R5:

DDR plays a crucial role in wide-area disturbance analysis, and the Responsible Entity needs to ensure that there are sufficient BES Elements identified for DDR data capture. Additionally, DDR is used for capturing the Bulk Electric System transient and post-transient response and for validating the system performance. The requirement for DDR data for identified BES Elements, for the purpose of this standard, is based upon industry experience with wide-area disturbance analysis and the need for adequate data to facilitate event analysis.

From its experience with changes to the Bulk Electric System that would affect DDR, the DMSDT decided that the five calendar year re-assessment of the list is a reasonable interval for this review.

The DDR data is to be captured for a BES Element, and with the exception of HVDC, is obtainable from one terminal of an Element. This pertains to “major transmission interfaces”.

For HVDC (Part 5.1.3), each Transmission Owner is only responsible for DDR data for the Elements that it owns.

Part 5.1.5 is intended to have DDR data for at least one BES Element in a portion of the BES with a voltage response for system events that has required the installation of a UVLS.

It is intended that a Responsible Entity will have DDR data for one BES Element and one additional BES Element for each 3,000 MW of its historical peak system Demand.

Communication of selected Elements is required to ensure that the owners of the respective Elements are aware of their responsibilities under this standard. The Responsible Entity is only required to share the list of required Elements that each Transmission Owner and Generator Owner owns.

DRAFT

~~Rationale for R5:~~

~~DDR plays a crucial role in wide area disturbance analysis, and the Responsible Entity needs to ensure that there are sufficient BES Elements identified for DDR data capture. Additionally, DDR is used for capturing the Bulk Electric System transient and post-transient response and for validating the system performance. The requirement for DDR for identified BES Elements, for the purpose of this standard, is based upon industry experience with wide-area disturbance analysis and the need for adequate data to facilitate event analysis.~~

~~From its experience with changes to the Bulk Electric System that would affect DDR, the SDT decided that the five calendar-year re-assessment of the list is a reasonable interval for this review.~~
~~The DDR data is to be captured for a BES Element, and with the exception of HVDC, is obtainable from one terminal of an Element.~~

~~For HVDC (Part 5.1.3), each Transmission Owner is only responsible for DDR data for the Elements that it owns.~~

~~Sub-Part 5.1.5 is intended to have DDR data for at least one BES Element in a portion of the BES with a voltage response for system events that has required the installation of a UVLS.~~

~~It is intended that a Responsible Entity will have DDR data for one BES Element, and one more BES Element for each 3,000 MW of its historical peak system Demand.~~

~~Communication of selected Elements is required to ensure that the owners of the respective Elements are aware of their responsibilities under this standard. The Responsible Entity is only required to share the list of required Elements that each Transmission Owner and Generator Owner owns.~~

R6. Each Transmission Owner shall have DDR data for each BES Element ~~they own~~it owns for which it received notification as ~~per~~identified in Requirement R5, to determine the following electrical quantities: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

6.1 One phase-to-neutral or positive sequence voltage.

6.2 The phase current for the same phase at the same voltage corresponding to the voltage in Requirement R6, Part 6.1, or the positive sequence current.

6.3 Real Power and Reactive Power flows expressed on a three- phase basis corresponding to all circuits where current measurements are required.

6.4 Frequency of any one of the voltage(s) in Requirement R6, Part 6.1.

M6. The Transmission Owner has evidence (electronic or ~~hardcopy~~hard copy) of DDR data to determine electrical quantities as specified in Requirement R6. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations; or (2) actual data recordings or derivations.

Rationale for R6:

Dynamic disturbance recording is used for measurement of transient response to system disturbances, during a relatively balanced post-fault condition. Therefore, it is sufficient to provide a phase-to-neutral voltage or positive sequence voltage. The electrical quantities can be determined (calculated, derived, etc.).

Because all of the buses within a location are at the same frequency one frequency measurement is adequate.

The data requirements for PRC-002-2 are based on a system configuration assuming all normally closed circuit breakers on a bus are closed.

~~Rationale for R6:~~

~~Dynamic Disturbance Recording is used for measurement of transient response to system disturbances, during a relatively balanced post-fault condition. Therefore, it is sufficient to provide a phase-to-neutral voltage or positive sequence voltage. The electrical quantities can be determined - calculated, derived, etc.~~

~~Because all of the buses within a location are at the same frequencies one frequency measurement is adequate. The data requirements for PRC-002-2 are based on a system configuration assuming all normally-closed circuit breakers on a bus are closed.~~

R7. Each Generator Owner shall have DDR data for each BES Element ~~they own as per~~it owns and is notified according to Requirement R5, to determine the following electrical quantities: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

7.1 One phase-to-neutral, phase-to-phase, or positive sequence voltage at either the generator step- up (GSU) transformer high-side or low-side voltage level.

7.2 The phase current for the same phase at the same voltage in Requirement R7, Part 7.1, phase current(s) for any phase-to-phase voltages, or positive sequence current.

7.3 Real Power and Reactive Power flows expressed on a three- phase basis corresponding to all circuits where current measurements are required.

7.4 Frequency of at least one of the voltages in Requirement R7, Part 7.1.

M7. –The Generator Owner has evidence (electronic or ~~hardcopy~~hard copy) of DDR data to determine electrical quantities as specified in Requirement ~~R9~~R7. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations; or (2) actual data recordings or derivations.

~~Rationale for R7:~~

~~A crucial part of wide-area disturbance analysis is understanding the dynamic response of generating resources. Therefore, it is necessary for Generator Owners to have DDR at either the high- or low-side of the generator step-up (GSU) transformer, measuring the specified electrical quantities, to adequately capture generator response. This standard defines the 'what' of DDR, not the 'how.' GOs may install this capability or, where the TO already has suitable DDR data, contract with the TO. However, the Generator Owner is still responsible for the provision of this data.~~

Rationale for R7:

A crucial part of wide-area disturbance analysis is understanding the dynamic response of generating resources. Therefore, it is necessary for Generator Owners to have DDR at either the high or low-side of the generator step up (GSU) transformer, measuring the specified electrical quantities, to adequately capture generator response. This standard defines the 'what' of DDR, not the 'how.' Generator Owners may install this capability or, where the Transmission Owners already have suitable DDR data, contract with the Transmission Owner. However, the Generator Owner is still responsible for the provision of this data.

R8. Each Transmission Owner and Generator Owner ~~that is~~ responsible for DDR data ~~as per~~in Requirement R5 shall have continuous data recording and storage. If the equipment was installed prior to the effective date of this standard and is not capable of

continuous recording, triggered records must meet the following: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

~~-~~**8.1** Triggered record lengths of at least three minutes.

8.2~~.~~ At least one of the following three triggers:

- Off nominal frequency trigger set at:

	Low	High
o Eastern Interconnection	<59.75 Hz	>61.0 Hz
o Western Interconnection	<59.55 Hz	>61.0 Hz
o ERCOT Interconnection	<59.35 Hz	>61.0 Hz
o Hydro-Quebec Interconnection	<58.55 Hz	>61.5 Hz

- Rate of change of frequency trigger set at:

o Eastern Interconnection	< -0.03125 Hz/sec	> 0.125 Hz/sec
o Western Interconnection	< -0.05625 Hz/sec	> 0.125 Hz/sec
o ERCOT Interconnection	< -0.08125 Hz/sec	> 0.125 Hz/sec
o Hydro-Quebec Interconnection	< -0.18125 Hz/sec	> 0.1875 Hz/sec

- Undervoltage trigger set no lower than 85% of normal operating voltage for a duration of 5 seconds.

~~no lower than 85% of normal operating voltage for a duration of 5 seconds~~

M8. Each Transmission Owner and Generator Owner has dated evidence (electronic or ~~hardcopy~~hard copy) of data recording and storage in accordance with Requirement R8. Evidence may include, but is not limited to: (1) documents describing the device specifications and configurations; or (2) actual data recordings.

Rationale for R8:

Large scale system outages generally are an evolving sequence of events that occur over an extended period of time, making DDR essential for event analysis. Data available pre- and post-contingency helps identify the causes and effects of each event leading to outages. Therefore, continuous recording and storage are necessary to ensure sufficient data is available for the entire event.

Existing DDR data recording across the BES may not record continuously. To accommodate its use for the purposes of this standard, triggered records are acceptable if the equipment was installed prior to the effective date of this standard. The frequency triggers are defined based on the dynamic response associated with each Interconnection. The undervoltage trigger is defined to capture possible delayed undervoltage conditions such as Fault Induced Delayed Voltage Recovery (FIDVR).

~~Rationale for R8:~~

~~Large scale system outages generally are an evolving sequence of events that occur over an extended period of time, making DDR essential for event analysis. Data available pre- and post-contingency helps identify the causes and effects of each event leading to outages. Therefore, continuous recording and storage are necessary to ensure sufficient data are available for the entire Disturbance.~~

~~Existing DDR recording across the BES may not record continuously. To accommodate its use for the purposes of this standard, triggered records are acceptable if the equipment was installed prior to the effective date of this standard. The frequency triggers are defined based on the dynamic response associated with each Interconnection. The undervoltage trigger is defined to capture possible delayed undervoltage conditions such as Fault Induced Delayed Voltage Recovery (FIDVR).~~

R9. Each Transmission Owner and Generator Owner in Requirement R5 shall have DDR data~~, for the Elements as per Requirement R5, which conform~~ that conforms to the following technical specifications: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

9.1 Input sampling rate of at least 960 samples per second.

9.2 Output recording rate of electrical quantities of at least 30 times per second.

M9. The Transmission Owner or Generator Owner has evidence (electronic or ~~hardcopy~~hard copy) that DDR data meets Requirement R9. Evidence may include, but is not limited to: (1) device specification and configuration, or (2) actual data recordings (R9, Part 9.2).

Rationale for R9:

An input sampling rate of at least 960 samples per second, which corresponds to 16 samples per cycle, on the input side of the DDR equipment, ensures adequate accuracy for calculation of recorded measurements such as complex voltage and frequency.

An output recording rate of electrical quantities of at least 30 times per second refers to the recording and measurement calculation rate of the device. Recorded measurements of at least 30 times per second provide adequate recording speed to monitor the low frequency oscillations typically of interest during power system disturbances.

~~Rationale for R9:~~

~~An input sampling rate of at least 960 samples per second, which corresponds to 16 samples per cycle, on the input side of the DDR equipment, ensures adequate accuracy for calculation of recorded measurements such as complex voltage and frequency.~~

~~An output recording rate of electrical quantities of at least 30 times per second refers to the recording and measurement calculation rate of the device. Recorded measurements of at least 30 times per second provide adequate recording speed to monitor low frequency oscillations typically of interest during power system disturbances.~~

R10. Each Transmission Owner and Generator Owner shall time synchronize all SER, FR and DDR data for the BES ~~bus~~ buses identified ~~per~~in Requirement R1 and BES Elements identified ~~per~~in Requirement R5 to within ± 2 milliseconds of Coordinated Universal Time (UTC), time stamped with or without a local time offset. *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M10. The Transmission Owner or Generator Owner has evidence (electronic or ~~hardcopy)~~hard copy) of time synchronization described in Requirement R10. Evidence may include, but is not limited to: (1) device specification and configuration, or (2) actual data recordings, or (3) station drawings.

~~Rationale for R10:~~

~~Time synchronization of disturbance monitoring data allows for the time alignment of large volumes of geographically dispersed data records from diverse recording sources. A universally recognized time standard is necessary to provide the foundation for this alignment. Coordinated Universal Time (UTC) is the foundation used for the time alignment of records. It is an international time standard utilizing atomic clocks for generating precision time measurements at fractions of a second levels. The local time offset, expressed as a negative number, is the difference between UTC and the local time zone where the measurements are recorded.~~

~~Accuracy of ±2 milliseconds for time synchronization is specified in response to Recommendation 12b in the NERC August, 2003, Blackout Final NERC Report Section V Conclusions and Recommendations:~~

~~"Recommendation 12b: Facilities owners shall, in accordance with regional criteria, upgrade existing dynamic recorders to include GPS time synchronization…"~~

~~Also, from the U.S. Canada Power System Outage Task Force Interim Report: Causes of the August 14th Blackout, November 2003, in the United States and Canada, page 103:~~

~~"Establishing a precise and accurate sequence of outage related events was a critical building block for the other parts of the investigation. One of the key problems in developing this sequence was that although much of the data pertinent to an event was time stamped, there was some variance from source to source in how the time stamping was done, and not all of the time stamps were synchronized…"~~

~~From NPCC's SP6 Report Synchronized Event Data Reporting, revised March 31, 2005, the investigation by the authoring working group revealed that existing GPS receivers can be expected to provide a time code output which has an uncertainty on the order of 1 millisecond, uncertainty being a quantitative descriptor.~~

~~The ±2 milliseconds accuracy requirement specified in this standard is realistically achievable with equipment available and proper cabling installation.~~

~~Stored data does not need to be maintained in UTC format. The data provided pursuant to a data request must be provided in UTC format with or without local time offset.~~

Rationale for R10:

Time synchronization of disturbance monitoring data allows for the time alignment of large volumes of geographically dispersed data records from diverse recording sources. A universally recognized time standard is necessary to provide the foundation for this alignment. Coordinated Universal Time (UTC) is the foundation used for the time alignment of records. It is an international time standard utilizing atomic clocks for generating precision time measurements at fractions of a second levels. The local time offset, expressed as a negative number, is the difference between UTC and the local time zone where the measurements are recorded.

Accuracy of ±2 milliseconds for time synchronization is specified in response to Recommendation 12b in the NERC August, 2003, Blackout Final NERC Report Section V Conclusions and Recommendations:

"Recommendation 12b: Facilities owners shall, in accordance with regional criteria, upgrade existing dynamic recorders to include GPS time synchronization…"

Also, from the U.S.-Canada Power System Outage Task Force Interim Report: Causes of the August 14th Blackout, November 2003, in the United States and Canada, page 103:

"Establishing a precise and accurate sequence of outage-related events was a critical building block for the other parts of the investigation. One of the key problems in developing this sequence was that although much of the data pertinent to an event was time-stamped, there was some variance from source to source in how the time-stamping was done, and not all of the time-stamps were synchronized…"

From NPCC's SP6 Report Synchronized Event Data Reporting, revised March 31, 2005, the investigation by the authoring working group revealed that existing GPS receivers can be expected to provide a time code output which has an uncertainty on the order of 1 millisecond, uncertainty being a quantitative descriptor.

The ±2 milliseconds accuracy requirement specified in this standard is realistically achievable with equipment available and proper cabling installation.

Stored data does not need to be maintained in UTC format. The data provided pursuant to a data request must be provided in UTC format with or without local time offset.

R11. Each Transmission Owner and Generator Owner shall provide all SER, FR, and DDR data for the BES ~~bus locations~~buses identified ~~per~~in Requirement R1 and BES Elements identified ~~per~~in Requirement R5 to the Reliability Coordinator, Regional Entity, or NERC as follows: *[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

11.1. The recorded data will be provided within 30 calendar days of a request.

11.2. The recorded data will be retrievable for the period of 10 calendar days preceding a request.

11.3. SER data will be provided in Comma Separated Value (.CSV) format following Attachment 2.

11.4. FR and DDR data will be provided in electronic C37.111, (C37.111-2013 or later) IEEE Standard for Common Format for Transient Data Exchange (COMTRADE), formatted files.

11.5. Data files will be named in conformance with C37.232, IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME).

M11. The Transmission Owner or Generator Owner has evidence (electronic or hardcopyhard copy) data was submitted upon request in accordance with Requirement R11. Evidence may include, but is not limited to: (1) dated transmittals to the requesting entity with formatted records, (2) device specification and configuration, or (3) actual data recordings.

Rationale for R11:

Multiple entities and data recordings may be involved in wide-area disturbance analysis. Standardized file format and naming conventions improves timely analysis.

The DMSDT determined that providing the data within 30 calendar days is reasonable based on normal business operations workload.

For Part 11.2, the DMSDT intends for data to be available for 10 days preceding a request for that data. Requests are usually initiated the same or next day following an event for which data is requested. A 10 calendar day time frame provides a practical limit on the duration of data required to be stored and informs the requesting entities as to how long the data will be available. The requester of data has to be aware of the Part 11.2 10 day retrievability. Realistic overwrite concerns may have to consider the recording capability implemented.

Part 11.4 specifies the IEEE C37.111-2013 COMTRADE format for the FR and DDR data. IEEE C37.111 is the Standard for Common Format for Transient Data Exchange, and it is well established in industry. It is necessary to specify a standard format as it will be incorporated with other submitted data to provide a detailed analysis of a power system disturbance. C37.111-2013 is a version of COMTRADE that includes formatting for phasor data for Disturbance Recording. Prior versions of C37.111 were not compatible with phasor data.

R12. Each Transmission Owner and Generator Owner shall, within 90 calendar days of the discovery of a failure of the recording capability for the SER and, FR data at the BES buses identified per Requirement R1 or DDR data for the BES Elements identified per Requirement R5, shall, restore the recording capability or develop a timeline for restoration and a Corrective Action Plan (CAP), to be submitted) for submission to the Regional Entity, to restore the recording ability which includes a timeline for the restoration.: *[:[Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]*

M12. The Transmission Owner or Generator Owner has dated evidence (electronic or ~~hardcopy~~hard copy) that meets Requirement R12. Evidence may include, but is not limited to: (1) dated reports of discovery of a failure, (2) documentation noting the date the data recording was restored, or (3) dated CAP transmittals to the Regional Entity.

~~Rationale for R12:~~

~~Each Transmission Owner and Generator Owner who owns equipment used for collecting the data required for this standard must repair any failures within 90 calendar days to ensure that adequate data is available for event analysis. Therefore, it is required to return the data recording ability to service within 90 calendar days of a discovery of failure. If the Disturbance Monitoring Equipment (DME) cannot be returned to service within 90 calendar days (e.g. budget cycle, service crews, vendors, etc.), the Entity must report it to the Regional Entity along with a Corrective Action Plan for returning the equipment to service. The timeline required for the CAP depends on the entity and they type of data required. For example, DDR data from a generator may not be restored until the next outage cycle. A CAP is not necessary if the recording capability is restored within 90 day of the discovery of the failure.~~

Rationale for R12:

Each Transmission Owner and Generator Owner who owns equipment used for collecting the data required for this standard must repair any failures within 90 calendar days to ensure that adequate data is available for event analysis. Therefore, it is required to return the data recording capability to service within 90 calendar days of a discovery of failure. If the Disturbance Monitoring Equipment (DME) cannot be returned to service within 90 calendar days (e.g. budget cycle, service crews, vendors, etc.), the Entity must develop a Corrective Action Plan (CAP) for restoring the data recording capability. The timeline required for the CAP depends on the entity and the type of data required. For example, DDR data from a generator may not be restored until the next outage cycle.

~~Rationale for R11:~~

~~Multiple entities and data recordings may be involved in wide area disturbance analysis. Standardized file format and naming conventions improves timely analysis.~~

~~The SDT determined that providing the data within 30 calendar days is reasonable based on normal business operations workload. A 10 calendar day time frame provides a practical limit on the duration of data required to be stored and informs the requesting entities how long the data will be available.~~

~~For Part 11.2, the SDT intends for data to be available for 10 days preceding a request for that data. Requests are usually initiated the same or next day following an event for which data is requested. A 10 calendar day time frame provides a practical limit on the amount of data required to be stored and lets the requesting entities how long the data will be available. The requester of data has to be aware of the Part 11.2 10 day retrievability.~~

~~Realistic overwrite concerns may have to consider the recording capability implemented.~~

~~Part 11.4 specifies the IEEE C37.111-2013 COMTRADE format for the FR and DDR data. IEEE C37.111 is the Standard for Common Format for Transient Data Exchange, and it is well established in the industry. It is necessary to specify a standard format as it will be incorporated with other submitted data to provide a detailed analysis of a power system disturbance. C37.111-2013 is a version of COMTRADE that includes formatting for phasor data for Disturbance Recording. Prior versions of C37.111 were not compatible with phasor data.~~

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

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

The Transmission Owner, Generator Owner, Planning Coordinator, and Reliability Coordinator shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The Transmission Owner shall retain evidence of Requirement R1, Measure M1 for five calendar years.

The Transmission Owner shall retain evidence of Requirement R6, Measure M6 for three calendar years.

The Generator Owner shall retain evidence of Requirement R7, Measure M7 for three calendar years.

The Transmission Owner and Generator Owner shall retain evidence of Requirements R2, R3, R4, R8, R9, R10, R11, and R12, Measures M2, M3, M4, M8, M9, M10, M11, and M12 for three calendar years.

The Responsible Entity (Planning Coordinator or Reliability Coordinator, as applicable) shall retain evidence of Requirement R5, Measure M5 for five calendar years.

If a Transmission Owner, Generator Owner, or Responsible Entity ~~(Planning Coordinator or Reliability Coordinator)~~ is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

DRAFT

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Lower	The Transmission Owner identified the BES buses as directed by Requirement R1 for more than 80% but less than 100% of the required BES buses. OR The Transmission Owner assessed the BES buses as directed by Requirement R1 but was late by 30 calendar days or less. OR The Transmission Owner as directed by Requirement R1 was late in notifying the other owners by 10 calendar days or less.	The Transmission Owner identified the BES buses as directed by Requirement R1 for more than 70% but less than or equal to 80% of the required BES buses. OR The Transmission Owner assessed the BES buses as directed by Requirement R1 but was late by greater than 30 calendar days and less than or equal to 60 calendar days. OR The Transmission Owner as directed by Requirement R1 was late in notifying the other owners by	The Transmission Owner identified the BES buses as directed by Requirement R1 for more than 60% but less than or equal to 70% of the required BES buses. OR The Transmission Owner assessed the BES buses as directed by Requirement R1 but was late by greater than 60 calendar days and less than or equal to 90 calendar days. OR The Transmission Owner as directed by Requirement R1 was late in notifying the other owners by	The Transmission Owner identified the BES buses as directed by Requirement R1for less than or equal to 60% of the required BES buses. OR The Transmission Owner assessed the BES buses as directed by Requirement R1but was late by greater than 90 calendar days. OR The Transmission Owner as directed by Requirement R1 was late in notifying one or more other owners by

DRAFT

				greater than 10 calendar days but less than or equal to 20 calendar days.	greater than 20 calendar days but less than or equal to 30 calendar days.	greater than 30 calendar days.
R2	Long-term Planning	Lower	Each Transmission or Generator Owner as directed by Requirement ~~R3~~R2 had more than 75% but less than 100% of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the ~~bus locations as per~~BES buses identified in Requirement ~~R2~~R1.	Each Transmission or Generator Owner as directed by Requirement ~~R3~~R2 had more than 50% but less than or equal to 75% of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the ~~bus locations as per~~BES buses identified in Requirement ~~R2~~R1.	Each Transmission or Generator Owner as directed by Requirement ~~R3~~R2 had more than 10% but less than or equal to 50% of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the ~~bus locations as per~~BES buses identified in Requirement ~~R2~~R1.	Each Transmission or Generator Owner as directed by Requirement ~~R3~~R2 had from 0% but less than or equal to 10% of the total SER data for circuit breaker position (open/close) for each of the circuit breakers at the ~~bus locations as per~~BES buses identified in Requirement ~~R2~~R1.
R3	Long-term Planning	Lower	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 75% but less than 100% of the total	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 50% but less than or equal to 75% of	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 10% but less than or equal to 50% of	The Transmission Owner or Generator Owner had FR data as directed by Requirement R3, Parts 3.1 and 3.2 that covers more than 0% but less than or equal to 10% of

DRAFT

			set of required electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities ~~per~~for each BES Element.	the total set of required electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities ~~per~~for each BES Element.	the total set of required electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities ~~per~~for each BES Element.	the total set of required electrical quantities, which is the product of the total number of monitored BES Elements and the number of specified electrical quantities ~~per~~for each BES Element.
R4	Long-term Planning	Lower	The Transmission Owner or Generator Owner had- FR data that meets more than 75% but less than 100% of the total recording properties as specified in Requirement R4.	The Transmission Owner or Generator Owner had FR data that meets more than 50% but less than or equal to 75% of the total recording properties as specified in Requirement R4.	The Transmission Owner or Generator Owner had FR data that meets more than 10% but less than or equal to 50% of the total recording properties as specified in Requirement R4.	The Transmission Owner or Generator Owner had FR data that meets more than 0% but less than or equal to 10% of the total recording properties as specified in Requirement R4.
R5	Long-term Planning	Lower	The Responsible Entity accurately identified the BES Elements for DDR as directed by Requirement R5 for more than 80% but less than 100% of the required BES Elements. OR	The Responsible Entity accurately identified the BES Elements for DDR as directed by Requirement R5 for more than 70% but less than or equal to 80% of the required BES Elements. OR	The Responsible Entity accurately identified the BES Elements for DDR as directed by Requirement R5 for more than 60% but less than or equal to 70% of the required BES Elements. OR	The Responsible Entity accurately identified the BES Elements for DDR as directed by Requirement R5 for less than or equal to 60% of the required BES Elements. OR

DRAFT

			The Responsible Entity assessed the BES Elements for DDR as directed by Requirement R5 but was late by 30 calendar days or less. OR The Responsible Entity as directed by Requirement R5 was late in notifying the owners by 10 calendar days or less.	The Responsible Entity assessed the BES Elements for DDR as directed by Requirement R5 but was late by greater than 30 calendar days and less than or equal to 60 calendar days. OR The Responsible Entity as directed by Requirement R5 was late in notifying the owners by greater than 10 calendar days but less than or equal to 20 calendar days.	The Responsible Entity assessed the BES Elements for DDR as directed by Requirement R5 but was late by greater than 60 calendar days and less than or equal to 90 calendar days. OR The Responsible Entity as directed by Requirement R5 was late in notifying the owners by greater than 20 calendar days but less than or equal to 30 calendar days.	The Responsible Entity assessed the BES Elements for DDR as directed by Requirement R5 but was late by greater than 90 calendar days. OR The Responsible Entity as directed by Requirement R5 was late in notifying one or more owners by greater than 30 calendar days.
R6	Long-term Planning	Lower	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 that covered more than 75% but less than 100% of the total required electrical quantities for all	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 for more than 50% but less than or equal to 75% of the total required electrical quantities for	The Transmission Owner had DDR data as directed by Requirement R6, Parts 6.1 through 6.4 for more than 0% but less than or equal to 50% of the total required electrical quantities for	The Transmission Owner failed to ~~had~~have DDR data as directed by Requirement R6, Parts 6.1 through 6.4.

DRAFT

			applicable BES Elements.	all applicable BES Elements.	all applicable BES Elements.	
R7	Long-term Planning	Lower	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 that covers more than 75% but less than 100% of the total required electrical quantities for all applicable BES Elements.	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 for more than 50% but less than or equal to 75% of the total required electrical quantities for all applicable BES Elements.	The Generator Owner had DDR data as directed by Requirement R7, Parts 7.1 through 7.4 for more than 0% but less than or equal to 50% of the total required electrical quantities for all applicable BES Elements.	The Generator Owner failed to have DDR data as directed by Requirement R7, Parts 7.1 through 7.4.
R8	Long-term Planning	Lower	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed in Requirement R8, for more than 75% but less than 100% of the BES Elements they own as determined in Requirement R5.	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed in Requirement R8, for more than 50% but less than or equal to 75% of the BES Elements they own as determined in Requirement R5.	The Transmission Owner or Generator Owner had continuous or non-continuous DDR data, as directed in Requirement R8, for more than 0% but less than or equal to 50% of the BES Elements they own as determined in Requirement R5.	The Transmission Owner or Generator Owner failed to have continuous or non-continuous DDR data, as directed in Requirement R8, for the BES Elements they own as determined in Requirement R5.
R9	Long-term Planning	Lower	The Transmission Owner or Generator Owner had DDR data that meets more than 75% but less than 100% of the total recording properties as	The Transmission Owner or Generator Owner had DDR data that meets more than 50% but less than or equal to 75% of the total recording	The Transmission Owner or Generator Owner had- DDR data that meets more than 10% but less than or equal to 50% of the total recording	The Transmission Owner or Generator Owner had DDR data that meets ~~more than 1% but~~ less than or equal to 10% of the total recording

			specified in Requirement R9.	properties as specified in Requirement R9.	properties as specified in Requirement R9.	properties as specified in Requirement R9.
R10	Long-term Planning	Lower	The Transmission Owner or Generator Owner had time synchronization for SER, FR, and DDR data for more than 90% but less than 100% of the ~~bus locations as per Requirements~~BES buses identified in Requirement R1 and BES Elements ~~as per~~identified in Requirement R5 as directed by Requirement R10.	The Transmission Owner or Generator Owner had time synchronization for SER, FR, and DDR data for more than 80% but less than or equal to 90% of the ~~bus locations as per Requirements~~ BES buses identified in Requirement R1 and BES Elements ~~as per~~identified in Requirement R5 as directed by Requirement R10.	The Transmission Owner or Generator Owner had time synchronization for SER, FR, and DDR data for more than 70% but less than or equal to 80% of the ~~bus locations as per Requirements~~ BES buses identified in Requirement R1 and BES Elements ~~as per~~identified in Requirement R5 as directed by Requirement R10.	The Transmission Owner or Generator Owner failed to have time synchronization for SER, FR, and DDR data for less than or equal to 70% of the ~~bus locations as per Requirements~~ BES buses identified in Requirement R1 and BES Elements ~~as per~~identified in Requirement R5 as directed by Requirement R10.

DRAFT

R11	Long-term Planning	Lower	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 provided the requested data more than 30 calendar days but less than 40 calendar days from the request. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Part ~~11~~3~~11~~.2 provided more than 90% but less than	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 provided the requested data more than 40 calendar days but less than or equal to 50 calendar days from the request. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.2 provided more than 80% but less than	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 provided the requested data more than 50 calendar days but less than or equal to 60 calendar days from the request. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.2 provided more than 70% but less than	The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.1 failed to provide the requested data more than 60 calendar days from the request. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Part 11.2 failed to provide less than or equal to

DRAFT

			100% of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided more than 90% of the data but less than 100% of the data in the proper data format.	or equal to 90% of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided more than 80% of the data but less than or equal to 90% of the data in the proper data format.	or equal to 80% of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided more than 70% of the data but less than or equal to 80% of the data in the proper data format.	70% of the requested data. OR The Transmission Owner or Generator Owner as directed by Requirement R11, Parts 11.3 through 11.5 provided less than or equal to 70% of the data in the proper data format.
R12	Long-term Planning	Lower	The Transmission Owner or Generator Owner as directed by Requirement R12 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 90 calendar days but less than or equal to 100 calendar days after discovery of the failure.	The Transmission Owner or Generator Owner as directed by Requirement R12 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 100 calendar days but less than or equal to 110 calendar days after discovery of the failure.	The Transmission Owner or Generator Owner as directed by Requirement R12 reported a failure and provided a Corrective Action Plan to the Regional Entity more than 110 calendar days but less than or equal to 120 calendar days after discovery of the failure.	The Transmission Owner or Generator Owner as directed by Requirement R12 failed to report a failure and provide a Corrective Action Plan to the Regional Entity more than 120 calendar days after discovery of the failure.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

G. References

IEEE C37.111-2013, Measuring relays and protection equipment Part 24: Common format for transient data exchange (COMTRADE) for power systems. Standard published 04/30/2013 by IEEE.

IEEE C37.232-2011, IEEE Standard for Common Format for Naming Time Sequence Data Files (COMNAME). Standard published 11/09/2011 by IEEE.

NPCC SP6 Report Synchronized Event Data Reporting, revised March 31, 2005

~~NERC~~U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003~~,~~ Blackout ~~Final NERC Report~~in the United States and Canada: Causes and Recommendations (2004).

U.S.-Canada Power System Outage Task Force Interim Report: Causes of the August 14th Blackout~~, November~~ in the United States and Canada (Nov. 2003~~, in the United States and Canada~~)

DRAFT

Attachment 1

Methodology for Selecting Buses for Capturing Sequence of Events ~~Recorder~~Recording (SER) and Fault ~~Recorder~~Recording (FR) Data

~~Locations Selection Methodology~~

(Requirement R1)

To identify monitored BES ~~bus locations~~buses for Sequence of Events ~~Recorder~~Recording (SER) and Fault ~~Recorder~~Recording (FR) data required by Requirement 1 ~~of PRC-002-2~~, each Transmission Owner shall follow sequentially, unless otherwise noted, the steps listed below:

Step 1. Determine a complete list of BES buses that it owns.

For the purposes of this standard, a single BES bus ~~location~~ includes physical buses connected at the same voltage level within the same physical location sharing a common ground grid. These buses may be modeled or represented by a single node in fault studies. For example, ring bus or breaker-and-a-half bus configurations are considered to be a single bus ~~locations~~.

Step 2. Reduce the list to those BES buses that have a maximum available calculated three phase short circuit MVA of 1500 MVA or greater. If there are no buses on the resulting list, proceed to Step 7.

Step 3. Determine the 11 BES buses ~~-~~on the list with the highest maximum available calculated three phase short circuit MVA level. If the list has 11 or fewer ~~bus locations~~buses, proceed to Step 7.

Step 4. Calculate the median MVA level of the 11 BES buses determined in Step 3.

Step 5. Multiply the median MVA level determined in Step 4 by 20%.

Step 6. Reduce the BES buses on the list to only those that have a maximum available calculated three phase short circuit MVA higher than the greater of:

- 1500 MVA or
- 20% of median MVA level determined in Step 5.

Step 7. If there are no BES buses on the list: the procedure is complete and no FR and SER data will be required. Proceed to Step 9.

If the list has 11 or fewer BES buses: FR and SER data is required at the BES buses with the highest maximum available calculated three phase short circuit MVA. Proceed to Step 9.

If the list has more than 11 BES buses: ~~FR~~SER and ~~SER~~FR data is required on at least the 10% of the BES buses, determined in Step 6, with the highest maximum

available calculated three phase short circuit MVA. Proceed to Step 8.

Step 8. ~~FR~~SER and ~~SER~~FR data is required at additional BES buses on the list determined in Step 6. The aggregate of the number of BES buses determined in Step 7 and this Step will be at least 20% of the BES ~~bus~~buses determined in Step 6.

The additional BES buses are selected, at the Transmission Owner's discretion, to provide maximum wide-area coverage for ~~FR~~SER and ~~SER~~FR data, therefore the following types of BES buses are recommended:

- Electrically distant buses or electrically distant from other DME devices.
- Voltage sensitive areas.
- Cohesive load and generation zones.
- BES buses with a relatively high number of incident transmission circuits.
- BES buses with reactive power devices.
- Major Facilities interconnecting outside the Transmission Owner's area.

Step 9. The list of monitored ~~locations~~BES buses for ~~FR~~SER and ~~SER~~FR data for ~~PRC-002-2~~ Requirement R1 is the aggregate of the BES buses determined in Steps 7 and 8.

DRAFT

Attachment 2

Sequence of Events ~~Recorder~~Recording (SER) Data Format

(Requirement R11, Part 11.3)

Date	Time	Local Time Offset from UTC	Substation	Device	State[1]
08/27/13	23:58:57.110	EST	Sub 1	Breaker 1	Close
08/27/13	23:58:57.082	EST	Sub 2	Breaker 2	Close
08/27/13	23:58:47.217	EST	Sub 1	Breaker 1	Open
08/27/13	23:58:47.214	EST	Sub 2	Breaker 2	Open

[1] Acceptable states are either "OPEN" or "CLOSE". Other status monitoring indications can be used for devices other than circuit breakers.

Guidelines and Technical Basis

High Level Requirement Overview

Requirement	Entity	Identify ~~Bus Locations~~ BES Buses	Notification	SER	FR	5 Year Assessment
R1	TO	X	X	X	X	X
R2	TO | GO			X		
R3	TO | GO				X	
R4	TO | GO				X	

Requirement	Entity	Identify BES Elements	Notification	DDR	5 Year Assessment
R5	RE (PC | RC)	X	X	X	X
R6	TO			X	
R7	GO			X	
R8	TO | GO			X	
R9	TO | GO			X	

Requirement	Entity	Time Synchronization	Provide SER, FR, DDR Data	SER, FR, DDR Availability
R10	TO | GO	X		
R11	TO | GO		X	
R12	TO | GO			X

DRAFT

Guidelines and Technical Basis Section

Introduction

The emphasis of PRC-002-2 is not on how Disturbance Monitoring data is captured, but what Bulk Electric System data is captured. There are a variety of ways to capture the data PRC-002-2 addresses, and existing and currently available equipment can meet the requirements of this standard. PRC-002-2 also addresses the importance of addressing the availability of Disturbance Monitoring capability to ensure the completeness of BES data capture.

~~From a compliance perspective, questions have been raised by industry regarding how conformance to this standard would be judged during a natural disaster which most likely would cause abnormal system conditions for the capturing of data that PRC-002-02 addresses, and also cause the loss of Disturbance Monitoring capability. This is addressed by NERC in its Appendix 4B Sanction Guidelines of the North American Electric Reliability Corporation, Section 2 Basic Principles, Section 2.8 Extenuating Circumstances effective Dec. 20, 2012:~~

~~"In unique extenuating circumstances causing or contributing to the violation, such as significant natural disasters, NERC or the Regional Entity may significantly reduce or eliminate penalties."~~

The data requirements for PRC-002-2 are based on a system configuration assuming all normally~~-~~ closed circuit breakers on a bus are closed.

Guideline for Requirement R1:

Sequence of events and fault records for the analysis, reconstruction, and reporting of system disturbances is important. However, SER and FR data are not required at every ~~location~~BES bus on the BES to conduct adequate or thorough analysis of a disturbance. As major tools of event analysis, the time synchronized time stamp for a breaker change of state and the recorded waveforms of voltage and current for individual circuit sallow precise reconstruction of events of both localized and wide-area disturbances.

In addition, more quality information is always better than less when performing event analysis. However, 100% coverage of all elements is not practical or required for effective analysis of wide-area disturbance. Therefore, selectivity of required ~~locations~~BES buses to monitor is important for the following reasons:

1. Identify key ~~locations~~BES buses where crucial information is available when required.
2. Excessive overlap of coverage is avoided.
3. Avoid gaps in critical coverage.
4. Provide coverage of system elements that could propagate a disturbance.
5. Avoid mandates to cover system elements that are more likely to be a casualty of a disturbance rather than a cause.
6. Establish selection criteria to provide effective coverage in different regions of the continent.

~~Listed as follows, the~~The major characteristics available to determine the selection process are:

1. System voltage level;
2. The number of transmission lines into a substation or switchyard;
3. The number and size of connected generating units;
4. The available short circuit levels.

Although it is straightforward to establish ~~a~~ bright line criteria for the application of identified ~~locations~~BES buses, analysis was required to establish a sound technical basis to fulfill the required objectives~~, rather than using opinions, feelings, or anecdotal judgment based upon experience in one area~~.

To answer these questions and establish criteria for ~~location~~BES buses of SER and FR, the DMSDT established a sub-team referred to as the Monitored Value Analysis Team (MVA Team). The ~~team~~MVA Team collected information from a wide variety of transmission systems throughout the continent to analyze transmission buses by the characteristics previously identified for the selection process.

The MVA Team learned that the development of criteria is not possible for adequate SER and FR coverage, based solely upon simple, bright-line characteristics, such as the number of lines into a substation or switchyard at a particular voltage level or at a set level of short circuit current. To provide the appropriate coverage, a relatively simple but effective ~~Location Selection Procedure~~Methodology for Selecting Buses for Capturing Sequence of Events Recording (SER) and Fault Recording (FR) Data was developed. This Procedure, included as Attachment 1, assists entities in fulfilling Requirement R1 of the standard.

~~The Location Selection Procedure~~The Methodology for Selecting Buses for Capturing Sequence of Events Recording (SER) and Fault Recording (FR) data is weighted to buses with higher short circuit levels. This is chosen for the following reasons:

1. The method is voltage level independent.
2. It is likely to select buses near large generation centers.
3. It is likely to select buses where delayed clearing can cause electric system cascading outages.
4. Selected buses directly correlate to the Universal Power Transfer equation: Lower Impedance – increased power flows – greater system impact.

To perform the ~~simple~~ calculations of Attachment 1~~ of the standard~~, the following information below is required and the following steps (provided in summary form) are required for systems with more than 11 BES ~~bus locations~~buses with three~~-~~ phase short circuit levels above 1500 MVA.

1. Total number of BES buses in the transmission system under evaluation.
   a. Only tangible substation or switchyard buses are included.
   b. Pseudo buses created for analysis purposes in system models are excluded.
2. Determine the three~~-~~ phase short~~-~~ circuit MVA for each bus.
3. Exclude buses from the list with short circuit levels below 1500 MVA.
4. Determine the median short circuit for the top 11 buses on the list (position number 6).

5. Multiply median short circuit level by 20%.
6. Reduce the list of BES buses with short circuit levels higher than 20% of the median.
7. Apply SER and FR at buses with short circuit levels in the top 10% of the list (from 6).
8. Apply SER and FR at buses at an additional 10% of the list using engineering judgment, and allowing flexibility to factor in the following considerations.:
   - a. Electrically distant bus locationsBES buses or electrically distant from other DME devices
   - b. Voltage sensitive areas
   - c. Cohesive load and generation zones
   - d. Bus locationsBES buses with a relatively high number of incident transmission circuits
   - e. Bus locationsBES buses with reactive power devices
   - f. Major facilities interconnecting outside the Transmission Owners' area.

There is no requirement for SER and FR for generating units in this standard.For event analysis purposes, more valuable information is attained about generators and their response to system events pre- and post-contingency through DDR data versus SER or FR records. SER data of the opening of the primary generator output interrupting devices (e.g. synchronizing breaker) may not reliably indicate the actual time that a generator tripped; for instance, when it trips on reverse power after loss of its prime mover (e.g. combustion or steam turbine). For event analysis purposes, more valuable information is attained about generators and their response to system events pre- and post-contingency through DDR data versus SER or FR recordsAs a result, this standard only requires DDR data.

The reevaluation interval of five years was chosen based upon the experience. Five years is long enough to avoid unnecessary reevaluations, but long enough of the DMSDT to address changing system configurations. while creating balance in the frequency of reevaluations.

Guideline for Requirement R3R2:

Analyses of wide-area disturbances often begin by evaluation of SERs to help determine the initiating event(s) and follow the disturbance propagation. Recording of breaker operations help determine the interruption of line flows while generator loading is best determined by DDR data, since generator loading can be essentially zero regardless of breaker position. SER ofdata for generator breaker operations provides little useful data of generator loading.

Generator Owners are included in this requirement because a Generator Owner may, in some instances, own breakers atconnected to the Transmission Owner's bus location. .

Guideline for Requirement R3:

The BES buses for which FR data is required are determined based on the methodology described in Attachment 1 of the standard. The Elements connected to those bus locationsBES buses for which FR data is required include:

- ~~Transmission lines, including interconnection facilities with generating resources~~
- Transformers with a low-side operating voltage of 100kV or above
- Transmission lines

Only those Elements that are identified as BES as ~~per~~identified in the latest in effect NERC definition are to be monitored. For example, radial lines or transformers with low-side voltage less than 100 kV are not included.

FR data must be determinable from each terminal of ~~an~~a BES Element connected to applicable BES buses.

Generator step~~-~~ up transformers (GSU) are excluded from the above based on the following:

- Current contribution from a generator in case of fault ~~in~~on the transmission system will be captured by FR data on the transmission system.
- For faults on the interconnection to generating facilities it is sufficient to have fault current data from the transmission station end of the interconnection. Current contribution from a generator can be readily calculated if needed.

The ~~SDT~~DMSDT, after ~~consultating~~consulting with NERC's Event Analysis group, determined that DDR data from selected generator locations was more important for event analysis than FR data.

Recording of Electrical Quantities

For effective fault analysis it is necessary to know values of all phase and neutral currents and all phase-to-neutral voltages. Based on such ~~FRs~~FR data it is possible to determine all fault types. FR data also ~~augment~~augments SERs in evaluating circuit breaker operation.

Current Recordings

The required electrical quantities are normally directly measured. Certain quantities can be derived if sufficient data is measured, for example residual or neutral currents.
Since a transmission system is generally well balanced, with phase currents having essentially similar magnitudes and phase angle differences of 120°, during normal conditions there is negligible neutral (residual) current. In case of a ground fault the resulting phase current imbalance produces residual current that can be either measured or calculated.

Neutral current, also known as ground or residual current $\mathbf{I}_r$, is calculated as a sum of vectors of three phase currents:

$\mathbf{I}_r = 3 \bullet \mathbf{I}_0 = \mathbf{I}_A + \mathbf{I}_B + \mathbf{I}_C$ ~~Equation 1~~

$\mathbf{I}_0$ - Zero-sequence current

$\mathbf{I}_A$, $\mathbf{I}_B$, $\mathbf{I}_C$ - Phase current (vectors)

Another example of how required electrical quantities can be derived is based on Kirchhoff's ~~law~~Law. Fault currents for one of the BES Elements connected to a particular BES bus ~~location~~

can be derived as a vectorial sum of fault currents recorded at the other BES Elements connected to that BES bus ~~location~~.

Voltage Recordings

Voltages are to be recorded at applicable BES buses. Note that the Requirement calls for the voltages to be determinable. There are two options for recording phase-to-neutral voltages at applicable ~~bus locations~~BES buses:

1. At terminals of each line. This option would apply to lines that have a full set of VTs/CVTs required for distance protections, which is quite common in practice.
2. At a particular BES bus, in which case all the BES Elements connected to that common BES bus are covered.

Guideline for Requirement R4:

This requirement directs the applicable entities having FR determined ~~per~~as identified in Requirement R1 that meets the following:

Requirement R4, Part 4.1 specifies the minimum amount of FR data. Pre- and post-~~-~~trigger fault data along with the SER breaker data, all time stamped to a common clock at millisecond accuracy, aid in the analysis of protection system operations after a fault to determine if ~~the~~a protection system operated as designed. Generally speaking, BES faults and the system response to them occur within a very short time period, approximately 1 to 30 cycles, thus a 30 cycle post-trigger record length captured adequate data. Multiple records allow for legacy microprocessor relays which when time synchronized to a common clock are capable of providing adequate fault data but not capable of providing fault data in a single record with ~~53~~30 cycle post trigger data.

Requirement R4, Part 4.2 specifies the minimum recording rate of FR data. A minimum recording rate of 16 samples per cycle is required to get accurate waveforms and to get 1 millisecond resolution for any digital input which may be used for SER.

Requirement R4, Part 4.3 specifies the minimum triggers to ensure FR data is available. A trigger is a set point on an ~~Oscilloscope~~oscilloscope or ~~Fault Recording~~FR device. The trigger can be set so that when the monitored value on the recording device goes above or below the trigger value, data is recorded. Requirement R4, Part 4.3.1 specifies a neutral (residual) overcurrent trigger for ground faults. Requirement R4, Part 4.3.2 specifies a phase undervoltage or overcurrent trigger for phase-to-phase faults.

Guideline for Requirement R5:

DDR data is used for wide-area disturbance monitoring to determine the system's electromechanical transient and post-transient response and validate system model performance. DDR is typically located based on strategic studies which include angular, frequency, voltage, and oscillation stability. However, for adequately monitoring the system's dynamic response and ensuring sufficient coverage to determine system performance, DDR is required ~~at~~for key ~~locations~~BES Elements in addition to a minimum requirement of DDR coverage.

Each Responsible Entity (PC or RC) is required to identify sufficient DDR data capture for, at a minimum, one BES Element and then one additional BES Element per 3,000 MW of historic peak Demand. This DDR data is included to provide adequate system-~~-~~wide coverage across an

Interconnection. To clarify, if any of the key BES Elements requiring DDR monitoring are within the Responsible Entity's area, DDR data capability is required. If a Responsible Entity (PC or RC) does not meet the requirements of Part 5.1, additional coverage ~~should~~had to be specified.

Loss of large generating resources poses a frequency and angular stability risk for all Interconnections across North America. Data capturing the dynamic response of these machines during a disturbance helps the analysis of large Disturbances. To determine and provide the basis for unit size criteria, the DMSDT acquired specific generating unit data from NERC's Generating Availability Data System (GADS) program. The data contained generating unit size information for each generating unit in North America which was reported in 2013 to the NERC GADS program. The ~~team~~DMSDT analyzed the spreadsheet data to determine: (i) how many units were above or below selected size thresholds; and (ii) the aggregate sum of the ratings of the units within the boundaries of those thresholds. Statistical information about this data was then produced, i.e. averages, means and percentages. The ~~team~~DMSDT determined the following basic information about the generating units of interest (current ~~NA~~North America fleet, i.e. units reporting in 2013) included in the spreadsheet:

- The number of individual generating units in total included in the spreadsheet.
- The number of individual generating units rated at 20 MW or larger included in the spreadsheet. These units would generally require that their owners be registered as GOs in the NERC CMEP.
- The total number of units within selected size boundaries.
- The aggregate sum of ratings, in MWs, of the units within the boundaries of those thresholds.
- The information in the spreadsheet does not provide information by which the plant location of each unit can be determined, i.e. the ~~team~~DMSDT could not use the information to determine which units were located together at a given generation site or facility.

DRAFT

From this information, the ~~team~~DMSDT was able to reasonably speculate the generating unit size thresholds proposed in Requirement R5, Part 5.1.1 of the standard. Generating resources intended for DDR data recording are those individual units with gross nameplate ratings "greater than or equal to 500 MVA~~.~~". The ~~500MVA~~500 MVA individual unit size threshold was selected because this number roughly accounts for 47% of the generating capacity in NERC footprint while only requiring DDR coverage on about 12.5% of the generating units. As mentioned, there was no data pertaining to unit location for aggregating plant/facility sizes. However, Requirement R5, Part 5.1.2 is included to capture larger units located at large generating plants which could pose a stability risk to the system if multiple large units were lost due to electrical or non-electrical contingencies. For generating plants, each individual generator at the plant/facility with a gross nameplate rating greater than or equal to 300 MVA must have DDR where the gross nameplate rating of the plant/facility is greater than or equal to 1000 MVA. The ~~300MVA~~300 MVA threshold was chosen based on the ~~Team's~~DMSDT's judgment and experience. The incremental impact to the number of units requiring monitoring is expected to be relatively low. The incremental impact to the number of units requiring monitoring is expected to be relatively low. ~~Wording was added to cover combined cycle plants, in which the loss of one unit will lead to the loss of a companion unit within a very short period of time. Because of the loss of the entire combined cycle plant, 500MVA was chosen as the threshold.~~

Major transmission interfaces are explicitly defined based on the Interconnection since a common naming convention for these interfaces does not exist. However, this data may be calculated, rather than directly measured~~,~~ if the accurate quantity can be derived (e.g. either end of the Flowgate line could be monitored since the other end could be derived). In the Western Interconnection, these major transmission interfaces are defined by the Regional Entity. In the ERCOT and Quebec Interconnections, the Responsible Entity will be required to identify those interfaces that are deemed significant enough to require monitoring (i.e. are utilized for real-time limits such as System Operating Limits or "contingencies"). Only one BES Element associated with a major transmission interface needs DDR data capability.

Locations where an undervoltage load shedding (UVLS) program is deployed are prone to voltage instability since they are areas of significant Demand. The Responsible Entity (PC or RC) will identify these areas where a UVLS is in service and identify a useful and effective ~~location~~BES Element to monitor for DDR such that action of the UVLS or voltage instability could be captured on the BES. For example, a major 500kV or 230kV substation on the EHV system close to the load pocket where the UVLS is deployed would likely be a valuable ~~location~~BES Element for DDR coverage and would aid in post-disturbance analysis of the load area's response to large system deviations (voltage, frequency, etc.). It is ~~not~~ intended to have DDR

data for ~~all areas affected by~~ "Any one BES Element within a major voltage sensitive area with an in-service undervoltage load shedding (UVLS) program."

Guideline for Requirement R6:

DDR data shows transient response to system disturbances after fault is cleared (post-fault), under a relatively balanced operating condition. Therefore, it is sufficient to provide a single phase-to-neutral voltage or positive sequence voltage. Recording of all three phases of a circuit is not required, although this may be used to compute and record the positive sequence voltage.

The bus where a voltage measurement is required is based on the list of BES Elements defined by the Responsible Entity (PC or RC) in Requirement R5. For example, a breaker-and-a-half or double bus configuration has a North (or East) Bus and South (or West) Bus, ~~which~~ would require that both buses should have voltage recording~~,~~ because either can be taken out of service indefinitely with the targeted BES Element remaining in service. This may be accomplished either by recording both bus voltages separately, or by providing a selector switch to connect either of the bus voltage sources to a single recording input of the DDR device. This component of the requirement is therefore included to mitigate the potential of failed frequency, phase angle, real power, and reactive power calculations due to voltage measurements removed from service while sufficient voltage measurement is actually available during these operating conditions.

It must be emphasized that the data requirements for PRC-002-2 are based on a system configuration assuming all normally~~-~~ closed circuit breakers on a bus are closed.

When current recording is required, it should be on the same phase as the voltage recording taken at the location if a single phase-to-neutral voltage is provided. Positive sequence current record is also acceptable.

For all circuits where current recording is required, real and reactive power will be recorded on a three~~-~~ phase basis. These recordings may be derived either from phase quantities or from positive sequence quantities.

Guideline for Requirement R7:

All Guidelines specified for Requirement R6, ~~-~~apply to Requirement R7~~, too~~. Since either of the high or low~~-~~side windings of the generator step~~-~~ up (GSU) transformer may be connected in delta, phase-to-phase voltage recording is an acceptable voltage recording. As ~~it~~ was explained in the Guideline for R6, the BES is operating under a relatively balanced operating condition and, if needed, phase-to-neutral quantities can be derived from phase-to-phase quantities.

Again it must be emphasized that the data requirements for PRC-002-2 are based on a system configuration assuming all normally~~-~~ closed circuit breakers on a bus are closed.

Guideline for Requirement R8:

Large scale system outages are generally an evolving sequence of events that occur over an extended period of time, making DDR data essential for event analysis. Pre- and post-contingency data helps identify the causes and effects of each event leading to the outages. This drives a need for continuous recording and storage to ensure sufficient data is available for the entire Disturbance.

Transmission Owners and Generator Owners are required to have continuous DDR for the BES Elements identified in Requirement R6. However, this requirement recognizes that legacy equipment may exist ~~at~~for some ~~locations~~BES Elements that do not have continuous data recording capabilities. For equipment that was installed prior to the effective date of the standard, triggered DDR records of three minutes are acceptable using at least one of the trigger types specified in Requirement R8, Part 8.2:

- Off nominal frequency triggers are used to capture high or low frequency excursions of significant size based on the Interconnection size and inertia.
- Rate- of- change of frequency triggers are used to capture major changes in system frequency which could be caused by large changes in generation or load, or possibly changes in system impedance.
- The undervoltage trigger specified in this standard is provided to capture possible sustained undervoltage conditions such as Fault Induced Delayed Voltage Recovery (FIDVR) events. A sustained voltage of 85% is outside normal schedule operating voltages and is sufficiently low to capture abnormal voltage conditions on the BES.

Guideline for Requirement R9:

DDR data contains the dynamic response of a power system to a disturbance and is used for analyzing complex power system events. This recording is typically used to capture short term and long- term disturbances, such as a power swing. Since the data of interest is changing over time, DDR data is normally stored in the form of RMS values or phasor values, as opposed to directly sampled data as found in ~~Fault Recorder~~FR data.

The issue of the sampling rate used in a recording instrument is quite important for at least two reasons: the anti-aliasing filter selection and accuracy of signal representation. The anti-aliasing filter selection is associated with the requirement of a sampling rate at least twice the highest frequency in sampled signal. At the same time, the accuracy of signal representation is also dependent on the selection of the sampling rate. In general, the higher the sampling rate, the better the representation. In the abnormal conditions of interest (e.g. faults or other disturbances); the input signal may contain frequencies in the range of 0-400 Hz. Hence, the rate of 960 samples per second (16 samples/cycle) is considered an adequate sampling rate that satisfies the input signal requirements.

In general dynamic events of interest are: inter-area oscillations, local generator oscillations, wind turbine- generator torsional modes, HVDC control modes, exciter control modes, and steam turbine torsional modes. Their frequencies range from 0.1-20 Hz. In order to reconstruct these dynamic events, a minimum recording time of 30 times per second is required.

Guideline for Requirement ~~R110:~~ ~~See rationale.~~R10: Time synchronization of disturbance monitoring data allows for the time alignment of large volumes of geographically dispersed data records from diverse recording sources. A universally recognized time standard is necessary to provide the foundation for this alignment. Coordinated Universal Time (UTC) is the foundation used for the time alignment of records. It is an international time standard utilizing atomic clocks for generating precision time measurements at fractions of a second levels. The local time offset, expressed as a negative number, is the difference between UTC and the local time zone where the measurements are recorded.

Accuracy of ±2 milliseconds for time synchronization is specified in response to Recommendation 12b in the NERC August, 2003, Blackout Final NERC Report Section V Conclusions and Recommendations:

"Recommendation 12b: Facilities owners shall, in accordance with regional criteria, upgrade existing dynamic recorders to include GPS time synchronization…"

Also, from the U.S.-Canada Power System Outage Task Force Interim Report: Causes of the August 14th Blackout, November 2003, in the United States and Canada, page 103:

"Establishing a precise and accurate sequence of outage-related events was a critical building block for the other parts of the investigation. One of the key problems in developing this sequence was that although much of the data pertinent to an event was time-stamped, there was some variance from source to source in how the time-stamping was done, and not all of the time-stamps were synchronized…"

From NPCC's SP6 Report Synchronized Event Data Reporting, revised March 31, 2005, the investigation by the authoring working group revealed that existing GPS receivers can be expected to provide a time code output which has an uncertainty on the order of 1 millisecond, uncertainty being a quantitative descriptor.

The ±2 milliseconds accuracy requirement specified in this standard is realistically achievable with equipment available and proper cabling installation.

Stored data does not need to be maintained in UTC format. The data provided pursuant to a data request must be provided in UTC format with or without local time offset.

Guideline for Requirement R11:

This requirement directs the applicable entities that upon requests from the Reliability Coordinator, Regional Entity or NERC to provide SER, FR data for BES buses determined in requirement R1 and DDR data for BES Elements determined per requirement R5. To facilitate the analysis of BES disturbances, it is important that the data is provided to the requestor within a reasonable period of time.

Requirement R11, Part 11.1 specifies the maximum ~~timeframe~~time frame of 30 calendar days to provide the data. Thirty calendar days is a reasonable time frame to allow for the collection of data, and submission to the requestor.

Requirement R11, Part 11.2 specifies that the minimum time period of 10 calendar days ~~that~~for which the data will be retrievable preceding a request. With the equipment in use that has the

capability of ~~making a~~ recording data, having the data retrievable for the 10 calendar days preceding a request is realistic and doable. It is important to note that applicable entities should account for any expected delays in retrieving data and this may require devices to have data available for more than 10 days. To clarify the 10 calendar day time frame, an incident occurs on a Day 1. If a request for data is made on Day 6, then that data has to be provided to the requester within 30 calendar days. However, if a request for the data is made on Day 11, that is outside the 10 calendar days specified in the requirement, and an entity would not be out of compliance if it did not have the data.

Requirement R11, Part ~~1~~11.3 specifies a Comma Separated Value (.CSV) format ~~per~~according to Attachment 2 for the SER data. It is necessary to establish a standard format as it will be incorporated with other submitted data to provide a detailed sequence of events timeline of a power system disturbance.

Requirement R11, Part 11.4 specifies the IEEE C37.111 COMTRADE format for the FR and DDR data. The IEEE C37.111 is the Standard for Common Format for Transient Data Exchange it is well established in the industry. It is necessary to specify a standard format as it will be incorporated with other submitted data to provide a detailed analysis of a power system disturbance. C37.111-2013 is a version of COMTRADE that includes formatting for phasor data for Disturbance Recording. Prior versions of C37.111 were not compatible with phasor data.

Requirement R11, Part ~~1~~11.5 specifies the IEEE C37.232 COMNAME format for the naming the data files of the SER, FR and DDR. The IEEE C37.232 is the Standard for Common Format for Naming Time Sequence Data Files first version was approved in 2007. From the August 14, 2003 blackout there was thousands of Fault Recording data files collected. The collected data files did not have a common naming convention and because of that it became difficult to discern which files came from which utilities and which ones were captured by which devices. The lack of a common naming practice seriously hindered the investigation process. Subsequently, and in ~~their~~its initial report on the blackout, NERC stressed the need for having a common naming practice and listed it as one of ~~their~~its top ten recommendations.

Guideline for Requirement R12:

This requirement directs the respective owners of Transmission and ~~Generator~~generator equipment to be alert to the proper functioning of equipment used for SER, FR, and DDR data capabilities for the BES buses and BES Elements which had been established in Requirements R1 and R5 and are found to be out of service. The owners are to ~~-~~ return the capability to service within 90 calendar days of discovery of a failure. This requirement is structured to recognize that the existence of a "reasonable" amount of capability out of service does not result in lack of sufficient data for coverage of the system. Furthermore, 90 calendar days is typically sufficient time for repair or maintenance to be performed. However, in recognition of the fact that there may be occasions for which it is not possible to return the capability to service within 90 calendar days, the requirement further provides that, for such cases, the entity must ~~provide~~develop a timeline and a Corrective Action Plan (CAP) for submission to the Regional

Entity. These actions are considered to be appropriate to provide for robust and adequate data availability.

DRAFT

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. Standard Authorization Request (SAR) posted for comment on January 20, 2010.
2. Revised SAR with supporting draft standard language posted for informal comment on September 10, 2013.

Description of Current Draft

This posting provides a complete draft standard and supporting documentation for an additional 30-day informal comment period to elicit further feedback from industry.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Ballot	June 2014
Final Ballot	September 2014
BOT Adoption	November 2014

Effective Dates

The standard shall become effective on the first day of the first calendar quarter that is 12 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is 12 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Version History

Version	Date	Action	Change Tracking
1.0	TBD	Completed revision, merging and updating PRC-010-0, PRC-020-1, PRC-021-1, and PRC-022-1.	

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Undervoltage Load Shedding Program (UVLS Program): An automatic load shedding program consisting of distributed relays and controls used to mitigate the risk of Cascading, voltage instability, voltage collapse, or uncontrolled separation resulting from undervoltage conditions. Centrally-controlled undervoltage-based load shedding is not included.

Rationale for Definition: As part of the development of PRC-010-1, the drafting team found it necessary to introduce the term Undervoltage Load Shedding Program (UVLS Program) to clearly establish PRC-010-1's applicability. The following discussion and characteristics were critical elements to the development of the proposed definition.

The definition for the term UVLS Program includes automatic load shedding programs that utilize only voltage inputs at locations where action is taken to shed load. Therefore, the failure of a single component is unlikely to affect the reliable performance of the program.

Centrally-controlled undervoltage-based load shedding is excluded, because the load shedding logic may utilize 1) voltage inputs from multiple locations; and/or 2) inputs other than voltages, such as generator reactive reserves, facility loadings, and equipment statuses. As such, its reliable performance could be affected by a single component failure, which is consistent with the nature of Special Protection Systems. Therefore, the drafting team has recommended that Project 2010-05.2 Protection System (Special Protection Systems) include centrally-controlled undervoltage-based load shedding in the definition of a Special Protection System.

The definition of UVLS Program is independent of whether the undervoltage load shedding relays are armed manually or automatically since the arming is done in anticipation of extreme conditions and not during the events when load shedding needs to occur.

In the current inventory of NERC Reliability Standards, there is one instance of the term undervoltage load shedding program in NUC-001-2.1. This standard is part of an open standard revision project, and the finalized definition of UVLS Program will be forwarded to that drafting team for consideration. Likewise, future projects containing standards that feature variations of the term (e.g., undervoltage load shedding system) will also be advised to consider the newly defined term.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title: Undervoltage Load Shedding**

2. **Number: PRC-010-1**

3. **Purpose:** To establish an integrated and coordinated approach to the design, evaluation, and reliable operation of Undervoltage Load Shedding Programs (UVLS Programs).

Rationale for Applicability: This standard is applicable to Planning Coordinators and Transmission Planners that have or are developing a UVLS Program, and to Distribution Providers and Transmission Owners responsible for the ownership, operation, or control of UVLS equipment as required by the UVLS Program established by the Transmission Planner or Planning Coordinator. These Distribution Providers and Transmission Owners are referred to as UVLS entities for the purpose of this standard.

The applicability includes both the Planning Coordinator and Transmission Planner because either may be responsible for designing and coordinating the program based on agreements, memorandums of understanding, or tariffs.

The phrase "Planning Coordinator or Transmission Planner" provides the flexibility for applicability to the entity that will perform the action. The expectation is not that both parties will perform the action, but rather that the Planning Coordinator and Transmission Planner will engage in discussion to determine the appropriate responsible entity.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Planning Coordinator

   4.1.2 Transmission Planner

   4.1.3 Undervoltage load shedding (UVLS) entities – Distribution Providers and Transmission Owners responsible for the ownership, operation, or control of UVLS equipment as required by the UVLS Program established by the Transmission Planner or Planning Coordinator.

5. Background:

UVLS Programs must work correctly to properly protect system reliability. Ensuring program effectiveness and coordination, and ensuring accurate and timely program implementation, assessment, and data will improve UVLS Program performance.

PRC-010-1 – Undervoltage Load Shedding is a consolidation and revision of the following Reliability Standards:

- PRC-010-0 – Assessment of the Design and Effectiveness of UVLS Program
- PRC-020-1 – Under-Voltage Load Shedding Program Database
- PRC-021-1 – Under-Voltage Load Shedding Program Data
- PRC-022-1 – Under-Voltage Load Shedding Program Performance

The UVLS Standard Drafting Team (or drafting team) developed the revised PRC-010-1 to meet the following objectives:

- Address the FERC directive in Order No. 693, Paragraph 1509 to modify PRC-010-0 to require an integrated approach to all protection systems.
- Replace the applicability to and involvement of the Regional Reliability Organization (RRO) in PRC-020-1 and PRC-021-1.
- Consolidate the UVLS-related standards into one comprehensive standard (similar to the construct of FERC-approved PRC-006-1– Automatic Underfrequency Load Shedding).
- Clearly identify and separate centrally-controlled undervoltage-based load shedding due to the reliability requirements needed for this type of load shedding as compared to other UVLS systems.
- Create a single, results-based standard that addresses current reliability issues associated with UVLS.

As noted above, the drafting team found it is necessary to establish a bright line with respect to the characteristics of centrally-controlled undervoltage-based load shedding in regard to its reliability requirement-related needs. Because the reliable performance of centrally-controlled undervoltage-based load shedding could be affected by a single component failure, the drafting team maintains that this type of load shedding is consistent with the nature of Special Protection Systems (SPSs) and should be covered by SPS-related Reliability Standards.

Therefore, PRC-010-1 introduces a new NERC Glossary term, UVLS Program, to clearly establish PRC-010-1's applicability to automatic load shedding programs consisting of distributed relays and controls used to mitigate the risk of Cascading, voltage instability, voltage collapse, or uncontrolled separation resulting from undervoltage conditions. It is noted that this term excludes centrally-controlled undervoltage-based load shedding.

Subsequently, since the current NERC Glossary definition of Special Protection System excludes UVLS, Project 2010-05.2 Protection Systems: Phase 2 (Special Protection Systems) will adjust the definition to exclude only UVLS Programs as defined above and therefore include centrally-controlled undervoltage-based load shedding.

Requirements of the revised Reliability Standard PRC-010-1 meet the following objectives:

- Demonstrate a UVLS Program's effectiveness prior to implementation, including the program's coordination with other protection systems and generator voltage ride-through capabilities.
- Adhere to UVLS Program specifications and implementation schedule.
- Perform periodic assessment and performance analysis of UVLS Programs and resolve identified deficiencies.
- Maintain and share UVLS Program data.

Also of note, Project 2009-03 Emergency Operations is retiring specific requirements and revising EOP-003-2 – Load Shedding Plans to eliminate identified redundancy between PRC-010-1 and EOP-003-2. In addition, the UVLS drafting team's intention is for PRC-004 to address appropriate types of UVLS Program Misoperations (as previously addressed by PRC-022-1); the introduction of this revision to PRC-004 is pending outcomes of PRC-004-3, which is currently in final stages of development under Project 2010-05.1 Protection Systems: Phase 1 (Misoperations).

B. Requirements and Measures

Rationale for R1: In Paragraph 1509 from Order No. 693, FERC directed NERC to require an integrated and coordinated approach to all protection systems. The drafting team agrees that a lack of coordination among protection systems is a key risk to reliability, and that each Planning Coordinator or Transmission Planner that develops a UVLS Program should demonstrate the program's viability and effectiveness prior to implementation. This demonstration should include studies and analyses used when developing the program that show implementation of the program resolves the identified undervoltage issues that led to its design. These studies and analyses should also show that the UVLS Program is integrated through coordination with generator voltage ride-through capabilities and other protection and control systems. Though presented as separate items, the drafting team recognizes that the studies that show coordination considerations and that the program addresses undervoltage issues may be interrelated and presented as one comprehensive analysis.

R1. Each Planning Coordinator or Transmission Planner that is developing a UVLS Program shall demonstrate its effectiveness prior to implementing the program. This demonstration shall include, but is not limited to, studies and analyses that show: *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

1.1. The implementation of the UVLS Program resolves the identified undervoltage issues that led to the UVLS Program's design.

1.2. The UVLS Program is integrated through coordination with generator voltage ride-through capabilities and other protection and control systems, including, but not limited to, transmission line protection, auto-reclosing, SPSs, and other undervoltage-based load shedding programs.

M1. Acceptable evidence may include, but is not limited to, studies and analyses, date-stamped reports, or other documentation detailing the effectiveness of the UVLS Program.

Rationale for R2: UVLS entities must implement a UVLS Program according to the specifications and schedule provided by the Planning Coordinator or Transmission Planner. If UVLS entities do not implement the UVLS Program according to the specifications and schedule provided, the UVLS Program may not be effective and may not achieve its intended goal.

R2. Each UVLS entity shall adhere to the UVLS Program specifications and implementation schedule determined by its Planning Coordinator or Transmission Planner. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

M2. Acceptable evidence may include, but is not limited to, date-stamped documentation identifying the feeders armed with UVLS relays, the UVLS relay settings, and the associated Load summaries.

Rationale for R3: A periodic comprehensive assessment (detailed analysis) should be conducted to capture the accumulated effects of minor changes to the system that have occurred since the last assessment was completed, and should include an evaluation of each UVLS Program to ensure the continued integration through coordination. This comprehensive assessment supplements the TPL-001-4 annual assessment requirement to evaluate the impact of protection systems.

Based on the drafting team's knowledge and experience, and in keeping with time frames contained in similar requirements from other PRC Reliability Standards, 60 calendar months was determined to be the maximum amount of time allowable between assessments. The drafting team asserts that there will be circumstances other than a periodic assessment, such as material changes to system topology or operating conditions, that could affect the performance of a UVLS Program and trigger assessments prior to the end of the 60-calendar month period. If so, the 60-calendar month time frame would reset after each assessment.

R3. Each Planning Coordinator or Transmission Planner shall perform a comprehensive assessment to evaluate the effectiveness of each existing UVLS Program in its area at least once every 60 calendar months or sooner if material changes are made to system topology or operating conditions. The assessment shall include, but is not limited to, studies and analyses that evaluate whether: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. The UVLS Program resolves the identified undervoltage issues for which the UVLS Program is designed.

3.2. The UVLS Program is integrated through coordination with generator voltage ride-through capabilities and other protection and control systems, including, but not limited to, transmission line protection, auto-reclosing, SPSs, and other UVLS programs.

M3. Acceptable evidence may include, but is not limited to, date-stamped reports or other documentation detailing the assessment of the UVLS Program.

Rationale for R4: A UVLS Program not functioning as expected during a voltage excursion event for which the UVLS Program was designed to operate presents a critical risk to system reliability. Therefore, a timely assessment to evaluate whether the UVLS Program resolved the undervoltage issues associated with the applicable event is essential. The 12 calendar months (from the date of the event) provides adequate time to coordinate with other Planning Coordinators and Transmission Planners, Transmission Operators, and UVLS entities, simulate pre- and post-event conditions, and complete the performance assessment.

R4. Each Planning Coordinator or Transmission Planner shall, within 12 calendar months of an event that resulted in a voltage excursion for which the program was designed to operate, perform an assessment to evaluate whether the UVLS Program resolved the undervoltage issues associated with the event. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M4. Acceptable evidence may include, but is not limited to, date-stamped event data, event analysis reports, or other documentation detailing the assessment of the UVLS Program.

Rationale for R5: If program deficiencies are identified during any assessment of a UVLS Program, a CAP must be developed to address the deficiencies. Based on the drafting team's knowledge and experience with UVLS studies, three calendar months was determined to provide a judicious balance between the reliability need to address deficiencies expeditiously and time needed to consider potential solutions, coordinate resources, and develop a CAP.

R5. Each Planning Coordinator or Transmission Planner that identifies deficiencies in its UVLS Program during an assessment shall develop a Corrective Action Plan (CAP) to address the deficiencies within three calendar months of identification. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M5. Acceptable evidence must include a CAP that addresses identified deficiencies and may also include date-stamped reports or other documentation supporting the CAP.

Rationale for R6: Having accurate and current data is required for the Planning Coordinator to perform undervoltage studies and for use in event analyses. Requirement R6 supports this reliability need by requiring the UVLS entity to provide UVLS Program data in accordance with specified parameters.

R6. Each UVLS entity shall provide data to its Planning Coordinator according to the format and schedule specified by the Planning Coordinator to support maintenance of each UVLS Program database. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. Acceptable evidence may include, but is not limited to, date-stamped emails, letters, or other documentation demonstrating data was provided to the Planning Coordinator as specified.

Rationale for R7: Having accurate and current data is required for the Planning Coordinator to perform studies and for use in event analyses. Requirement R7 supports this reliability need by requiring the Planning Coordinator to update its UVLS Program database at least once each calendar year.

R7. Each Planning Coordinator that has a UVLS Program in its area shall update a database containing data necessary to model its UVLS Program for use in event analyses and assessments of the UVLS Program at least once each calendar year. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M7. Acceptable evidence may include, but is not limited to, date-stamped spreadsheets, database reports, or other documentation demonstrating a UVLS Program database was updated.

Rationale for R8: Requirement R8 supports the integrated and coordinated approach to UVLS programs directed by Paragraph 1509 of Order No. 693 by requiring that UVLS Program data be shared with neighboring Planning Coordinators and Transmission Planners within a reasonable time frame of a request.

R8. Each Planning Coordinator that has a UVLS Program in its area shall provide its UVLS Program database to other Planning Coordinators and Transmission Planners within its Interconnection within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M8. Acceptable evidence may include, but is not limited to, date-stamped emails, letters, or other documentation demonstrating that the UVLS Program database was provided as requested within 30 calendar days.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

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

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

- The applicable entity shall keep data or evidence to show compliance with Requirements R1, R2, R3, R5, R6, R7, and R8 since the last audit.
- The applicable entity shall keep data or evidence to show compliance with Requirement R4 for six calendar years.

If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	High	N/A	N/A	N/A	The applicable entity that developed the UVLS Program failed to demonstrate the program's effectiveness prior to implementation in accordance with Requirement R1, including the items specified in Parts 1.1 and 1.2.
R2	Long-term Planning	High	N/A	N/A	The applicable entity failed to adhere to the UVLS Program specifications in accordance with Requirement R2. OR The applicable entity failed to adhere to the UVLS Program implementation schedule in accordance with Requirement R2.	The applicable entity failed to adhere to the UVLS Program specifications and implementation schedule in accordance with Requirement R2.

R3	Long-term Planning	Medium	N/A	N/A	N/A	The applicable entity failed to perform an assessment at least once during the 60 calendar months in accordance with Requirement R3, including the items specified in Parts 3.1 and 3.2.
R4	Operations Planning	Medium	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 12 calendar months but less than or equal to 13 calendar months after an applicable event.	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 13 calendar months but less than or equal to 14 calendar months after an applicable event.	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 14 calendar months but less than or equal to 15 calendar months after an applicable event.	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 15 months after an applicable event. OR The applicable entity failed to perform an assessment in accordance with Requirement R4.

R5	Operations Planning	Medium	The applicable entity developed a CAP in accordance with Requirement R5, but was late by less than or equal to 15 calendar days.	The applicable entity developed a CAP in accordance with Requirement R5, but was late by more than 15 calendar days but less than or equal to 30 calendar days.	The applicable entity developed a CAP in accordance with Requirement R5, but was late by more than 30 calendar days but less than or equal to 45 calendar days.	The applicable entity developed a CAP in accordance with Requirement R5, but was late by more than 45 calendar days. OR The responsible entity failed to develop a CAP in accordance with Requirement R5.
R6	Operations Planning	Lower	The applicable entity provided data in accordance with Requirement R6, but was late by less than or equal to 30 calendar days per the specified schedule. OR The applicable entity provided data in accordance with Requirement R6, but the data was not according to the specified format.	The applicable entity provided data in accordance with Requirement R6, but was late by more than 30 calendar days but less than or equal to 60 calendar days per the specified schedule.	The applicable entity provided data in accordance with Requirement R6, but was late by more than 60 calendar days but less than or equal to 90 calendar days per the specified schedule.	The applicable entity provided data in accordance with Requirement R6, but was late by more than 90 calendar days per the specified schedule. OR The applicable entity failed to provide data in accordance with Requirement R6.

R7	Operations Planning	Lower	The applicable entity updated the database in accordance with Requirement R7, but was late by less than or equal to 30 calendar days.	The applicable entity updated the database in accordance with Requirement R7, but was late by more than 30 calendar days but less than or equal to 60 calendar days.	The applicable entity updated the database in accordance with Requirement R7, but was late by more than 60 calendar days but less than or equal to 90 calendar days.	The applicable entity updated the database in accordance with Requirement R7, but was late by more than 90 calendar days. OR The applicable entity failed to update the database in accordance with Requirement R7.
R8	Operations Planning	Lower	The applicable entity provided its UVLS Program database in accordance with Requirement R8, but was late by less than or equal to 15 calendar days.	The applicable entity provided its UVLS Program database in accordance with Requirement R8, but was late by more than 15 calendar days but less than or equal to 30 calendar days.	The applicable entity provided its UVLS Program database in accordance with Requirement R8, but was late by more than 30 calendar days but less than or equal to 45 calendar days.	The applicable entity provided its UVLS Program database in accordance with Requirement R8, but was late by more than 60 calendar days. OR The applicable entity failed to provide its UVLS Program database in accordance with Requirement R8.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Introduction

PRC-010-1 is a single, comprehensive standard that addresses the same reliability principles outlined in its legacy standards, PRC-010-0, PRC-020-1, PRC-021-1, and PRC-022-1. The standard also addresses a FERC directive from Order No. 693, Paragraph 1509. This paragraph directs NERC to develop a modification to PRC-010-0 that requires an integrated and coordinated approach to all protection systems, including generators and transmission lines, generators' low voltage ride through capabilities, and UFLS and UVLS programs.

Since FERC-approved PRC-006-1 – Automatic Underfrequency Load Shedding was developed under a similar construct of combining existing standards and addressing a FERC Order No. 693 directive, the drafting team looked to this standard as a guide. With the understanding that UVLS and UFLS programs have fundamental differences, the drafting team adopted PRC-006-1's industry-vetted reliability principles and language as applicable to UVLS Programs.

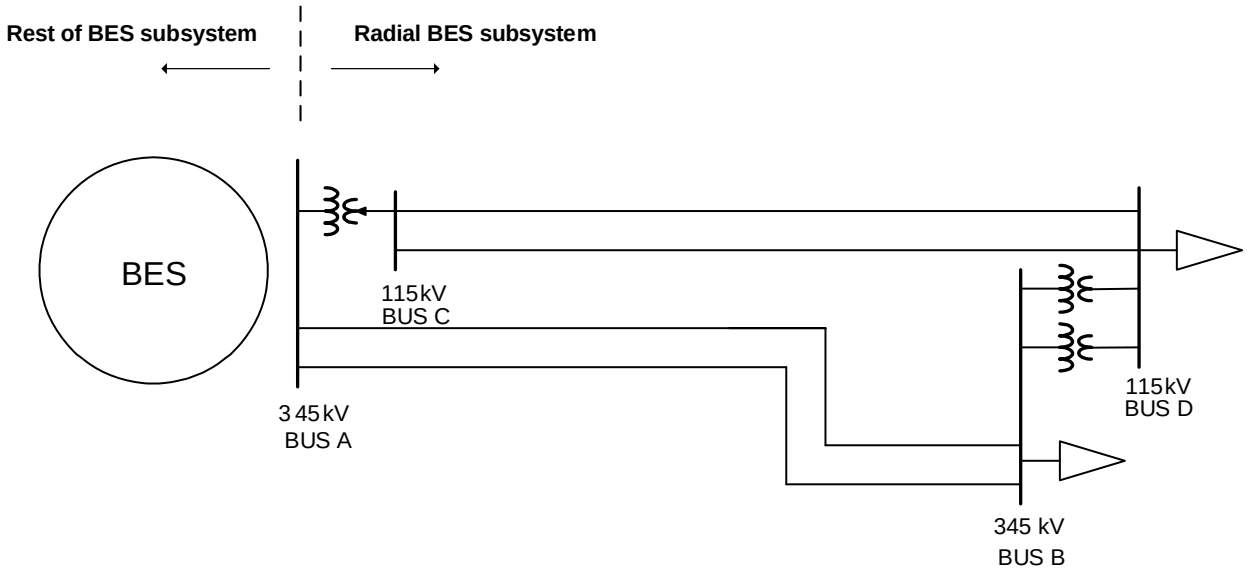
The drafting team's established purpose for PRC-010-1 is to clearly define the responsibilities of applicable entities to pursue an integrated and coordinated approach to the design, evaluation, and reliable operation of UVLS Programs. Since the need for and design of UVLS Programs is unique to each system preservation footprint, the intent of the standard is to provide a framework of reliability requirements for such programs to which each individual entity can apply its program's specific considerations and characteristics. The drafting team emphasizes that PRC-010-1 does not require a mandatory UVLS Program, nor does this standard address the need to have a UVLS Program. PRC-010-1 applies only after an entity has determined the need for a UVLS Program as a result of its own planning studies.

The drafting team provides the following discussion to support the approach to the standard. The information is meant to enhance the understanding of the reliability needs and deliverable expectations of each requirement, supported as necessary by technical principles and industry experience.

Guidelines for UVLS Program Definition

To ensure that the UVLS Program standard's applicability is to only those undervoltage-based load shedding programs whose performance has an impact on system reliability, a UVLS Program must mitigate risk of one more of the following: Cascading, voltage instability, wide area voltage collapse, or uncontrolled separation. An example of a program that would not fall under this category is undervoltage-based load shedding installed to mitigate damage to equipment or local loads that are directly affected by the low voltage event.

Below is an example of a radial Bulk Electric System (BES) subsystem for which a UVLS system could be used as a solution to mitigate various issues following the loss of the 345 kV double circuit line between bus A and bus B (TPL category C Contingency). If the consequence of this Contingency is limited to undervoltage conditions, loss of load, or overloading of facilities within the contained area formed by buses A to D, a UVLS system (at buses B and D) used to mitigate this case would not fall under the definition of a UVLS Program. However, if this same UVLS system would be used to mitigate Adverse Reliability Impact outside this contained area, it would be classified as a wide-area undervoltage problem and would fall under the definition of UVLS Program.



High Level Requirement Overview

Requirement	Entity	Demonstrate Program Effectiveness	Adhere to Program Specifications and Schedule	Program Assessment (Periodic or Performance)	CAP to Address Program Deficiencies	Update and/or Share Program Data
R1	PC or TP	X				
R2	UVLS entity		X			
R3	PC or TP	X		X		
R4	PC or TP	X		X		
R5	PC or TP				X	
R6	UVLS entity					X
R7	PC					X
R8	PC					X

Guidelines for Requirement R1:

A UVLS Program may be developed and implemented to either serve as a safety net system protection measure against unforeseen extreme Contingencies or to achieve specific system performance for known transmission Contingencies for which dropping of load is allowed under TPL Reliability Standards. Regardless of the purpose, it is important that the UVLS Program being implemented is effective in terms that it mitigates the risk of Cascading, voltage instability, wide-area voltage collapse, or uncontrolled separation resulting from undervoltage conditions. Consideration should be given to voltage set points and time delays, rate of voltage decay or recovery, power flow levels, etc. when designing a UVLS Program.

For the UVLS Program to be effective in achieving its goal, it is also necessary that the UVLS Program is coordinated with generator voltage ride-through capabilities and other protection and control systems that may have an impact on the performance of UVLS Program. Some of these protection and control systems may include, but are not limited to, transmission line protection, SPSs, other undervoltage-based load shedding programs, auto-reclosing, and controls of shunt capacitors, reactors, and SVSs.

For example, if the purpose of a UVLS Program is to mitigate fault-induced delayed voltage recovery (FIDVR) events in a large load center that also includes local generation, it is important that such a UVLS Program is coordinated with local generators' voltage ride-through capabilities. Generators in the vicinity of a load center are critical to providing dynamic voltage support to the system during FIDVR events. To maximize the benefit of online generation, the best practice may be to shed load prior to generation trip. However, occasionally, it may be best to let generation

trip prior to load shed. Therefore, the impact of generation tripping should be considered while designing a UVLS Program.

Another example that can be highlighted is the coordination of a UVLS Program with automatic shunt reactor tripping devices if there are any on the system. Most likely, any shunt reactors on the system will trip off automatically after some time delay during low voltage conditions. In such cases, shunt reactors should be tripped before the load is shed to preserve the system. This may require coordination of time delays associated with the UVLS Program with shunt reactor tripping devices.

Examples given above demonstrate that, for a UVLS Program to be effective, proper consideration should be given to coordination of a UVLS Program with generator ride-through capabilities and other protection and control systems.

Guidelines for Requirement R2:

Once a Planning Coordinator or Transmission Planner has identified a need for a UVLS Program, the Planning Coordinator or Transmission Planner will develop a program that includes specifications and an implementation schedule, which are then provided to UVLS entities. Specifications may include voltage set points, time delays, amount of load to be shed, the location at which load needs to be shed, etc. If UVLS entities do not implement the UVLS Program according to the specifications and schedule provided, the UVLS Program may not be effective and may not achieve its intended goal.

Guidelines for Requirement R3:

In addition to the initial studies required to develop a UVLS Program, periodic comprehensive assessments (detailed analyses) are required to ensure its continued effectiveness. This assessment should be completed at least once every 60 calendar months to capture the accumulated effects of minor changes to the system that have occurred since the last assessment was completed. There may also be material changes to system topology or operating conditions that would necessitate this same comprehensive assessment at any point in time. Regardless of the trigger, the assessment should include an evaluation of each UVLS Program to ensure the continued integration through coordination.

This comprehensive assessment supplements the TPL-001-4 annual assessment requirement to evaluate the impact of protection systems. The 60-month period is the same time frame used in TPL-001-4 and in PRC-006-1.

The material change terminology is also used in the TPL-001-4 standard. The industry concluded that the term material change is not transportable on a continent wide basis. Requirement R2, Part 6.2 of TPL-001-4 specifies that documentation to support the technical rationale for determining material changes shall be included. Similar documentation should also support a UVLS Program assessment that is a result of a material change.

As specified in Requirement R3, a comprehensive assessment must be performed at least once every 60 calendar months. If a comprehensive assessment necessitated by a material change is

conducted within the 60-month window, the 60-month time period would restart upon completion of this assessment.

Guidelines for Requirement R4:

The goal of the assessment required in Requirement R4 is to evaluate whether the UVLS Program resolved the undervoltage issues for an event that occurred on the system. It is expected that the assessment should include event data analysis, such as the relevant sequence of events leading to the undervoltage conditions (e.g., Contingencies, operation of protection systems, and SPSs) and field measurements useful to analyzing the behavior of the system. A comprehensive description of the UVLS Program operation should be presented, including conditions of the trigger (e.g., voltage levels, time delays) and amount of load shed for each affected substation. Simulations of the event shall be performed to evaluate the level of performance of the program for the event of interest and to identify deficiencies to be included in a CAP per Requirement R5.

The studies and analyses showing the effectiveness of the UVLS Program can be similar to what is required in Requirements R1 and R3, but should include a clear link between the demonstration of effectiveness (in studies using simulations) and the analysis of the event (with measurements and event data) that actually occurred. For example, differences between the expected and actual system behavior for the event of interest should be discussed and modeling assumptions should be evaluated. Important discrepancies between the simulations and the actual event should be investigated.

Considering the importance of an event that involves the operation of a UVLS Program, the 12-calendar month period provides adequate time to analyze the event and perform an assessment while identifying deficiencies within a reasonable time. This time period is also required in PRC-006-1.

Guidelines for Requirement R5:

Requirement 5 promotes the prudent correction of an identified problem during assessment evaluations of each UVLS Program. An assessment of an active UVLS Program is triggered:

- After material changes are made to system topology or operating conditions. Since every UVLS is unique, the Planning Coordinator or Transmission Planner will decide the degree to which the change in topology or operating condition becomes a material change sufficient to trigger an assessment of the existing UVLS Program.

- Within 12 calendar months of an event that resulted in a voltage excursion for which the program was designed to operate.

- At least once every 60 months. The default time frame of 60 months or less between assessments has the intention to assure that the cumulative changes to the network and operating condition affecting the UVLS Program are evaluated.

The 60-calendar month time frame would reset after each assessment.

A CAP is a list of actions and an associated timetable for implementation to remedy a specific problem. It is a proven tool for resolving operational problems. The responsible entity is required to implement and complete a CAP to accomplish the purpose of this requirement, which is to prevent future deficiencies in the UVLS Program, thereby minimizing risk to the system. The responsible entity is also required to complete the CAP, document the plan implementation, and retain the appropriate evidence to demonstrate implementation and completion.

Deferrals or other relevant changes to the CAP need to be documented so that the record includes not only what was planned, but what was implemented. Depending on the planning and documentation format used by the responsible entity, evidence of a successful CAP execution could consist of signed-off work orders, printouts from work management systems, spreadsheets of planned versus completed work, timesheets, work inspection reports, paid invoices, photographs, walk-through reports, or other evidence. Documentation of a CAP provides an auditable progress and completion confirmation for the identified UVLS Program deficiency.

CAP examples:

CAP Example 1 - Corrective actions for a quick triggering problem; preemptive actions for similar installations:

Fault records showed that a group of UVLS relays did trigger at the right undervoltage level but with shorter delays that expected. On-site inspections were completed in three weeks, confirming that the delay time programmed on the relays was 60 cycles instead of 90 cycles. A plan was scheduled for the next eight weeks to correct to a 90-cycle time delay setting of those UVLS relays identified to have shorter time delay settings.

Applicability to other UVLS relays: Based on our risk assessment, we scheduled to verify and adjust all remaining UVLS relays time delay settings within a one-year period.

CAP Example 2 - Corrective actions for a firmware problem; preemptive actions for similar installations:

Fault records were provided to the manufacturer on 6/4/2014. On 6/11/2014, the manufacturer responded that the misoperation of the UVLS relay was caused by a bug in version 2 firmware, and recommended installing version 3 firmware. Version 3 firmware was installed on 6/12/2014.

> Applicability to other UVLS relays: Based on our risk assessment, we plan to install firmware version 3 at all of our installations that are determined to be version 2. Proposed completion date is 12/31/2014.
>
> The firmware replacements were completed on 12/4/2014.

Based on industry experience and operational coordination timeframes, the drafting team believes that within three calendar months from the date the problem was identified is a reasonable time frame for development of a CAP, including time to consider alternative solutions and coordination of resources. The "within three calendar months" time frame is solely to develop a CAP and it does not include the time needed for its implementation.

Determining the cause of the deficiency is essential in developing an effective CAP to avoid future re-occurrence of the same problem. A CAP can be revised if additional causes are found.

Guidelines for Requirements R6–R8

An accurate UVLS Program database is necessary for the Planning Coordinator or Transmission Planner to perform system reliability assessment studies and event analysis studies. Without accurate data, there is a possibility that annual reliability assessment studies that are performed by the Planning Coordinator can lead to erroneous results and therefore impact reliability. Also, without the accurate data, it is very difficult for the Planning Coordinator or Transmission Planner to match a UVLS event and determine the root cause of the problem.

To support a UVLS Program database, it is necessary for each UVLS entity to provide accurate data to its Planning Coordinator. Each UVLS entity will provide the data according to the specified format and schedule provided by the Planning Coordinator. This is required in order for the Planning Coordinator to maintain and support a comprehensive UVLS Program database. By having a comprehensive database, the Planning Coordinator can embark on a reliability assessment or event analysis/benchmarking studies, identify the issues with the UVLS Program, and develop remedial action plans.

Items to be included in the UVLS database are as follows:

- Owner and operator of the UVLS Program
- Size and location of customer load, or percent of connected load, to be interrupted
- Corresponding voltage set points and overall scheme clearing times
- Time delay from initiation to trip signal
- Breaker operating times
- Any other schemes that are part of or impact the UVLS Programs, such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS, and SPSs.

Additionally, the UVLS Program database should be updated annually (once every calendar year) by the Planning Coordinator. The intent here is for UVLS entities to review the data annually and provide changes to the Planning Coordinators so that Planning Coordinators can keep the databases current and accurate for performing event analysis and other assessments.

Finally, a Planning Coordinator is required to provide information to other Planning Coordinators and Transmission Planners within its Interconnection within 30 calendar days of a request. The 30 calendar days was selected as an acceptable time frame as it is considered to be reasonable and well-accepted by the industry. Also, this requirement of sharing the database with other Planning Coordinators and Transmission Planners supports the directive provide by FERC that requires an integrated and coordinated approach to UVLS programs (Paragraph 1509 of FERC Order No. 693).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-02 Undervoltage Load Shedding (PRC-010-1)

VRF and VSL Justifications

This document provides the Undervoltage Load Shedding Standard Drafting Team's (drafting team's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in PRC-010-1 – Undervoltage Load Shedding.

Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

The drafting team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project:

NERC Criteria - Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a Cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or Cascading failures; or, a requirement in a planning time frame that, if violated, could, under Emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a Cascading sequence of failures; place the Bulk Electric System at an unacceptable risk of instability, separation, or Cascading failures; or hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or Cascading failures; or, a requirement in a planning time frame that, if violated, could, under Emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under Emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or Cascading failures nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the Emergency, abnormal, or

restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System or the ability to effectively monitor, control, or restore the Bulk Electric System. A planning requirement that is administrative in nature.

FERC Violation Risk Factor Guidelines

Guideline (1) — Consistency with the Conclusions of the Final Blackout Report

The Commission seeks to ensure that Violation Risk Factors assigned to requirements of reliability standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk Power System.

In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief

Guideline (2) — Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

Guideline (3) — Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) — Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) — Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such requirements must not be watered down to reflect the lower risk level associated with the less important objective of the reliability standard.

The following discussion addresses how the drafting team considered FERC's VRF Guidelines 2 through 5. The team did not address Guideline 1 directly because of an apparent conflict between Guidelines 1 and 4. Whereas Guideline 1 identifies a list of topics that encompass nearly all topics within NERC's Reliability Standards and implies that these requirements should be assigned a "High" VRF, Guideline 4 directs assignment of VRFs based on the impact of a specific requirement to the reliability of the system. The drafting team believes that Guideline 4 is reflective of the intent of VRFs in the first instance and, therefore, concentrated its approach on the reliability impact of the requirements.

PRC-010-1 – Undervoltage Load Shedding is a revision of PRC-010-0 – Assessment of the Design and Effectiveness of UVLS Program, with the stated purpose: *To establish an integrated and coordinated approach to the design, evaluation, and reliable operation of Undervoltage Load Shedding Programs.* FERC Order No. 693 requested that PRC-010-0 be modified to require that an integrated and coordinated approach be included in all protection systems on the Bulk Power System, including generators and transmission lines, generators' low voltage ride-through capabilities, and underfrequency loading shedding (UFLS) and undervoltage load shedding (UVLS) programs. PRC-010-1 addresses this directive in addition to consolidating and revising PRC-010-0 with the three (3) other existing UVLS standards: PRC-020-1 – Under-Voltage Load Shedding Program Database, PRC-021-1 – Under-Voltage Load Shedding Program Data, and PRC-022-1 – Under-Voltage Load Shedding Program Performance.

PRC-010-1 has eight (8) requirements that incorporate and enhance the intent of the requirements of PRC-010-0, PRC-020-1, PRC-021-1, and PRC-022-1. The revised standard requires that entities developing an Undervoltage Load Shedding Program demonstrate the program's effectiveness prior to implementation. Applicable entities are then required to adhere to the Undervoltage Load Shedding Program specifications and implementation schedule. The standard also requires an assessment of the program at least once every 60 months (or sooner if needed) and an assessment to evaluate program performance within 12 months of an applicable event. If program deficiencies are identified as a result of any of these assessments, entities are required to develop a Corrective Action Plan within three (3) months. In addition, there are requirements to update, provide data for, and share an Undervoltage Load Shedding database containing information necessary to model the program for use in event analyses and assessments.

The requirements of PRC-010-1 do not map, one-to-one, with the requirements of the legacy standards. The new requirements comingle various reliability attributes of the legacy standards with new reliability objectives, thus a requirement-to-requirement comparison of VRFs is not possible. In developing the new

VRFs for the requirements of PRC-010-1, the drafting team carefully considered the NERC criteria for developing VRFs, as well as the FERC VRF guidelines. The VRFs of FERC-approved PRC-006-1 – Automatic Underfrequency Load Shedding influenced (citing FERC VRF Guideline 3) the drafting team's VRF decisions, as the drafting team used PRC-006-1 as a model with respect to PRC-010-1's language and construct.

NERC Criteria - Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance, and may have only one, two, or three VSLs.

VSLs should be based on the guidelines shown in the table below:

Lower	Moderate	High	Severe
Missing a minor element (or a small percentage) of the required performance. The performance or product measured has significant value as it almost meets the full intent of the requirement.	Missing at least one significant element (or moderate percentage) of the required performance. The performance or product measured still has significant value in meeting the intent of the requirement.	Missing more than one significant element (or missing a high percentage) of the required performance or is missing a single vital component. The performance or product has limited value in meeting the intent of the requirement.	Missing most or all of the significant elements (or a significant percentage) of the required performance. The performance measured does not meet the intent of the requirement or the product delivered cannot be used in meeting the intent of the requirement.

FERC Order on Violation Severity Levels

In its June 19, 2008 Order on Violation Severity Levels, FERC indicated it would use the following four guidelines for determining whether to approve VSLs:

Guideline 1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior Levels of Non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when Levels of Non-compliance were used.

Guideline 2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

Guideline 2a: A violation of a "binary" type requirement must be a "Severe" VSL.

Guideline 2b: Do not use ambiguous terms such as “minor” and “significant” to describe noncompliant performance.

Guideline 3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline 4: Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the “default” for penalty calculations.

VRF and VSL Justifications – PRC-010-1, R1	
Proposed VRF	High
NERC VRF Discussion	This is a planning requirement that meets the NERC criterion for a High VRF. Failure to ensure the effectiveness of an Undervoltage Load Shedding Program could, under anticipated Emergency, abnormal, or restorative conditions, directly contribute to Bulk Electric System instability, separation, or Cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report:** N/A
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard:** The requirement has Parts that all support the reliability objective so only one VRF was assigned; therefore no conflict(s) exist.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards:** This requirement is similar to EOP-003-2, Requirements R3 and R7, which have approved VRFs of High.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs:** This is a planning requirement that meets the NERC criterion for a High VRF. Failure to ensure the effectiveness of an Undervoltage Load Shedding Program as specified in Requirement R1 could, under anticipated Emergency, abnormal, or restorative conditions, directly contribute to Bulk Electric System instability, separation, or Cascading failures.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation:** This requirement does not co-mingle reliability objectives of differing risk; the assigned VRF of High is consistent throughout the requirement.
Proposed Lower VSL	N/A
Proposed Moderate VSL	N/A
Proposed High VSL	N/A
Proposed Severe VSL	The applicable entity that developed the UVLS Program failed to demonstrate the program's effectiveness prior to implementation in accordance with Requirement R1, including the items specified in Parts 1.1 and 1.2.
NERC VSL Guidelines Discussion	Meets NERC's VSL Guidelines—there is a binary aspect for failure; the VSL addresses the degrees of compliance with respect to equal importance of the two Parts.

VRF and VSL Justifications – PRC-010-1, R1	
FERC VSL G1 Discussion	**Guideline 1- Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance:** This is a new requirement; therefore, there is no prior level of compliance.
FERC VSL G2 Discussion	**Guideline 2- Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties** **Guideline 2a- The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent:** The proposed VSL for this binary requirement is consistent with the guideline in that it is classified as a severe VSL. **Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language** The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	**Guideline 3- Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement:** The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4	**Guideline 4- Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations:** The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justifications – PRC-010-1, R2	
Proposed VRF	High
NERC VRF Discussion	This is a planning requirement that meets the NERC criterion for a High VRF. Failure to adhere to the Undervoltage Load Shedding Program specifications and implementation schedule could, under anticipated Emergency, abnormal, or restorative conditions, directly contribute to Bulk Electric System instability, separation, or Cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report:** N/A
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard:** The requirement has no Parts so only one VRF was assigned.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards:** This requirement is consistent with PRC-006-1, Requirement R9 and EOP-003-2, Requirement R5, which have approved VRFs of High.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs:** This is a planning requirement that meets the NERC criterion for a High VRF. Failure to adhere to the Undervoltage Load Shedding Program specifications and implementation schedule could, under anticipated Emergency, abnormal, or restorative conditions, directly contribute to Bulk Electric System instability, separation, or Cascading failures.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation:** This requirement does not co-mingle reliability objectives of differing risk; the assigned VRF of High is consistent throughout the requirement.
Proposed Lower VSL	N/A
Proposed Moderate VSL	N/A
Proposed High VSL	The applicable entity failed to adhere to the UVLS Program specifications in accordance with Requirement R2. OR The responsible entity failed to adhere to the UVLS Program implementation schedule in accordance with Requirement R2.
Proposed Severe VSL	The applicable entity failed to adhere to the UVLS Program specifications and implementation schedule in accordance with Requirement R2.
NERC VSL Guidelines Discussion	Meets NERC's VSL Guidelines—the VSLs cover aspects of the requirement that are equal in importance.

VRF and VSL Justifications – PRC-010-1, R2	
FERC VSL G1 Discussion	**Guideline 1- Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance:** This is a new requirement; therefore, there is no prior level of compliance.
FERC VSL G2 Discussion	**Guideline 2- Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties** **Guideline 2a- The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent:** N/A **Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language** The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	**Guideline 3- Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement:** The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4	**Guideline 4- Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations:** The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justifications – PRC-010-1, R3	
Proposed VRF	Medium
NERC VRF Discussion	This is a planning requirement that meets NERC's criterion for a Medium VRF. Failure to perform a comprehensive assessment to evaluate the effectiveness of each existing Undervoltage Load Shedding Program in its area at least once every 60 calendar months or sooner if material changes are made to system topology or operating conditions, could, under anticipated Emergency, abnormal, or restorative conditions, directly and adversely affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of the requirement is unlikely to lead to Bulk Electric System instability, separation, or Cascading failures. The applicable entities are always responsible for maintaining the reliability of the Bulk Electric System regardless of the situation.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report:** N/A
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard:** The requirement has Parts that all support the reliability objective so only one VRF was assigned; therefore no conflict(s) exist.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards:** This requirement is consistent with PRC-010-0, Requirement R1, which has an approved VRF of Medium.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs:** This is a planning requirement that meets NERC's criterion for a Medium VRF. Failure to perform a comprehensive assessment to evaluate the effectiveness of each existing Undervoltage Load Shedding Program in its area at least once every 60 calendar months or sooner if material changes are made to system topology or operating conditions, could, under anticipated Emergency, abnormal, or restorative conditions, directly and adversely affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of the requirement is unlikely to lead to Bulk Electric System instability, separation, or Cascading failures. The applicable entities are always responsible for maintaining the reliability of the Bulk Electric System regardless of the situation.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation:** This requirement does not co-mingle reliability objectives of differing risk; the assigned VRF of Medium is consistent throughout the requirement.

VRF and VSL Justifications – PRC-010-1, R3	
Proposed Lower VSL	N/A
Proposed Moderate VSL	N/A
Proposed High VSL	N/A
Proposed Severe VSL	The applicable entity failed to perform an assessment at least once during the 60 calendar months in accordance with Requirement R3, including the items specified in Parts 3.1 and 3.2.
NERC VSL Guidelines Discussion	Meets NERC's VSL Guidelines—there is a binary aspect for failure; the VSLs address the degrees of compliance with respect to equal importance of the two Parts.
FERC VSL G1 Discussion	**Guideline 1- Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance:** The VSL is consistent in nature with the current VSL associated with the existing requirement being replaced (PRC-010-0, Requirement R1) and therefore does not lower the current level of compliance.
FERC VSL G2 Discussion	**Guideline 2- Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties** **Guideline 2a- The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent:** The proposed VSL for this binary requirement is consistent with the guideline in that it is classified as a severe VSL. **Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language** The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	**Guideline 3- Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement:** The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4	**Guideline 4- Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations:** The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justifications – PRC-010-1, R4	
Proposed VRF	Medium
NERC VRF Discussion	This requirement meets NERC's criterion for a Medium VRF. Failure to perform an assessment to evaluate whether the Undervoltage Load Shedding Program resolved the undervoltage issues associated with a qualifying event in a timely manner could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of the requirement is unlikely to lead to Bulk Electric System instability, separation, or Cascading failures. The applicable entities are always responsible for maintaining the reliability of the Bulk Electric System regardless of the situation.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report:** N/A
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard:** The requirement has no Parts so only one VRF was assigned.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards:** This requirement is similar to PRC-022-1, Requirement 1 and PRC-006-1, Requirement R11, which have approved VRFs of Medium.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs:** This requirement meets NERC's criterion for a Medium VRF. Failure to perform an assessment to evaluate whether the Undervoltage Load Shedding Program resolved the undervoltage issues associated with a qualifying event in a timely manner could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of the requirement is unlikely to lead to Bulk Electric System instability, separation, or Cascading failures. The applicable entities are always responsible for maintaining the reliability of the Bulk Electric System regardless of the situation.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation:** This requirement does not co-mingle reliability objectives of differing risk; the assigned VRF of Medium is consistent throughout the requirement.
Proposed Lower VSL	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 12 calendar months but less than or equal to 13 calendar months after an applicable event.
Proposed Moderate VSL	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 13 calendar months but less than or equal to 14 calendar months after an applicable event.

VRF and VSL Justifications – PRC-010-1, R4	
Proposed High VSL	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 14 calendar months but less than or equal to 15 calendar months after an applicable event.
Proposed Severe VSL	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 15 months after an applicable event. OR The applicable entity failed to perform an assessment in accordance with Requirement R4.
NERC VSL Guidelines Discussion	Meets NERC's VSL Guidelines—there is an incremental aspect to the VSL for tardiness and a binary aspect for failure.
FERC VSL G1 Discussion	**Guideline 1- Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance:** The VSLs' associated requirement is different in construct from the existing requirement being replaced (PRC-022-1, Requirement R1) and, therefore, the VSLs cannot be compared. The VSLs for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Discussion	**Guideline 2- Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties** **Guideline 2a- The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent:** N/A **Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language** The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	**Guideline 3- Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement:** The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4	**Guideline 4- Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations:** The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justifications – PRC-010-1, R5	
Proposed VRF	Medium
NERC VRF Discussion	This requirement meets NERC's criterion for a Medium VRF. Failure to develop a Corrective Action Plan to address the deficiencies identified as a result of an Undervoltage Load Shedding Program assessment in a timely manner could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of the requirement is unlikely to lead to Bulk Electric System instability, separation, or Cascading failures. The applicable entities are always responsible for maintaining the reliability of the Bulk Electric System regardless of the situation.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report:** N/A
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard:** The requirement has no Parts so only one VRF was assigned.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards:** This requirement is similar to PRC-006-1, Requirement R12, which has an approve VRF of Medium.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs:** This requirement meets NERC's criterion for a Medium VRF. Failure to develop a Corrective Action Plan to address the deficiencies identified as a result of an Undervoltage Load Shedding Program assessment in a timely manner could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of the requirement is unlikely to lead to Bulk Electric System instability, separation, or Cascading failures. The applicable entities are always responsible for maintaining the reliability of the Bulk Electric System regardless of the situation.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation:** This requirement does not co-mingle reliability objectives of differing risk; the assigned VRF of Medium is consistent throughout the requirement.
Proposed Lower VSL	The applicable entity developed a CAP in accordance with Requirement R5, but was late by less than or equal to 15 calendar days.
Proposed Moderate VSL	The applicable entity developed a CAP in accordance with Requirement R5, but was late by more than 15 calendar days but less than or equal to 30 calendar days.

VRF and VSL Justifications – PRC-010-1, R5	
Proposed High VSL	The applicable entity developed a CAP in accordance with Requirement R5, but was late by more than 30 calendar days but less than or equal to 45 calendar days.
Proposed Severe VSL	The applicable entity developed a CAP in accordance with Requirement R5, but was late by more than 45 calendar days. OR The applicable entity failed to develop a CAP in accordance with Requirement R5.
NERC VSL Guidelines Discussion	Meets NERC's VSL Guidelines—there is an incremental aspect to the VSL for tardiness and a binary aspect for failure.
FERC VSL G1 Discussion	**Guideline 1- Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance:** The VSLs' associated requirement is different in construct from the existing requirement being replaced (PRC-022-1, Requirement R1.5) and, therefore, the VSLs cannot be compared. The VSLs for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Discussion	**Guideline 2- Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties** **Guideline 2a- The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent:** N/A **Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language** The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	**Guideline 3- Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement:** The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4	**Guideline 4- Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations:** The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justifications – PRC-010-1, R6	
Proposed VRF	Lower
NERC VRF Discussion	This is an administrative planning requirement that meets NERC's criterion for a Lower VRF. Failure to provide data according to the specified format and schedule to support maintenance of each Undervoltage Load Shedding Program database would not, under the anticipated Emergency, abnormal, or restorative conditions, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. The applicable entities are always responsible for maintaining the reliability of the Bulk Electric System regardless of the situation.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report:** N/A
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard:** The requirement has no Parts so only one VRF was assigned.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards:** This requirement is consistent with PRC-006-1, Requirement R8, which has an approved VRF of Lower.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs:** This is an administrative planning requirement that meets NERC's criterion for a Lower VRF. Failure to provide data according to the specified format and schedule to support maintenance of each Undervoltage Load Shedding Program database would not, under the anticipated Emergency, abnormal, or restorative conditions, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. The applicable entities are always responsible for maintaining the reliability of the Bulk Electric System regardless of the situation.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation:** This requirement does not co-mingle reliability objectives of differing risk; the assigned VRF of Lower is consistent throughout the requirement.

VRF and VSL Justifications – PRC-010-1, R6	
Proposed Lower VSL	The applicable entity provided data in accordance with Requirement R6, but was late by less than or equal to 30 calendar days per the specified schedule. OR The applicable entity provided data in accordance with Requirement R6, but the data was not according to the specified format.
Proposed Moderate VSL	The applicable entity provided data in accordance with Requirement R6, but was late by more than 30 calendar days but less than or equal to 60 calendar days per the specified schedule.
Proposed High VSL	The applicable entity provided data in accordance with Requirement R6, but was late by more than 60 calendar days but less than or equal to 90 calendar days per the specified schedule.
Proposed Severe VSL	The applicable entity provided data in accordance with Requirement R6, but was late by more than 90 calendar days per the specified schedule. OR The applicable entity failed to provide data in accordance with Requirement R6.
NERC VSL Guidelines Discussion	Meets NERC's VSL Guidelines—the VSLs cover aspects of the requirement that are not equal in importance; there is an incremental aspect to the VSL for tardiness and a binary aspect for failure.
FERC VSL G1 Discussion	**Guideline 1- Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance:** The VSLs' associated requirement is different in construct from the existing requirement being replaced (PRC-021-1, Requirement R1) and, therefore, the VSLs cannot be compared. The VSLs for this requirement meet or exceed the current level of compliance.
FERC VSL G2 Discussion	**Guideline 2- Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties** **Guideline 2a- The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent:** N/A **Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language** The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – PRC-010-1, R6	
FERC VSL G3	**Guideline 3- Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement:** The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4	**Guideline 4- Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations:** The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justifications – PRC-010-1, R7	
Proposed VRF	Lower
NERC VRF Discussion	This is an administrative planning requirement that meets NERC's criterion for a Lower VRF. Failure to update an Undervoltage Load Shedding Program database would not, under the anticipated Emergency, abnormal, or restorative conditions, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. The applicable entities are always responsible for maintaining the reliability of the Bulk Electric System regardless of the situation.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report:** N/A
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard:** The requirement has no Parts so only one VRF was assigned.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards:** This requirement is consistent with PRC-006-1, Requirement R6, which has an approved VRF of Lower.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs:** This is an administrative planning requirement that meets NERC's criterion for a Lower VRF. Failure to update an Undervoltage Load Shedding Program database would not, under the anticipated Emergency, abnormal, or restorative conditions, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. The applicable entities are always responsible for maintaining the reliability of the Bulk Electric System regardless of the situation.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation:** This requirement does not co-mingle reliability objectives of differing risk; the assigned VRF of Lower is consistent throughout the requirement.
Proposed Lower VSL	The applicable entity updated the database in accordance with Requirement R7, but was late by less than or equal to 30 calendar days.
Proposed Moderate VSL	The applicable entity updated the database in accordance with Requirement R7, but was late by more than 30 calendar days but less than or equal to 60 calendar days.
Proposed High VSL	The applicable entity updated the database in accordance with Requirement R7, but was late by more than 60 calendar days but less than or equal to 90 calendar days.

VRF and VSL Justifications – PRC-010-1, R7	
Proposed Severe VSL	The applicable entity updated the database in accordance with Requirement R7, but was late by more than 90 calendar days. OR The applicable entity failed to update the database in accordance with Requirement R7.
NERC VSL Guidelines Discussion	Meets NERC's VSL Guidelines— there is an incremental aspect to the VSL for tardiness and a binary aspect for failure.
FERC VSL G1 Discussion	**Guideline 1- Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance:** The existing requirement being replaced (PRC-020-1, Requirement R1) is applicable to the Regional Reliability Organization and has no associated VSLs. Therefore, there is no prior level of compliance.
FERC VSL G2 Discussion	**Guideline 2- Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties** **Guideline 2a- The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent:** N/A **Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language** The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	**Guideline 3- Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement:** The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4	**Guideline 4- Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations:** The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justifications – PRC-010-1, R8	
Proposed VRF	Lower
NERC VRF Discussion	This is an administrative planning requirement that meets NERC's criterion for a Lower VRF. Failure to provide an Undervoltage Load Shedding Program database within a timely manner of a request would not, under the anticipated Emergency, abnormal, or restorative conditions, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. The applicable entities are always responsible for maintaining the reliability of the Bulk Electric System regardless of the situation.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report:** N/A
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard:** The requirement has no Parts so only one VRF was assigned.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards:** This requirement is consistent with PRC-006-1, Requirement R7, which has an approved VRF of Lower.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs:** This is an administrative planning requirement that meets NERC's criterion for a Lower VRF. Failure to provide an Undervoltage Load Shedding Program database within a timely manner of a request would not, under the anticipated Emergency, abnormal, or restorative conditions, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. The applicable entities are always responsible for maintaining the reliability of the Bulk Electric System regardless of the situation.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation:** This requirement does not co-mingle reliability objectives of differing risk; the assigned VRF of Lower is consistent throughout the requirement.
Proposed Lower VSL	The applicable entity provided its UVLS Program database in accordance with Requirement R8, but was late by less than or equal to 15 calendar days.
Proposed Moderate VSL	The applicable entity provided its UVLS Program database in accordance with Requirement R8, but was late by more than 15 calendar days but less than or equal to 30 calendar days.

VRF and VSL Justifications – PRC-010-1, R8	
Proposed High VSL	The applicable entity provided its UVLS Program database in accordance with Requirement R8, but was late by more than 30 calendar days but less than or equal to 45 calendar days.
Proposed Severe VSL	The applicable entity provided its UVLS Program database in accordance with Requirement R8, but was late by more than 60 calendar days. OR The applicable entity failed to provide its UVLS Program database in accordance with Requirement R8.
NERC VSL Guidelines Discussion	Meets NERC's VSL Guidelines—there is an incremental aspect to the VSL for tardiness and a binary aspect for failure.
FERC VSL G1 Discussion	**Guideline 1- Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance:** The existing requirement being replaced (PRC-020-1, Requirement R2) is applicable to the Regional Reliability Organization and has no associated VSLs. Therefore, there is no prior level of compliance.
FERC VSL G2 Discussion	**Guideline 2- Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties** **Guideline 2a- The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent:** N/A **Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language** The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	**Guideline 3- Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement:** The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4	**Guideline 4- Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations:** The VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

PRC-004-3 – Protection System Misoperation Identification and Correction

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s):[2]	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	Audit
Names of Auditors:	Supplied by CEA

Applicability of Requirements *[RSAW developer to insert correct applicability]*

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1		X	X									X			
R2		X	X									X			
R3		X	X									X			
R4		X	X									X			
R5		X	X									X			
R6		X	X									X			

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Facilities

4.2.1 Protection Systems for BES Elements, with the following exclusions:

4.2.1.1 Non-protective functions that are embedded within a Protection System.

4.2.1.2 Protective functions intended to operate as a control function during switching.[3]

4.2.1.3 Special Protection Systems (SPS).

4.2.1.4 Remedial Action Schemes (RAS).

4.2.2 Underfrequency load shedding (UFLS) that is intended to trip one or more BES Elements.

Subject Matter Experts

Identify Subject Matter Expert(s) responsible for this Reliability Standard. -(Insert additional rows if necessary)

Registered Entity Response (Required):

SME Name	Title	Organization	Requirement(s)

[3] For additional information and examples, see the "Non-Protective Functions" and "Control Functions" sections in the Application Guidelines.

DRAFT

R1 Supporting Evidence and Documentation

R1. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, identify whether its Protection System component(s) caused a Misoperation ~~when:~~under the following circumstances:

1.1 The BES interrupting device operation was caused by a Protection System or by manual intervention in response to a Protection System failure to operate; and

1.2 The BES interrupting device owner owns all or part of the Composite Protection System; and

1.3 The BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation.

~~**M1.**~~ **M1.** Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it identified the Misoperation of its Protection System component(s), if any, that meet the circumstances in Requirement R1, Parts 1.1, 1.2, and 1.3 within the allotted time period. Acceptable evidence for Requirement R1, including Parts 1.1, 1.2, and 1.3 may include, but is not limited to, the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested:[i]

Provide the following evidence, or other evidence to demonstrate compliance. Please contact your CEA with any questions regarding requested evidence.
A list of BES interrupting device operations within the audit period meeting the criteria of Requirement R1 Parts 1.1 through 1.3.
Of these BES interrupting device operations, evidence such as in Measure M1 identifying whether its Protection System component(s) caused a Misoperation (or not).

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to PRC-004-3, R1

This section to be completed by the Compliance Enforcement Authority

	Select, all or a sample thereof, BES interrupting device operations from the list of such operations outlined in the Evidence Requested section above.
	~~For BES interrupting device operations, as selected by auditor, verify that such operations met the criteria outlined in Requirement R1 Parts 1.1 through 1.3. If criteria is not met, then no identification necessary and no further audit testing is required.~~
	~~If Requirement R1 Parts 1.1 through 1.3 criteria is met for~~For selected BES interrupting device operations, verify the entity identified whether or not its Protection System component(s) caused a Misoperation within 120 calendar days of the BES interrupting device operation.

Note to Auditor: Auditors should use their professional judgment in selecting BES interrupting device operations for testing. Sources of such operations could include entity lists or auditor's knowledge of events occurring on the entity's system. In order to determine if entity identified whether there was a Misoperation (in accordance with Requirement R1) the auditor should seek evidence, such as that provided in Measure M1, associated with analyses of those BES interrupting device operations meeting Requirement R1, Parts 1.1 through 1.3.

If the BES interrupting device operation does not meet the criteria, then no identification is necessary and no further audit testing is required.

Auditor ~~should~~may identify instances where an entity identified a Misoperation of its Protection System component(s), but did not determine the cause(s) of the Misoperation (within the 120 calendar day period of R1) for verification of compliance with Requirement R4.

Auditor ~~-~~Notes:~~-~~

R2 Supporting Evidence and Documentation

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, ~~notify the other owner(s) of the Protection System of the operation when:~~ provide notification as described in 2.1 and 2.2:

~~2~~**2.1** For a BES interrupting device operation by a Composite Protection System, notification of the operation shall be provided to the other owner(s) that share Misoperation identification responsibility for the Composite Protection System under the following circumstances:

2.1.1 The BES interrupting device owner shares the Composite Protection System ownership with any other ~~entity~~owner; and

2.1.2 The BES interrupting device owner has determined that a Misoperation occurred or cannot rule out a Misoperation; and

2.1.3 The BES interrupting device owner has determined that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation.

2.2 For a BES interrupting device operation by a Protection System component intended to operate as backup protection for a condition on another entity's Element, notification of the operation shall be provided to the other Protection System owner(s) for which that backup protection was provided.

M2. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates notification to the other owner(s), within the allotted time period for either Requirement R2, Part 2.1, including subparts 2.1.1, 2.1.2, and 2.1.3 and Requirement R2, Part 2.2.Acceptable evidence for Requirement R2, including Parts 2.1, ~~2.2,~~ and 2.~~3~~2 may include, but is not limited to, the following dated documentation (electronic or hardcopy format): emails, facsimiles, or transmittals.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested:[i]

Provide the following evidence, or other evidence to demonstrate compliance. Please contact your CEA with any questions regarding requested evidence.
A list of BES interrupting device operations within the audit period meeting the criteria of ~~Requirement R2~~Part 2.1, Parts 2.1.1 through 2.1.3.
For Requirement R2 Part 2.2, a list of BES interrupting device operations within the audit period that operated as backup protection for a condition on another entity's Element.
Of these BES interrupting device operations, evidence such as in Measure M2 of entity notifying other owner(s) of the Composite Protection System.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to PRC-004-3, R2
This section to be completed by the Compliance Enforcement Authority

	Select, all or a sample thereof, BES interrupting device operations meeting Requirement R2, Parts 2.1 ~~through~~and 2.~~3~~2.
	~~For BES interrupting device operations, as selected by auditor, verify that such operations met the criteria outlined in Requirement R2 Parts 2.1 through 2.3 for notifying other owner(s) of the Protection System of the operation. If criteria is not met, then no notification is necessary and no further audit testing is required.~~
	For selected BES interrupting device operations requiring notifying other owner(s), verify entity notified the other owners of the operation within 120 days of the operation.

Note to Auditor: Auditors should use their professional judgment in selecting BES interrupting device operations for testing. Sources of such operations could include entity lists or auditor's knowledge of events occurring on the entity's system. In order to determine if entity notified other owners of the Composite Protection System (in accordance with Requirement R2) auditor should seek evidence, as provided in Measure M2 associated with selected operations.

See Application Guidelines under section Requirement R2 for notification requirements for vertically integrated utilities.

Auditor ~~-~~Notes:~~-~~

R3 Supporting Evidence and Documentation

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that receives notification, pursuant to Requirement R2 shall, within the later of 60 calendar days of notification or 120 calendar days of the BES interrupting device(s) operation, ~~shall~~ identify whether its Protection System component(s) caused a Misoperation.

~~**M3.**~~ **M3.** Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it identified whether its Protection System component(s) caused a Misoperation within the allotted time period. Acceptable evidence for Requirement R3 may include, but is not limited to, the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested:[i]

Provide the following evidence, or other evidence to demonstrate compliance. Please contact your CEA with any questions regarding requested evidence.
List of notifications received by entity within the audit period pursuant to Requirement R2.
Of these notifications, evidence such as in Measure M3 of the entity identifying whether its Protection System component(s) caused a Misoperation (or not).

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to PRC-004-3, R3

This section to be completed by the Compliance Enforcement Authority

	Select, all or a sample thereof, notifications received by entity pursuant to Requirement R2.~~–~~
	For notifications received by entity, as selected by auditor, verify entity identified, within the timeframes established in Requirement R3, whether its Protection System component(s) caused a Misoperation ~~within the timeframes established in Requirement R3.~~.

Note to Auditor: Auditors should use their professional judgment in selecting notifications for audit testing. Sources of such notifications could include entity lists, auditor's knowledge of events occurring on the entity's system, or inquiries of neighboring entities. In order to determine if entity identified whether its Protection System component(s) caused a Misoperation, the auditor should seek evidence, as provided in Measure M3, associated with selected notifications.

Auditor ~~should~~may identify instances where an entity identified a Misoperation of its Protection System component(s) (in accordance with Requirement R3), but did not determine the cause(s) of the Misoperation for verification of compliance with Requirement R4.

Auditor ~~-~~Notes:~~-~~

R4 Supporting Evidence and Documentation

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that has not determined the cause(s) of a Misoperation, for a Misoperation identified in accordance with Requirement R1 or R3 shall perform investigative action(s) to determine the cause of the Misoperation at least once every two full calendar quarters after the Misoperation was first identified, until one of the following completes the investigation:-

- The identification of the cause(s) of the Misoperation; or
- A declaration that no cause was identified.

~~**M4.**~~ **M4.** Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it performed at least one investigative action according to Requirement R4 every two full calendar quarters until a cause is identified or a declaration is made. Acceptable evidence for Requirement R4 may include, but is not limited to, the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested:[i]

Provide the following evidence, or other evidence to demonstrate compliance. Please contact your CEA with any questions regarding requested evidence.
List of identified Misoperations ~~where a cause has not been identified by entity within the parameters of~~ pursuant to Requirement R1 or R3, within the audit period, where the cause of the Misoperation was not revealed.
Of the Misoperation list, documented cause(s) of the Misoperation pursuant to Requirement R4.
Of the Misoperation list, declarations where no cause was identified.
Evidence such as in Measure M4.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to PRC-004-3, R4
This section to be completed by the Compliance Enforcement Authority

	Select, all or a sample of, identified Misoperations where a cause has not been identified by the entity.-
	For each identified Misoperation without a cause selected, verify entity performed (or is performing) investigative action(s) to determine the cause(s) of the Misoperation at least once every two full calendar quarters after the Misoperation was first identified ~~at the frequency prescribed in Requirement R4.~~ .
	For completed investigative actions, verify that entity has either determined a cause or has a declaration that no cause was identified.

Note to Auditor: Auditors should use their professional judgment in selecting Misoperations for audit testing. Sources of such Misoperations could include entity lists or knowledge gained by the auditor via their review of Requirements R1 or R3. In order to determine if entity performed the investigative action(s) established in Requirement R4, the auditor should seek evidence, as provided in Measure M4, associated with selected Misoperations.

~~An~~The following is an example of~~,~~ what is meant by "once every two full calendar quarters after the Misoperation was first identified~~" is a~~:" A Misoperation ~~where~~(with no cause ~~is~~) initially identified on February ~~1~~10 (Quarter One) must be investigated (per Requirement R4) by ~~the end of~~ September 30 (Quarter three) of the same year ~~the Misoperation is first identified.~~ . Quarters two and three are the full quarters counted.

Auditor ~~-~~Notes:~~-~~

R5 Supporting Evidence and Documentation

R5. Each Transmission Owner, Generator Owner, and Distribution Provider that owns the Protection System component(s) that caused the Misoperation shall, within 60 calendar days of first identifying a cause of the Misoperation:

- Develop a Corrective Action Plan (CAP) for the identified Protection System component(s), and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations, or
- Explain in a declaration why corrective actions are beyond the entity's control or would not improve BES reliability, and that no further corrective actions will be taken.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it developed a CAP and an evaluation of the CAP's applicability to other Protection Systems and locations, or a declaration in accordance with Requirement R5. Acceptable evidence for Requirement R5 may include, but is not limited to~~,~~ the following dated documentation (electronic or hardcopy format): ~~a dated~~ CAP and evaluation, or ~~a dated~~ declaration.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested:[i]

Provide the following evidence, or other evidence to demonstrate compliance. Please contact your CEA with any questions regarding requested evidence.
~~Evidence~~Within the audit period, evidence such as in Measure M5 for Misoperations with an identified cause.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to PRC-004-3, R5

This section to be completed by the Compliance Enforcement Authority

	Select, all or a sample thereof, identified Misoperations with a cause.
	For identified Misoperations with a cause, as selected by the auditor, verify entity developed a CAP and evaluation, or a declaration as described in Requirement R5.
	Verify CAP and evaluation, or declaration, was developed within 60 calendar days of the first identified cause.
	Verify CAP contains actions and a timetable to resolve the cause(s) of the identified Misoperation and verify entity evaluated the CAP's applicability ~~of the cause~~ to the entity's other Protection Systems and locations; or that the declaration contains why no corrective action will be taken according to Requirement R5.

Note to Auditor: Auditors should use their professional judgment in selecting Misoperations with an identified cause for audit testing. Sources of such Misoperations for audit testing should be obtained from information learned by, or provided to, the auditor from testing of Misoperations for Requirements R1, R3, or R4.

Auditor Notes:

R6 Supporting Evidence and Documentation

R6. Each Transmission Owner, Generator Owner, and Distribution Provider shall implement each CAP developed in Requirement R5, and update each CAP if actions or timetables change, until completed.

M6. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it implemented each CAP, including updating actions or timetables. Acceptable evidence for Requirement R6 may include, but is not limited to, the following dated documentation (electronic or hard copy format): dated records that document the implementation of each CAP and the completion of actions for each CAP including revision history of each CAP. Evidence may also include work management program records, work orders, and maintenance records.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested:[i]

Provide the following evidence, or other evidence to demonstrate compliance. Please contact your CEA with any questions regarding requested evidence.
From the CAPs developed in Requirement R5, evidence such as in Measure M6 demonstrating implementation of each CAP.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to PRC-004-3, R6

This section to be completed by the Compliance Enforcement Authority

	Select, all or a sample thereof, CAPs for correcting the cause(s) of an identified Misoperation.
	For CAPs selected, verify implementation and that CAP was updated in accordance with Requirement R6.

Note to Auditor: Auditors should use their professional judgment in selecting CAPs for audit testing. Sources of CAPs for audit testing should be obtained from information learned by, or provided to, the auditor in Requirement R5.~~–~~

In checking for implementation, auditors should verify evidence (such as described in Measure M6) that the actions or activities prescribed by the CAP were actually performed by the entity.

Items, such as work management records, supporting the implementation of actions and timetables to implement the CAP are alternatives to a written document.

Auditor ~~-~~Notes:~~-~~

DRAFT

Additional Information:

Reliability Standard

The RSAW developer should provide the following information without hyperlinks. Update the information below as appropriate.

The full text of PRC-004-3 may be found on the NERC website (www.nerc.com) under "Program Areas & Departments", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC website.

In addition to the Reliability Standard, there is background information available on the NERC website.

Capitalized terms in the Reliability Standard refer to terms in the *Glossary of Terms used in NERC Reliability Standards*, which may be found on the NERC website.

Sampling Methodology [If developer deems reference applicable]

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria, or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language – [Developer to ensure RSAW has been provided to NERC Legal for links to appropriate Regulatory Language – See example below]

E.g. FERC Order No. 742 paragraph 34: "Based on NERC's……."

E.g. FERC Order No. 742 Paragraph 55, Commission Determination: "We affirm NERC's……."

Selected Glossary Terms [If developer deems applicable]

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Revision History

Version	Date	Reviewers	Revision Description
1	2/14/2014	NERC Compliance	New Document
2	5/30/2014	NERC Compliance	Revised based on revisions to Reliability Standard and comments received during formal comment period.

[i] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

DRAFT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2010-05.1 – Protection Systems: Phase 1 (Misoperations)

Requested Approvals

- PRC-004-3 – Protection System Misoperation Identification and Correction
- Definitions of "Composite Protection System" and "Misoperation"

Requested Retirements

- PRC-003-1 – Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection System
- PRC-004-2.1a – Analysis and Mitigation of Transmission and Generation Protection System Misoperations

Prerequisite Approvals

- None

Revisions to Defined Terms in the NERC Glossary

The standard drafting team proposes the following new definition:

Composite Protection System:

The total complement of ~~the~~ Protection System(s) that function collectively to protect an Element~~, such as any primary, secondary, local backup, and communication-assisted relay systems.~~. Backup protection provided ~~by~~to a remote Protection System is excluded.

The standard drafting team proposes the following revised definition:

Misoperation:

The failure of a Composite Protection System to operate as intended~~.~~ for protection purposes. Any of the following is a Misoperation:

1. **Failure to Trip – During Fault** – A failure of a Composite Protection System to operate for a Fault condition for which it is designed. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.
2. **Failure to Trip – Other Than Fault** – A failure of a Composite Protection System to operate for a non-Fault condition ~~for which it is designed, such as a power swing, undervoltage,~~

~~overexcitation, or loss of excitation. The failure of a Protection System component is not a Misoperation as long as~~if the ~~performance of~~duration of its operating time resulted in the operation of at least one other Element's Composite Protection System ~~is correct~~.

3. **Slow Trip – During Fault** – A Composite Protection System operation that is slower than required for a Fault condition ~~for which it is designed. Delayed clearing~~if the duration of ~~a Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or~~its operating time resulted in the operation of ~~any~~at least one other Element's Composite Protection System.
4. **Slow Trip – Other Than Fault** – A Composite Protection System operation that is slower than required for a non-Fault condition ~~for which it is designed~~, such as a power swing, undervoltage, overexcitation, or loss of excitation~~. Delayed clearing~~ if the duration of ~~a non-Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or~~its operating time resulted in the operation of ~~any~~at least one other Element's Composite Protection System.
5. **Unnecessary Trip – During Fault** – An unnecessary Composite Protection System operation for a Fault condition on another Element.
6. **Unnecessary Trip – Other Than Fault** – An unnecessary Composite Protection System operation for a non-Fault condition ~~for which it is not designed. A~~. A Composite Protection System operation that is caused by personnel during on-site maintenance, testing, inspection, construction or commissioning activities is not a Misoperation.

General Considerations

The implementation period allows adequate time for applicable entities to develop or modify its procedures and processes for reviewing Protection System operations. ~~The obligation for reporting Misoperations has been removed from PRC-004 and is being developed under the NERC Rules of Procedure, Section 1600 – Request for Data or Information.~~ The development and implementation of a Corrective Action Plan remains within the scope of PRC-004; therefore, little additional time and resources should be needed to account for the increased detail in the required performance identified in the proposed PRC-004-3 Reliability Standard. The obligation for reporting Misoperations has been removed from PRC-004 and is being developed under the NERC Rules of Procedure, Section 1600 – Request for Data or Information.

Applicability

This standard applies to the following functional entities:

- Transmission Owner
- Generator Owner
- Distribution Provider

This standard applies to the following Facilities:

- Protection Systems for BES Elements. Non-protective functions that are embedded within a Protection System are excluded. Protective functions intended to operate as a control function during switching are excluded.
- Underfrequency load shedding (UFLS) that is intended to trip one or more BES Elements.

Effective Dates of New or Revised Standards and Definitions

~~Except in the Western Interconnection, the~~ The standard, the revised definition of "Misoperation" and ~~definitions~~the new definition of "Composite Protection System" shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. ~~Except in the Western Interconnection, where~~Where approval by an applicable governmental authority is not required, the standard, the revised definition of "Misoperation" and ~~definitions~~the new definition of "Composite Protection System" shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

~~In the Western Interconnection, the standard and definitions shall become effective on the first day of the first calendar quarter that is twenty-four months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In the Western Interconnection, where approval by an applicable governmental authority is not required, the standard and definitions shall become effective on the first day of the first calendar quarter that is twenty-four months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.~~

~~Implementation Plan for PRC-004-3, All Requirements~~

~~Each Transmission Owner, Generator Owner, and Distribution Provider applicable to this standard shall be 100% compliant upon the effective date of the standard.~~

~~The extended implementation for the Western Interconnection is provided to allow an opportunity to make the necessary changes to the PRC-004-WECC-1 Regional Reliability Standard. An overlap in performance between the regional and proposed continent-wide standard was identified during the development of the proposed PRC-004-3 Reliability Standard.~~

~~**Implementation Plan for definitions**~~

~~The revised definition of Misoperation and the new definition of Composite Protection System shall be implemented concurrently with the standard upon the effective dates noted above. Note that the Western Interconnection has an extended implementation.~~

Retirement of Existing Standards

~~Except in the Western Interconnection, the~~The existing standards, PRC-003-1 and PRC-004-2.1a, shall be retired at midnight of the day immediately prior to the ~~effective date~~Effective Date of PRC-004-3.~~ In the Western Interconnection, the existing standards PRC-003-1 and PRC-004-2.1a shall be retired at midnight of the day immediately prior to the effective date of PRC-004-3 for the Western Interconnection.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document

Project 2010-05.1 Protection Systems: Phase 1 (Misoperations)

Revisions or Retirements to Already Approved Standards

This mapping document shows the translation of PRC-003-1 – Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems and PRC-004-2.1a – Analysis and Mitigation of Transmission and Generation Protection System Misoperations into the proposed PRC-004-3 – Protection System Misoperation Identification and Correction Reliability Standard. The following table identifies the sections of the approved standard that shall be added, retired, or revised when this standard is implemented. If the standard drafting team is recommending revisions to the standard, those changes are identified in the "~~Proposed Replacement~~Translation to PRC-004-3 or Other Action" column.

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
4. Applicability: **4.1.** Regional Reliability Organization	**4. Applicability:** **4.1. Functional Entities:** **4.1.1** Transmission Owner **4.1.2** Generator Owner **4.1.3** Distribution Provider	The proposed standard properly assigns responsibility to the registered entity functions that are responsible for Protection System Misoperation identification and correction. The Transmission Owner, Generator Owner, and Distribution Provider, by function, are Protection System asset owners and are in the best position be aware of and apply resources to review Protection System operations.

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
R1. Each Regional Reliability Organization shall establish, document and maintain its procedures for, review, analysis, reporting and mitigation of transmission and generation Protection System Misoperations. These procedures shall include the following elements:		The Requirements in the proposed PRC-004-3 standard by their results-based standard (RBS) construction requires performance that is implicit of having procedures for the analysis of Protection System operations (R1, R2, R3, and R4) and mitigation of identified Misoperations (R5 and R6). The proposed requirements also ~~direct~~directs focus to areas most important to reliability. For example, Requirement R1 requires the applicable entity to initiate a review upon a Bulk Electric System (BES) interrupting device operation and identify any Misoperation. Requirement R2 requires the applicable entity to notify all other owners that share a Misoperation identification responsibility of the Composite Protection System when it determines (or is unsure) its Protection System ~~components~~component(s) did not cause the BES interrupting device operation or it cannot rule out a Misoperation. Requirement R3 requires the notified entity to identify any Misoperation of its Protection System component(s) similar to Requirement

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
		R1. Requirement R4 directs the applicable entity to continue its investigative work to determine the cause(s) of an identified Misoperation, if not determined in R1 or R3, until the cause(s) is determined or the entity ~~concludes~~declares that it is unable to determine the cause. Requirements R5 and R6 for developing and implementing a Corrective Action Plan (CAP) are also implicit of having a documented procedure. The implicit performance required by Requirements R1 through R6 necessitate that an entity have procedures to accomplish the objectives of the proposed standard. Requiring the applicable entities to have procedures is an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES.
R1.1. The Protection Systems to be reviewed and analyzed for Misoperations (due to	**4.2.** Facilities: **4.2.1** Protection Systems for BES Elements~~.~~, with the following exclusions:	The previous PRC-003-1, Requirement R1.1 required the Regional Reliability Organization (RRO) to identify the Protection Systems to be reviewed and analyzed for Misoperation.

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
their potential impact on BES reliability).	**4.2.1.1** Non-protective functions that are embedded within a Protection System ~~are excluded.~~ . **4.2.1.2** Protective functions intended to operate as a control function during switching ~~are excluded.~~. **4.2.1.3** Special Protection Systems (SPS). **4.2.1.4** Remedial Action Schemes (RAS). **4.2.2** Underfrequency load shedding (UFLS) that is intended to trip one or more BES Elements.	The applicable Facilities have been clarified in the proposed PRC-004-3 to include Protection Systems for BES Elements. Additional language is provided for clarity that non-protective functions ~~are not applicable~~ and those protective functions that are intended to operate as a control function (e.g., a reverse power relay operated to remove a generating unit from service~~). The~~ as opposed to providing anti-motoring protection) are not applicable. The standard's Applicability is further clarified to include underfrequency load shedding (UFLS) that is intended to trip one or more BES Elements to be more precise. Protection Systems associated with Special Protection Systems (SPS) and Remedial Action Schemes (RAS) are excluded and will be addressed in phase two of this project and have been excluded in the Applicability.
(Continued) **R1.1.** The Protection Systems to be reviewed and analyzed	**R1.** Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that	The applicable entities will be required to identify whether a Misoperation occurred for each BES interrupting device operation which meet criteria 1.1

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
for Misoperations (due to their potential impact on BES reliability).	operated shall, within 120 calendar days of the BES interrupting device operation, identify whether its Protection System component(s) caused a Misoperation ~~when~~under the following circumstances: **1.1** The BES interrupting device operation was caused by a Protection System or by manual intervention in response to a Protection System failure to operate; and **1.2** The BES interrupting device owner owns all or part of the Composite Protection System; and **1.3** The BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation.	through 1.3. Requirement R1 is most clearly the direct carryover from the PRC-003-1 Reliability Standard which involves the "owner" of the Protection System. The previous standard was silent on the responsibilities of other Protection System owners and had no provision for ensuring that other owners had a responsibility to be involved in the review and analysis.

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
(Continued) **R1.1.** The Protection Systems to be reviewed and analyzed for Misoperations (due to their potential impact on BES reliability).	**R2.** ~~Each~~ Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, ~~notify the other owner(s) of the Protection System of the operation when:~~provide notification as described in 2.1 and 2.2. **2.1** When a BES interrupting device operation by a Composite Protection System, notification of the operation shall be provided to the other owner(s) that share Misoperation identification responsibility for the Composite Protection System under the following circumstances: **2.1.1** The BES interrupting device owner shares the Composite Protection	Requirement R2 ~~now~~ asserts a responsibility on the initiating entity (i.e., BES interrupting device owner) to notify other owners of the Composite Protection System when the cause of a Protection System operation was not caused (or is undetermined) by the BES interrupting device owner and a Misoperation occurred (or cannot be ruled out) in accordance with ~~criteria~~Part 2.1, including sub-parts 2.1.1 through 2.1.3.

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
	System ownership with any other entity; and **2.1.2** The BES interrupting device owner has determined that a Misoperation occurred or cannot rule out a Misoperation; and **2.1.3** ~~**2.3**~~ The BES interrupting device owner has determined that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation. **2.2** For a BES interrupting device operation by a Protection System	(Part 2.2) Since Requirement R1 initiates the reliability activity upon the operation of a BES interrupting device, Requirement R1 does not address the case of a Protection System failure where a remote BES interrupting device operates. The second Part 2.2 of Requirement R2 is a provision to require notification to the other owners when a remote BES interrupting device owner in performing Requirement R1 determines that it's Protection System

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
	component intended to operate as backup protection for a condition on another entity's Element, notification of the operation shall be provided to the other Protection System owner(s) for which that backup protection was provided.	operated as backup for another BES interrupting device which has most likely failed to operate. Part 2.2 requires the other owner for which backup protection was provided to be notified, thus initiating the reliability activity to identify a possible Misoperation under Requirement R3 for the other owner.
(Continued) **R1.1.** The Protection Systems to be reviewed and analyzed for Misoperations (due to their potential impact on BES reliability).	**R3.** Each Transmission Owner, Generator Owner, and Distribution Provider that receives notification, pursuant to Requirement R2 shall, within the later of 60 calendar days of notification or 120 calendar days of the BES interrupting device(s) operation, ~~shall~~ identify whether its Protection System component(s) caused a Misoperation.	Requirement R3 places responsibility on the applicable entity that receives notification to review its Protection System component(s) for Misoperations similar to Requirement R1. It is common practice for the BES interrupting device owner that initiates the review to be in communication and collaboration with other Protection System component(s) owners during its review ~~with~~within the 120 calendar day period. The shorter 60 calendar day period for the notified entity assures that in the rare case where the notifying entity takes the majority of its allotted time (120 days) to review an operation, the receiving entity will always have

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
		a minimum and reasonable time (60 days) to conduct its review.
(Continued) **R1.1.** The Protection Systems to be reviewed and analyzed for Misoperations (due to their potential impact on BES reliability).	**R4.** Each Transmission Owner, Generator Owner, and Distribution Provider that has not determined the cause(s) of a Misoperation, for a Misoperation identified in accordance with Requirement R1 or R3, shall perform investigative action(s) to determine the cause of the Misoperation at least once every two full calendar quarters after the Misoperation was first identified, until one of the following completes the investigation: • The identification of the cause(s) of the Misoperation; or • A declaration that no cause was identified.	Requirement R4 is essentially a new requirement to determine the cause(s) of a Misoperation where the previous requirements (i.e., R1 or R3) failed to reveal the cause(s) of a Misoperation. In most cases, the cause(s) of a Misoperation will be revealed during the course of review and when ~~a~~the cause(s) is not readily apparent, the applicable entity is required in Requirement R4 to conduct at least one investigative action every two full calendar quarters until the entity determines the cause(s) or declares that it ~~has taken reasonable action and~~ could not determine the cause.

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
R1.2. Data reporting requirements (periodicity and format) for Misoperations.	None.	NERC Rules of Procedure, Section 1600 Request for Information or Data will replace the reporting obligations of applicable entities. As such, Regional reporting will end and continent-wide single reporting to the Electric Reliability Organization (ERO) will be required. The ERO will analyze the data to: develop meaningful metrics; identify trends in Protection System performance that negatively impact reliability; identify remediation techniques; and publicize lessons learned for the industry. Metrics will be shared with each Region. The removal of the data collection from the standard does not result in a reduction of reliability.
R1.3. Process for review, analysis follow up, and documentation of Corrective Action Plans for Misoperations.	**R5.** Each Transmission Owner, Generator Owner, and Distribution Provider that owns the Protection System component(s) that caused the Misoperation shall, within 60 calendar days of first identifying a cause of the Misoperation:	The proposed PRC-004-3, Requirement R5 provides a step not apparent in the previous PRC-003-1 which is the development of a Corrective Action Plan (CAP) within 60 calendar days of first identifying the Misoperation cause. Requirement R5 also requires each applicable entity to perform an evaluation of the CAP's applicability to the entity's other Protection Systems, including those at other locations.

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
	• Develop a Corrective Action Plan (CAP) for the identified Protection System component(s), and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations, or • Explain in a declaration why corrective actions are beyond the entity's control or would not improve BES reliability, and that no further corrective actions will be taken.	Furthermore, Requirement R5 accounts for those cases why corrective actions are beyond the entity's control or would not improve BES reliability and that no further corrective actions will be taken. This could be a result of a cause created by a non-registered third party, such as a communication provider. Also, should implementing the changes not improve BES reliability, the entity may document this as well~~.~~ and not make a change. In cases where the entity, in its judgment, determines that a CAP is not practical for improving BES reliability, the entity must explain in a declaration its conclusions why no further action will be taken.
(Continued) **R1.3.** Process for review, analysis follow up, and documentation of Corrective Action Plans for Misoperations.	**R6.** Each Transmission Owner, Generator Owner, and Distribution Provider shall implement each CAP developed in Requirement R5, and update each CAP if actions or timetables change, until completed.	Requirement R6 requires the implementation of the CAP. The applicable entity must update the CAP if actions or timetables change until the CAP is completed.

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
R1.4. Identification of the Regional Reliability Organization group responsible for the procedures and the process for approval of the procedures.	None.	The proposed PRC-004-3 now requires the applicable entities (GO, DP, and TO) to individually address Misoperations of its Protection ~~System~~Systems for BES Elements without regard to the Region or Regions in which it owns Protection Systems for BES Elements. The proposed PRC-004-3 Reliability Standard ~~and~~, revised definition of "Misoperation," and new definition of "Composite Protection System" provide sufficient clarity to entities; therefore, there is no reliability benefit to obtain the Regional Entity's (formerly Regional Reliability Organization or RRO) approval. Each applicable entity will be measured on its performance with the proposed PRC-004-3 requirements.
R2. Each Regional Reliability Organization shall maintain and periodically update documentation of its procedures for review, analysis, reporting, and mitigation of transmission	**4. Applicability:** **4.1. Functional Entities:** **4.1.1** Transmission Owner **4.1.2** Generator Owner **4.1.3** Distribution Provider	The proposed PRC-004-3 implicitly requires each applicable entity to have its own procedures and processes; therefore, there is no need to have a specific requirement for dictating the updating of such procedures or processes by the previous Regional Reliability Organization (now Regional Entity) or applicable entities. Requiring the applicable entities to

Standard: PRC-003-1 - Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
and generation Protection System Misoperations.		update procedures is an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES.
R3. Each Regional Reliability Organization shall distribute procedures in Requirement 1 and any changes to those procedures, to the affected Transmission Owners, Distribution Providers that own transmission Protection Systems, and Generator Owners within 30 calendar days of approval of those procedures.	None.	The proposed PRC-004-3 implicitly requires each applicable entity to have its own procedures and processes; therefore, there is no longer a need to distribute such procedures or processes by the previous Regional Reliability Organization (now Regional Entity) or applicable entities. Requiring the applicable entities to distribute procedures is an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES.

Standard: PRC-004-2.1a - Analysis and Mitigation of Transmission and Generation Protection System Misoperations		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
4. Applicability: **4.1.** Transmission Owner **4.2.** Distribution Provider that owns a transmission Protection System **4.3.** Generator Owner	**4. Applicability:** **4.1. Functional Entities:** **4.1.1** Transmission Owner **4.1.2** Generator Owner **4.1.3** Distribution Provider **4.2.** Facilities: **4.2.1** Protection Systems for BES Elements~~.~~, with the following exclusions: **4.2.1.1** Non-protective functions that are embedded within a Protection System ~~are excluded.~~ . **4.2.1.2** Protective functions intended to operate as a control function during switching ~~are excluded.~~. **4.2.1.3** Special Protection Systems (SPS).	The same applicable entities will transition to the new PRC-004-3 standard. The clause about the Distribution Provider "*that owns a transmission Protection System*" has been removed because it was ambiguous. This clause is replaced by "*Protection Systems for BES Elements*" found in Section 4.2, Facilities and applies to all the applicable entities. Having the Applicability section address Facilities specifically removes the ambiguity of what a "*transmission Protection System*" includes. The proposed PRC-004-3 standard is specific that it includes those Protection Systems for BES Elements, including UFLS that is intended to trip one or more BES Elements. Additional language is provided for clarity that non-protective functions ~~are not applicable~~ and those protective functions that are intended to operate as a control function (e.g., a reverse power relay operated to remove a generating unit from service~~).~~) are not applicable. Protection Systems associated with Special Protection Systems (SPS) and Remedial Action

Standard: PRC-004-2.1a - Analysis and Mitigation of Transmission and Generation Protection System Misoperations		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
	4.2.1.4 Remedial Action Schemes (RAS). **4.2.2** Underfrequency load shedding (UFLS) that is intended to trip one or more BES Elements.	Schemes (RAS) are addressed in phase two of this project~~.~~ and have been excluded in the Applicability.
R1. The Transmission Owner and any Distribution Provider that owns a transmission Protection System shall each analyze its transmission Protection System Misoperations and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Entity's procedures.	**R1.** Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, identify whether its Protection System component(s) caused a Misoperation ~~when~~under the following circumstances: **1.1** The BES interrupting device operation was caused by a Protection System or by manual intervention in response to a Protection System failure to operate; and **1.2** The BES interrupting device owner owns all or part of the Composite Protection System; and	The ~~already~~currently approved standard PRC-004-2.1a, Requirements R1 and R2 include three levels of performance which is analyze (Protection System operations), develop (CAP), and implement (CAP). The proposed standard, which includes the same three applicable entities (DP, GO, and TO), divides the three levels of performance into six discrete Requirements. Requirement R1 provides the "analyze" portion, requiring the initiating BES interrupting device owner to review its Protection System for each BES interrupting device operation that meets the three criteria (i.e., 1.1 thorough 1.3). The "analyze" portion is further clarified in the proposed Requirement R2 by ensuring that any other owners of the Composite Protection System are

Standard: PRC-004-2.1a - Analysis and Mitigation of Transmission and Generation Protection System Misoperations		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
R2. The Generator Owner shall analyze its generator and generator interconnection Facility Protection System Misoperations, and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Entity's procedures.	The BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation. **R2.** ~~Each~~ Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, ~~notify the other owner(s) of the Protection System of the operation when:~~provide notification as described in 2.1 and 2.2. **2.1** When a BES interrupting device operation by a Composite Protection System, notification of the operation shall be provided to the other owner(s) that share Misoperation identification responsibility for the Composite Protection System under the following circumstances:	notified when the cause of a Protection System operation was not caused (or is undetermined) by the BES interrupting device owner and a Misoperation occurred (or cannot be ruled out) in accordance with criteria 2.1 through 2.3. Requirement R3 provides the necessary performance for the notified Protection System owner to review its component(s) for Misoperation. Last, Requirement R4 requires the applicable entity to conduct investigative actions until ~~is~~it determines the cause(s) or declares that it has been unable to determine the cause(s). Requirement R5 addresses the "develop" a Corrective Action Plan (CAP)" portion, and Requirement R6 addresses the "implement" portion of the CAP.

Standard: PRC-004-2.1a - Analysis and Mitigation of Transmission and Generation Protection System Misoperations		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
	2.1.1 The BES interrupting device owner shares the Composite Protection System ownership with any other entity; and **2.1.2** The BES interrupting device owner has determined that a Misoperation occurred or cannot rule out a Misoperation; and **2.1.3** The BES interrupting device owner has determined that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation.	

Standard: PRC-004-2.1a - Analysis and Mitigation of Transmission and Generation Protection System Misoperations		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
	2.2 For a BES interrupting device operation by a Protection System component intended to operate as backup protection for a condition on another entity's Element, notification of the operation shall be provided to the other Protection System owner(s) for which that backup protection was provided. **R3.** Each Transmission Owner, Generator Owner, and Distribution Provider that receives notification, pursuant to Requirement R2 shall, within the later of 60 calendar days of notification or 120 calendar days of the BES interrupting device(s) operation, ~~shall~~ identify whether its Protection System component(s) caused a Misoperation. **R4.** Each Transmission Owner, Generator Owner, and Distribution Provider that has not determined the cause(s) of a	

Standard: PRC-004-2.1a - Analysis and Mitigation of Transmission and Generation Protection System Misoperations		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
	Misoperation, for a Misoperation identified in accordance with Requirement R1 or R3, shall perform investigative action(s) to determine the cause of the Misoperation at least once every two full calendar quarters after the Misoperation was first identified, until one of the following completes the investigation: • The identification of the cause(s) of the Misoperation; or • A declaration that no cause was identified. **R5.** Each Transmission Owner, Generator Owner, and Distribution Provider that owns the Protection System component(s) that caused the Misoperation shall, within 60 calendar days of first identifying a cause of the Misoperation: • Develop a Corrective Action Plan (CAP) for the identified Protection System	

Standard: PRC-004-2.1a - Analysis and Mitigation of Transmission and Generation Protection System Misoperations		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
	component(s), and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations, or • Explain in a declaration why corrective actions are beyond the entity's control or would not improve BES reliability, and that no further corrective actions will be taken. **R6.** Each Transmission Owner, Generator Owner, and Distribution Provider shall implement each CAP developed in Requirement R5, and update each CAP if actions or timetables change, until completed.	
R3. The Transmission Owner, any Distribution Provider that owns a transmission Protection System, and the Generator Owner shall each provide to its	None.	Since the NERC Rules of Procedure, Section 1600 Request for Data or Information ~~or Data~~ will replace the reporting obligations~~.~~, NERC will receive the data on a periodic basis, analyze, establish metrics, and share results accordingly with the Regional Entities as well as industry. Having reporting obligations as a

Standard: PRC-004-2.1a - Analysis and Mitigation of Transmission and Generation Protection System Misoperations		
Requirement in Approved Standard	**Translation to PRC-004-3 or Other Action**	**Comments**
Regional Entity, documentation of its Misoperations analyses and Corrective Action Plans according to the Regional Entity's procedures.		Requirement is an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. The SC authorized moving the SAR forward for standard development at their June 9, 2011 meeting.
2. The SAR was posted for informal comment June 10 – July 11, 2011.
3. Draft 1 of PRC-004-3 was posted for a 30-day formal comment period from June 10 – July 11, 2011.
4. Draft 2 of PRC-004-3 was posted for a 45-day formal comment period from July 25 – September 7, 2012 and an initial ballot in the last ten days of the comment period from August 29 – September 7, 2012.
5. Draft 3 of PRC-004-3 was posted for a 30-day formal comment period from January 22 – February 20, 2013 and a successive ballot in the last ten days of the comment period from February 11-20, 2013.
6. Draft 4 of PRC-004-3 was posted for a 45-day additional comment period from January 17 – March 11, 2014 and an additional ballot in the last ten days of the comment period from February 2 – March 11, 2014 under the new Standards Process Manual (Effective: June 26, 2013).

Description of Current Draft

The Protection System Misoperations Standard Drafting Team (PSMSDT) is posting Draft 45 of PRC-004-3 – Protection System Misoperation Identification and Correction for a 45-day additional comment period and additional ballot in the last ten days of the comment period under the new Standards Process Manual (Effective: June 26, 2013).

Anticipated Actions	Anticipated Date
Additional 45-day Formal Comment Period with Parallel Ballot	~~January~~May 2014
10-day Final Ballot	~~March~~July 2014
BOT Approval	~~May~~August 2014

Effective Dates

~~Except in the Western Interconnection, the~~ The standard, the revised definition of "Misoperation" and ~~definitions~~the new definition of "Composite Protection System" shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. ~~Except in the Western Interconnection, where~~Where approval by

an applicable governmental authority is not required, the standard, the revised definition of "Misoperation" and ~~definitions~~the new definition of "Composite Protection System" shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

~~In the Western Interconnection, the standard and definitions shall become effective on the first day of the first calendar quarter that is twenty-four months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In the Western Interconnection, where approval by an applicable governmental authority is not required, the standard and definitions shall become effective on the first day of the first calendar quarter that is twenty-four months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.~~

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/06
2		Modified to address Order No. 693 Directives contained in paragraph 1469.	Revised
2	August 5, 2010	Adopted by NERC Board of Trustees	
1a	February 17, 2011	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers	Project 2009-17 interpretation
1a	February 17, 2011	Adopted by the Board of Trustees	
1a	September 26, 2011	FERC Order issued approving the interpretation of R1 and R3 (FERC's	

		Order is effective as of September 26, 2011)	
2a	September 26, 2011	Appended FERC-approved interpretation of R1 and R3 to version 2	
2.1a		Errata change: Edited R2 to add "…and generator interconnection Facility…"	Revision under Project 2010-07
2.1a	February 9, 2012	Errata change adopted by the Board of Trustees	
2.1a	September 19, 2013	FERC Order issued approving PRC-004-2.1a (approval becomes effective November 25, 2013).	
~~1~~3	TBD	~~Project 2010-05.1 – Protection Systems: Phase 1 (Misoperations)~~Adopted by Board of Trustees	~~New~~Revision under Project 2010-05.1

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the *Glossary of Terms used in NERC Reliability Standards* ("NERC Glossary") are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the ~~glossary~~NERC Glossary.

Composite Protection System:

The total complement of ~~the~~ Protection System(s) that function collectively to protect an Element~~, such as any primary, secondary, local backup, and communication-assisted relay systems.~~. Backup protection provided ~~by~~to a remote Protection System is ~~excluded~~included.

Misoperation:

The failure of a Composite Protection System to operate as intended~~.~~ for protection purposes. Any of the following is a Misoperation:

1. **Failure to Trip – During Fault** – A failure of a Composite Protection System to operate for a Fault condition for which it is designed. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.
2. **Failure to Trip – Other Than Fault** – A failure of a Composite Protection System to operate for a non-Fault condition for which it is designed, such as a power swing, undervoltage, overexcitation, or loss of excitation. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.
3. **Slow Trip – During Fault** – A Composite Protection System operation that is slower than required for a Fault condition ~~for which it is designed. Delayed clearing~~if the duration of ~~a Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or~~its operating time resulted in the operation of ~~any~~at least one other Element's Composite Protection System.
4. **Slow Trip – Other Than Fault** – A Composite Protection System operation that is slower than required for a non-Fault condition ~~for which it is designed~~, such as a power swing, undervoltage, overexcitation, or loss of excitation~~. Delayed clearing~~, if the duration of ~~a non-Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or~~its operating time resulted in the operation of ~~any~~at least one other Element's Composite Protection System.
5. **Unnecessary Trip – During Fault** – An unnecessary Composite Protection System operation for a Fault condition on another Element.
6. **Unnecessary Trip – Other Than Fault** – An unnecessary Composite Protection System operation for a non-Fault condition ~~for which it is not designed. A.~~ A Composite Protection System operation that is caused by personnel during on-site maintenance, testing, inspection, construction, or commissioning activities is not a Misoperation.

When this standard has received ballot approval, the ~~text~~rationale boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** **Protection System Misoperation Identification and Correction**

2. **Number:** PRC-004-3

3. **Purpose:** Identify and correct the causes of Misoperations of Protection Systems for Bulk Electric System (BES) Elements.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Transmission Owner

   4.1.2 Generator Owner

   4.1.3 Distribution Provider

   4.2. Facilities:

   4.2.1 Protection Systems for BES Elements~~. Non-protective functions that are embedded within a Protection System are excluded. Protective functions intended to operate as a control function during switching are excluded.[1]~~, with the following exclusions:

   4.2.1.1 Non-protective functions that are embedded within a Protection System.

   4.2.1.2 Protective functions intended to operate as a control function during switching.[2]

   4.2.1.3 Special Protection Systems (SPS).

   4.2.1.4 Remedial Action Schemes (RAS).

   4.2.2 Underfrequency load shedding (UFLS) that is intended to trip one or more BES Elements.

Rationale for Applicability: Protection Systems that protect BES Elements are integral to the operation and reliability of the BES. Some functions of relays are not used as protection but as control functions or for automation; therefore, any operation of the control function portion or the automation portion of relays is excluded from this standard. See the Application Guidelines for detailed examples of non-protective functions. Special Protection Systems (SPS) and Remedial Action Schemes (RAS) are ~~not included~~excluded in this standard because they are planned to be handled in the second phase of this project.

[1] ~~For additional information and examples, see the "Non-Protective Functions" and "Control Functions" sections in the Application Guidelines.~~

[2] For additional information and examples, see the "Non-Protective Functions" and "Control Functions" sections in the Application Guidelines.

5. Background:

A key ~~element~~factor for BES reliability is the correct performance of Protection Systems. The monitoring of Protection System events for BES Elements, as well as identifying and correcting the causes of Misoperations, will improve Protection System performance. This Reliability Standard PRC-004-3 – Protection System Misoperation Identification and Correction is a revision of PRC-004-2.1a – Analysis and Mitigation of Transmission and Generation Protection System Misoperations. The Reliability Standard PRC-003-1 – Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems requires Regional Entities to establish procedures for analysis of Misoperations. In the FERC Order No. 693, the Commission identified PRC-003-0 as a "fill-in-the-blank" standard. The Order stated that because the regional procedures had not been submitted, the Commission proposed not to approve or remand PRC-003-0. Because PRC-003-0 (now PRC-003-1) is not enforceable, there is not a mandatory requirement for Regional Entity procedures to support the requirements of PRC-004-2.1a. This is a potential reliability gap; consequently, PRC-004-3 combines the reliability intent of the two legacy standards PRC-003-1 and PRC-004-2.1a.

This project includes revising the existing definition of Misoperation, which reads:

Misoperation

- Any failure of a Protection System element to operate within the specified time when a fault or abnormal condition occurs within a zone of protection.
- Any operation for a fault not within a zone of protection (other than operation as backup protection for a fault in an adjacent zone that is not cleared within a specified time for the protection for that zone).
- Any unintentional Protection System operation when no fault or other abnormal condition has occurred unrelated to on-site maintenance and testing activity.

In general, this definition needs more specificity and clarity. The terms "specified time" and "abnormal condition" are ambiguous. In the third bullet, more clarification is needed as to whether an unintentional Protection System operation for an atypical yet explainable condition is a Misoperation.

The SAR for this project also includes clarifying reporting requirements. Misoperation data, as currently collected and reported, is not optimal to establish consistent metrics for measuring Protection System performance. As such, the data reporting obligation for this standard is being removed and is being developed under the NERC Rules of Procedure, Section 1600 – Request for Data or Information ("data request"). As a result of the data request, NERC will analyze the data to: develop meaningful metrics; identify trends in Protection System performance that negatively impact reliability; identify remediation techniques; and publicize lessons learned for the industry. The removal of the data collection obligation from the standard does not result in a reduction of reliability. The standard and data request have been developed in a manner such that evidence used for

compliance with the standard and data request are intended to be independent of each other.

The proposed requirements of the revised Reliability Standard PRC-004-3 meet the following objectives:

- Review all Protection System operations on the BES to identify those that are Misoperations of Protection Systems for Facilities that are part of the BES.
- Analyze Misoperations of Protection Systems for Facilities that are part of the BES to identify the cause(s).
- Develop and implement Corrective Action Plans to address the cause(s) of Misoperations of Protection Systems for Facilities that are part of the BES.

Misoperations associated with Special Protection Schemes (SPS) and Remedial Action Schemes (RAS) are not addressed in this standard due to their inherent complexities. NERC plans to handle SPS and RAS in the second phase of this project.

The Western Electric Coordinating Council (WECC) Regional Reliability Standard PRC-004-WECC-1 – Protection System and Remedial Action Scheme Misoperation relates to the reporting of Misoperations of Protection Systems and RAS for a limited set of WECC Paths. The WECC region plans to conduct work to harmonize the regional standard with this continent-wide proposed standard and the second phase of this project concerning SPS and RAS.

6. Effective Dates: ~~See Implementation Plan~~

The standard shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

R1. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, identify whether its Protection System component(s) caused a Misoperation ~~when~~under the following circumstances: *[Violation Risk Factor: Medium][Time Horizon: Operations Assessment, Operations Planning]*

1.1 The BES interrupting device operation was caused by a Protection System or by manual intervention in response to a Protection System failure to operate; and

1.2 The BES interrupting device owner owns all or part of the Composite Protection System; and

1.3 The BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation.

~~**M1.**~~ **M1.** Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it identified the Misoperation of its Protection System component(s), if any, that meet the circumstances in Requirement R1, Parts 1.1, 1.2, and 1.3 within the allotted time period. Acceptable evidence for Requirement R1, including Parts 1.1, 1.2, and 1.3 may include, but is not limited to~~,~~ the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

Rationale for R1: This requirement ensures that entities review those Protection System operations meeting the ~~criteria~~circumstances in all three Parts (1.1, 1.2, and 1.3) and identify any that are Misoperations. The BES interrupting device owner ~~has~~is assigned the responsibility to initiate the review because the owner is in the best position to be aware of the operation. Manual intervention is included as a condition that initiates a review. Occasionally, Protection System failures do not yield other Protection System operations and manual intervention is required to isolate the problematic equipment. The 120 calendar day period accounts for the sporadic volumes of Protection System operations, and provides the opportunity to identify any Misoperations which were initially missed.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, ~~notify the other owner(s) of the Protection System of the operation when:~~provide notification as described in 2.1 and 2.2. *[Violation Risk Factor: Medium][Time Horizon: Operations Assessment, Operations Planning]*

~~2~~**2.1** For a BES interrupting device operation by a Composite Protection System, notification of the operation shall be provided to the other owner(s) that share Misoperation identification responsibility for the Composite Protection System under the following circumstances:

2.1.1 The BES interrupting device owner shares the Composite Protection System ownership with any other ~~entity~~owner; and

2.1.2 The BES interrupting device owner has determined that a Misoperation occurred or cannot rule out a Misoperation; and

2.1.3 The BES interrupting device owner has determined that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation.

2.2 For a BES interrupting device operation by a Protection System component intended to operate as backup protection for a condition on another entity's Element, notification of the operation shall be provided to the other Protection System owner(s) for which that backup protection was provided.

M2. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates notification to the other owner(s), within the allotted time period for either Requirement R2, Part 2.1, including subparts 2.1.1, 2.1.2, and 2.1.3 and Requirement R2, Part 2.2. Acceptable evidence for Requirement R2, including Parts 2.1~~, 2.2,~~ and 2.~~3~~2 may include, but is not limited to~~,~~ the following dated documentation (electronic or hardcopy format): emails, facsimiles, or transmittals.

Rationale for R2: ~~This requirement~~Part 2.1 ensures that the BES interrupting device owner notifies the other owners of the Composite Protection System ~~when the criteria in all three Parts (2.1, 2.2, and 2.3) are met~~. The phrase "owner(s) that share Misoperation identification responsibility" allows entities to notify the specific others that will actually review the operation to determine if a Misoperation occurred. Part 2.2 ensures that the Protection System owner(s) for which that backup protection was provided receives notification, within the same 120 calendar day period as R1. This ensures other entities are notified to review their Protection System components. The expectation is that entities will communicate accordingly and when it is clear that ~~the three conditions~~when Part 2.1, 2.2, or both are met, the entity would make the notification. It is not intended for entities to automatically and unnecessarily notify other entities before adequate detail is known.

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that receives notification, pursuant to Requirement R2 shall, within the later of 60 calendar days of notification or 120 calendar days of the BES interrupting device(s) operation, ~~shall~~ identify whether its Protection System component(s) caused a Misoperation. *[Violation Risk Factor: Medium][Time Horizon: Operations Assessment, Operations Planning]*

M3. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it identified whether its Protection System component(s) caused a Misoperation within the allotted time period. Acceptable evidence for Requirement R3 may include, but is not limited to~~,~~ the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

Rationale for R3: When an entity receives notification of a Protection System operation by the BES interrupting device owner, the Protection System owner is allotted at least 60 calendar days to identify whether it was a Misoperation. A shorter time period is allotted on the basis that the BES interrupting device owner has already performed preliminary work, collaborated with the other owners, and that other owners generally have fewer associated Protection System components.

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that has not determined the cause(s) of a Misoperation, for a Misoperation identified in accordance with Requirement R1 or R3, shall perform investigative action(s) to determine the cause of the Misoperation at least once every two full calendar quarters after the Misoperation was first identified, until one of the following completes the investigation: *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment, Operations Planning]*

- The identification of the cause(s) of the Misoperation; or
- A declaration that no cause was identified.

M4. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it performed at least one investigative action according to Requirement R4 every two full calendar quarters until a cause is identified or a declaration is made. Acceptable evidence for Requirement R4 may include, but is not limited to~~,~~ the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

Rationale for R4: If a Misoperation cause is not identified within the time period established by Requirements R1 or R3 (i.e., 120 calendar days), the Protection System component owner must demonstrate investigative actions toward identifying the cause(s). Performing at least one action every two full calendar quarters from first identifying the Misoperation encourages periodic focus on finding the cause of the Misoperation.

R5. Each Transmission Owner, Generator Owner, and Distribution Provider that owns the Protection System component(s) that caused the Misoperation shall, within 60 calendar days of first identifying a cause of the Misoperation: [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning, Long-Term Planning*]

- Develop a Corrective Action Plan (CAP) for the identified Protection System component(s), and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations~~,~~; or
- Explain in a declaration why corrective actions are beyond the entity's control or would not improve BES reliability, and that no further corrective actions will be taken.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it developed a CAP and an evaluation of the CAP's applicability to other Protection Systems and locations, or a declaration in accordance with Requirement R5. Acceptable evidence for Requirement R5 may include, but is not limited to~~,~~ the following dated documentation (electronic or hardcopy format): ~~a dated~~ CAP and evaluation, or ~~a dated~~ declaration.

Rationale for R5: A formal CAP is a proven tool for resolving and reducing the possibility of reoccurrence of operational problems. A time period of 60 calendar days is based on industry experience and operational coordination time needed for considering such things as alternative solutions, coordination of resources, or development of a schedule. When the cause of a Misoperation is identified, a CAP will generally be developed. An evaluation of the CAP's applicability to the entity's other Protection Systems including other locations helps identify similar problems, potential for Misoperation occurrences in other Protection Systems, common mode failure, design problems, etc. In rare cases, altering the Protection System to avoid a Misoperation recurrence may lower the reliability or performance of the BES. In those cases, a statement documenting the reasons for taking no corrective actions is essential for future reference and for justifying the ~~close of the Misoperation in lieu~~absence of a CAP ~~and for future reference~~.

R6. Each Transmission Owner, Generator Owner, and Distribution Provider shall implement each CAP developed in Requirement R5, and update each CAP if actions or timetables change, until completed. *[Violation Risk Factor: Medium][Time Horizon: Operations Planning, Long-Term Planning]*

M6. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it implemented each CAP, including updating actions or timetables. Acceptable evidence for Requirement R6 may include, but is not limited to~~,~~ the following dated documentation (electronic or hard copy format): ~~dated~~ records that document the implementation of each CAP and the completion of actions for each CAP including revision history of each CAP. Evidence may also include work management program records, work orders, and maintenance records.

Rationale for R6: ~~The~~Each CAP must accomplish all identified objectives to be complete. During the course of implementing a CAP, updates may be necessary for a variety of reasons such as new information, scheduling conflicts, or resource issues. Documenting changes or completion of CAP tivities provides measurable progress and confirmation of completion.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

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

The Transmission Owner, Generator Owner, and Distribution Provider shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirements R1, R2, R3, and R4, Measures M1, M2, M3, and M4 for 12 calendar months.
- The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R5, Measure M5 for 12 calendar months following ~~completion~~development of each CAP, development of each evaluation, and development of each declaration.
- The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R6, Measure M6 for 12 calendar months following completion of each CAP.

If a Transmission Owner, Generator Owner, or Distribution Provider is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

Periodic Data Submittal

1.4. Additional Compliance Information

None**.**

D. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Assessment, Operations Planning	Medium	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 120 calendar days and less than or equal to 150 calendar days of the BES interrupting device operation.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 150 calendar days and less than or equal to 165 calendar days of the BES interrupting device operation.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 165 calendar days and less than or equal to 180 calendar days of the BES interrupting device operation.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 180 calendar days of the BES interrupting device operation. OR The responsible entity failed to identify whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Assessment, Operations Planning	Medium	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 120 calendar days and less than or equal to 150 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 150 calendar days and less than or equal to 165 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 165 calendar days and less than or equal to 180 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 180 calendar days of the BES interrupting device operation. OR The responsible entity failed to notify one or more of the other owner(s) of the Protection System component(s) in accordance with Requirement R2.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Operations Assessment, Operations Planning	Medium	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was less than or equal to 30 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 30 calendar days and less than or equal to 45 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 45 calendar days and less than or equal to 60 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 60 calendar days late. OR The responsible entity failed to identify whether or not a Misoperation of its Protection System component(s) occurred in accordance with Requirement R3.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	Operations Assessment, Operations Planning	Medium	The responsible entity performed at least one investigative action in accordance with Requirement R4, but was less than or equal to one calendar quarter late.	The responsible entity performed at least one investigative action in accordance with Requirement R4, but was greater than one calendar quarter and less than or equal to two calendar quarters late.	The responsible entity performed at least one investigative action in accordance with Requirement R4, but was greater than two calendar quarters and less than or equal to three calendar quarters late.	The responsible entity performed at least one investigative action in accordance with Requirement R4, but was more than three calendar quarters late. OR The responsible entity failed to perform investigative action(s) in accordance with Requirement R4.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Operations Planning, Long-Term Planning	Medium	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 60 calendar days and less than or equal to 70 calendar days of first identifying a cause of the Misoperation. OR (See next page)	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 70 calendar days and less than or equal to 80 calendar days of first identifying a cause of the Misoperation. OR (See next page)	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 80 calendar days and less than or equal to 90 calendar days of first identifying a cause of the Misoperation. OR (See next page)	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 90 calendar days of first identifying a cause of the Misoperation. OR The responsible entity failed to develop a CAP or explain in a declaration in accordance with Requirement R5. OR (See next page)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	(Continued)		The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 60 calendar days and less than or equal to 70 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 70 calendar days and less than or equal to 80 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 80 calendar days and less than or equal to 90 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 90 calendar days of first identifying a cause of the Misoperation. OR The responsible entity failed to develop an evaluation in accordance with Requirement R5.
R6	Operations Planning, Long-Term Planning	Medium	The responsible entity implemented, but failed to update a CAP, when actions or timetables changed, in accordance with Requirement R6.	N/A	N/A	The responsible entity failed to implement a CAP in accordance with Requirement R6.

E. Regional Variances

None.

F. Interpretations

None.

G. Associated Documents

None.

Guidelines and Technical Basis

Introduction

This standard addresses the reliability issues identified in the letter[3] from Gerry Cauley, NERC President and CEO, dated January 7, 2011.

> "Nearly all major system failures, excluding perhaps those caused by severe weather, have misoperations of relays or automatic controls as a factor contributing to the propagation of the failure. …Relays can misoperate, either operate when not needed or fail to operate when needed, for a number of reasons. First, the device could experience an internal failure – but this is rare. Most commonly, relays fail to operate correctly due to incorrect settings, improper coordination (of timing and set points) with other devices, ineffective maintenance and testing, or failure of communications channels or power supplies. Preventable errors can be introduced by field personnel and their supervisors or more programmatically by the organization."

The standard also addresses the findings in the 2011 Risk Assessment of Reliability Performance[4]; July 2011.

> "…a number of multiple outage events were initiated by protection system Misoperations. These events, which go beyond their design expectations and operating procedures, represent a tangible threat to reliability. A deeper review of the root causes of dependent and common mode events, which include three or more automatic outages, is a high priority for NERC and the industry."

Definitions

The Misoperation definition is based on the IEEE/PSRC Working Group I3 "Transmission Protective Relay System Performance Measuring Methodology[5]." Misoperations of a Protection System include failure to operate, slowness in operating, or operating when not required either during a ~~Fault~~fault or non-~~Fault~~fault condition.

[3] http://www.nerc.com/pa/Stand/Project%20201005%20Protection%20System%20Misoperations%20DL/20110209130708-Cauley%20letter.pdf
[4] http://www.nerc.com/files/2011_RARPR_FINAL.pdf
[5] "Transmission Protective Relay System Performance Measuring Methodology," Working Group I3 of Power System Relaying Committee of IEEE Power Engineering Society, 1999.

For reference, a "Protection System" is defined in the *Glossary of Terms used in NERC Reliability Standards* ("NERC Glossary") as:

- Protective relays which respond to electrical quantities,
- Communications systems necessary for correct operation of protective functions,
- Voltage and current sensing devices providing inputs to protective relays,
- Station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply), and
- Control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.

A BES interrupting device is a BES Element, typically a circuit breaker or circuit switcher that has the capability to interrupt fault current. Although BES interrupting device mechanisms are not part of a Protection System, the standard uses the operation of a BES interrupting device by a Protection System to initiate the review for Misoperation.

The following two definitions are being proposed for inclusion in the NERC Glossary:

> **Composite Protection System –** *The total complement of ~~the~~ Protection System(s) that function collectively to protect ~~a~~an Element~~, such as any primary, secondary, local backup, and communication-assisted relay systems.~~. Backup protection provided ~~by~~to a remote Protection System is ~~excluded~~included.*

The Composite Protection System definition is based on the principle that an Element's multiple layers of protection are intended to function collectively. This definition has been introduced in this standard and incorporated into the proposed definition of Misoperation to clarify that the ~~entity must consider the entire Protection System associated with the BES interrupting device that operated. Additionally, the definition accounts for those Protection Systems with multiple levels of protection (e.g., redundant systems), such that if one component fails, but the overall intended performance of the composite protection is met – it would not be identified as a Misoperation under the definition~~overall performance of an Element's total complement of protection should be considered while evaluating an operation.

Composite Protection System – Line Example

The Composite Protection System of the Alpha-Beta line (Circuit #123) is comprised of current differential, permissive overreaching transfer trip (POTT), step distance (classic zone 1, zone 2, and zone 3), instantaneous-overcurrent, time-overcurrent, out-of-step, and overvoltage protection. The protection is housed at the Alpha and Beta substations, and includes the associated relays, communications systems, voltage and current sensing devices, DC supplies, and control circuitry.

Composite Protection System – Transformer Example

The Composite Protection System of the Alpha transformer (#2) is comprised of internal differential, overall differential, instantaneous-overcurrent, and time-overcurrent protection. The protection is housed at the Alpha substation, and includes the associated relays, voltage and current sensing devices, DC supplies, and control circuitry.

Composite Protection System – Generator Example

The Composite Protection System of the Beta generator (#3) is comprised of generator differential, overall differential, overcurrent, stator ground, reverse power, volts per hertz, loss-of-field, and undervoltage protection. The protection is housed at the Beta generating plant and at the Beta substation, and includes the associated relays, voltage and current sensing devices, DC supplies, and control circuitry.

Composite Protection System – Breaker Failure Example

Breaker failure protection provides backup protection for the breaker, and therefore is part of the breaker's Composite Protection System. Considering breaker failure protection to be part of another Element's Composite Protection System could lead to an incorrect conclusion that a breaker failure operation automatically satisfies the "Slow Trip" criteria of the Misoperation definition.

Misoperation – *The failure a Composite Protection System to operate as intended for protection purposes. Any of the following is a Misoperation:*

1. **Failure to Trip – During Fault** *– A failure of a Composite Protection System to operate for a Fault condition for which it is designed. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.*
2. ***Failure to Trip – Other Than Fault*** *– A failure of a Composite Protection System to operate for a non-Fault condition for which it is designed, such as a power swing, undervoltage, overexcitation, or loss of excitation. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.*
3. ***Slow Trip – During Fault*** *– A Composite Protection System operation that is slower than required for a Fault condition ~~for which it is designed. Delayed clearing~~if the duration of ~~a Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or~~its operating time resulted in the operation of ~~any~~at least one other Element's Composite Protection System.*
4. ***Slow Trip – Other Than Fault*** *– A Composite Protection System operation that is slower than required for a non-Fault condition ~~for which it is designed~~, such as a power swing, undervoltage, overexcitation, or loss of excitation~~. Delayed clearing~~, if the duration of ~~a non-Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or~~its operating time resulted in the operation of ~~any~~at least one other Element's Composite Protection System.*
5. ***Unnecessary Trip – During Fault*** *– An unnecessary Composite Protection System operation for a Fault condition on another Element.*

6. ***Unnecessary Trip – Other Than Fault*** *– An unnecessary Composite Protection System operation for a non-Fault condition ~~for which it is not designed. A~~. A Composite Protection System operation that is caused by personnel during on-site maintenance, testing, inspection, construction, or commissioning activities is not a Misoperation.*

The Misoperation definition is based on the principle that an Element's total complement of protection is intended to operate dependably and securely.

Failure to automatically reclose after a ~~Fault~~fault condition is not included as a Misoperation because reclosing equipment is not included within the definition of Protection System.

A breaker failure operation does not, in itself, constitute a Misoperation.

A remote backup operation resulting from a "Failure to Trip" or a "Slow Trip" does not, in itself, constitute a Misoperation.

This proposed definition of Misoperation provides additional clarity over the current version. A Misoperation is the failure of a Composite Protection System to operate as intended. The definition includes six categories which provide further differentiation ~~and examples~~ of what ~~is~~constitutes a Misoperation. These categories are discussed in greater detail in the following sections.

Failure to Trip – During Fault

This category of Misoperation typically results in the ~~Fault~~fault condition being cleared by remote backup Protection System operation.

> **Example 1a:** A failure of a transformer's Composite Protection System to operate for a transformer ~~Fault~~fault is a Misoperation.
>
> **Example 1b:** A failure of a "primary" transformer relay (or any other component) to operate for a transformer ~~Fault~~fault is not a "Failure to Trip – During Fault" Misoperation as long as another component of the transformer's Composite Protection System operated ~~to clear the Fault~~.
>
> **Example 1c:** A lack of target information does not by itself constitute a Misoperation. When a high-speed pilot system does not target because a high-speed zone element trips first, it would not in and of itself be a Misoperation.
>
> **Example 1d:** A failure of an overall differential relay to operate is not a "Failure to Trip – During Fault" Misoperation as long as another component such as a generator differential relay operated.

In analyzing the Protection System for Misoperation, the entity must also consider whether the "Slow Trip – During Fault" category applies to the operation.

Failure to Trip – Other Than Fault

This category of Misoperation may have resulted in operator intervention. The "Failure to Trip – Other Than Fault" conditions cited in the definition are examples only, and do not constitute an all-inclusive list.

Example 2a: A failure of a generator's Composite Protection System to operate for an unintentional loss of field condition is a Misoperation.

Example 2b: A failure of an overexcitation relay (or any other component) is not a "Failure to Trip – Other Than Fault" Misoperation as long as ~~another component of~~ the generator's Composite Protection System operated as intended ~~(e.g.,~~ isolating the generator~~).~~ from the BES.

In analyzing the Protection System for Misoperation, the entity must also consider whether the "Slow Trip – Other Than Fault" category applies to the operation.

Slow Trip – During Fault

This category of Misoperation typically results in remote backup Protection System operation before the ~~Fault~~fault is cleared.

Example 3: A failure of a line's Composite Protection System to operate as quickly as intended for a line ~~Fault is a Misoperation~~fault is a Misoperation. The current differential element of a multiple function relay failed to operate for a line fault. The same relay's time-overcurrent element operated after a time delay. However, an adjacent line also operated from a time-overcurrent element. The faulted line's time-overcurrent element was found to be set to trip too slowly.

Installing high-speed protection may be a part of a utility's standard practice without having the need for high-speed protection to prevent voltage or dynamic instability or to maintain relay coordination. For this case, a "Slow Trip – During Fault" of the high-speed protection is not a Misoperation because it would not negatively impact the dynamic BES performance, unless the Composite Protection System operation is slower than previously identified as being necessary to prevent voltage or dynamic instability. The Composite Protection System must also coordinate with other Protection Systems to prevent the trip (e.g., an over-trip) of additional Protection Systems.

The phrase "slower than required" means the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System ~~operated slower than the objective of the owner(s).~~ It would be impractical to provide a precise tolerance in the definition that would be applicable to every type of Protection System. Rather, the owner(s) reviewing each Protection System operation should understand whether the speed and outcome of its Protection System operation met their objective. The intent is not to require documentation of exact Protection System operation times, but to assure consideration of relay coordination and stability by the owner(s) reviewing each Protection System operation.

The phrase "resulted in the operation of any other Composite Protection System" refers to the need to ensure that relaying operates in the proper or planned sequence (i.e., the primary relaying for a faulted Element operates before the remote backup relaying for the faulted Element).

In analyzing the Protection System for Misoperation, the entity must also consider the "Unnecessary Trip – During Fault" category to determine if an "unnecessary trip" applies to the Protection System operation of an Element other than the faulted Element.

If a coordination error was at the local terminal (i.e., set too slow), then it was a "Slow Trip," category of Misoperation at the local terminal.

Slow Trip – Other Than Fault

The phrase “slower than required” means the duration of its operating time resulted in the operation of at least one other Element’s Composite Protection System ~~operated slower than the objective of the owner(s).~~. It would be impractical to provide a precise tolerance in the definition that would be applicable to every type of Protection System. Rather, the owner(s) reviewing each Protection System operation should understand whether the speed and outcome of its Protection System operation met their objective. The intent is not to require documentation of exact Protection System operation times, but to assure consideration of relay coordination and stability by the owner(s) reviewing each Protection System operation.

> **Example 4:** A failure of a generator's Composite Protection System to operate as quickly as intended for an overexcitation condition is a Misoperation. ~~This category of Misoperation could result in equipment damage.~~

The “Slow Trip – Other Than Fault” conditions cited in the definition are examples only, and do not constitute an all-inclusive list.

Unnecessary Trip – During Fault

An operation of a properly coordinated remote Protection System is not in and of itself a Misoperation if the ~~Fault~~fault has persisted for a sufficient time to allow the correct operation of the Composite Protection System of the ~~Faulted~~faulted Element to clear the ~~Fault~~fault. A BES interrupting device failure, a “failure to trip” Misoperation, or a “slow trip” Misoperation may result in a proper remote Protection System operation.

> **Example 5:** An operation of a transformer's Composite Protection System which trips (i.e., over-trips) for a properly cleared line ~~Fault~~fault is a Misoperation. The ~~Fault~~fault is cleared properly by the faulted equipment's Composite Protection System (i.e., line relaying) without the need for an external Protection System operation resulting in an unnecessary trip of the transformer protection; therefore, the transformer Protection System operation is a Misoperation.

Unnecessary Trip – Other Than Fault

Unnecessary trips for non-~~Fault~~fault conditions include but are not limited to, power swings, overexcitation, loss of excitation, frequency excursions, and normal operations.

> **Example 6a:** An operation of a line's Composite Protection System due to a relay failure during normal operation is a Misoperation.
>
> **Example 6b:** Tripping a generator by the operation of the loss of field protection during an off-nominal frequency condition while the field is intact is a Misoperation assuming the Composite Protection System was not intended to operate under this condition.

Example 6c: An impedance line relay trip for a power swing that entered the relay's characteristic is a Misoperation if the power swing was stable and the relay operated because power swing blocking was enabled and should have prevented the trip, but did not.

Example 6d: Tripping a generator operating at normal load by the operation of a reverse power protection relay due to a relay failure is a Misoperation.

Additionally, an operation that occurs during a non-~~Fault~~fault condition but was initiated directly by on-site (i.e., real-time) maintenance, testing, inspection, construction, or commissioning is not a Misoperation.

Example ~~6d~~6e: A BES interrupting device operation that occurs at the remote end of a line during a non-~~Fault~~fault condition because a direct transfer trip was initiated by system maintenance and testing activities at the local end of the line is not a Misoperation.

The "on-site" activities at one location that initiates a trip to another location are included in this exemption; however, once the maintenance, testing, inspection, construction, or commissioning is complete, the "on-site" Misoperation exclusion no longer applies, regardless of the presence of on-site personnel.

If a coordination error was at the remote terminal (i.e., set too fast), then it was an "Unnecessary Trip," category of Misoperation at the remote terminal.

Special Cases

Protection System operations for these cases would not be a Misoperation.

Example 7a: A generator Protection System operation prior to closing the unit breaker(s) is not a Misoperation provided no in-service Elements are tripped.

This type of operation is not a Misoperation because the generating unit is not synchronized and is isolated from the BES. Protection System operations which occur with the protected Element out of service, that do not trip any in-service Elements, are not Misoperations.

In some cases where zones of protection overlap, the owner(s) of Elements may decide to allow a Protection System to operate faster in order to gain better overall Protection System performance for an Element.

Example 7b: The high-side of a transformer connected to a line may be within the zone of protection of the supplying line's relaying. In this case, the line relaying is planned to protect the area of the high side of the transformer and into its primary winding. In order to provide faster protection for the line, the line relaying may be designed and set to operate without direct coordination (or coordination is waived) with local protection for ~~Faults~~faults on the high-side of the connected transformer. Therefore, the operation of the line relaying for a high-side transformer ~~Fault~~fault operated as intended and would not be a Misoperation.

~~The above~~Below are examples ~~only, and do not constitute an all-inclusive list~~ of conditions that would ~~not~~ be a Misoperation.

Example7c: A 230 kV shunt capacitor bank trips due to a settings error in the capacitor bank differential relay upon energization. The operation trips only the capacitor bank breaker that was closed to energize the bank. Since closing the breaker put the capacitor bank into service, this is a Misoperation.

Example 7d: A 230/115 kV BES transformer bank trips out when being re-energized due to an incorrect operation of the transformer differential relay for inrush following a maintenance outage. Only the high-side breaker opens since the low-side breaker had not yet been closed. Since closing the breaker put the transformer bank into service, this is a Misoperation.

Non-Protective Functions

BES interrupting device operations which are initiated by non-protective functions, such as those associated with generator controls, excitation controls, or turbine/boiler controls, static voltampere-reactive compensators (SVC), flexible ac transmission systems (FACTS), high-voltage dc (HVdc) transmission systems, circuit breaker mechanisms, or other facility control systems are not operations of a Protection System. The standard is not applicable to non-protective functions such as automation (e.g., data collection) or control functions that are embedded within a Protection System.

Control Functions

The entity must make a determination as to whether the standard is applicable to each operation of its Protection System in accordance with the provided exclusions in the standard's Applicability, see Section 4.2.1. The subject matter experts (SME) developing this standard recognize that entities use Protection Systems as part of a routine practice to control BES Elements. This standard is not applicable to operation of protective functions within a Protection System when intended for controlling a BES Element as a part of an entity's process or planned switching sequence. The following are examples of conditions to which this standard is not applicable:

Example 8a: The reverse power protective function that operates to remove a generating unit from service using the entity's normal or routine process.

Example 8b: The reverse power relay enables a permissive trip and the generator operator trips the unit.

~~In the example above, the~~

The standard is not applicable~~; however~~ to operation of the protective relay because its operation is intended as a control function as part of a controlled shutdown sequence for the generator. However, the standard remains applicable to operation of the reverse power relay ~~as a part of the generator Protection System~~ when ~~intended to provide generator anti-~~ it operates for conditions not associated with the controlled shutdown sequence, such as a motoring ~~protection. For example, reverse power relays are typically installed as~~condition caused by a trip of the ~~primary protection for a generating unit to guard against motoring. Though, operators often take advantage of this functionality and use the Protection System's reverse power protective function as a normal procedure to shutdown a generating unit~~prime mover.

The following is another example of a condition to which this standard is not applicable:

> **Example 8c:** Operation of a capacitor bank interrupting device for voltage control using functions embedded within a microprocessor based relay that is part of a Protection System.

The above are examples only, and do not constitute an all-inclusive list to which the standard is not applicable.

Extenuating Circumstances

In the event of a natural disaster or other extenuating circumstances, the December 20, 2012 Sanction Guidelines of the North American Electric Reliability Corporation, Section 2.8, Extenuating Circumstances, ~~says~~reads: "In unique extenuating circumstances causing or contributing to the violation, such as significant natural disasters, NERC or the Regional Entity may significantly reduce or eliminate Penalties." The Regional Entities to whom NERC has delegated authority will consider extenuating circumstances when considering any sanctions in relation to the timelines outlined in this standard.

The volume of Protection System operations tend to be sporadic. If a high rate of Protection System operations is not sustained, utilities will have an opportunity to catch up within the 120 day period.

Requirement R1

This requirement initiates a review of each BES interrupting device operation to identify whether or not a Misoperation may have occurred. Since the BES interrupting device owner typically monitors and tracks device operations, the owner is the logical starting point for identifying Misoperations of Protection Systems for BES Elements. A review is required when (1) a BES interrupting device operates that is caused by a Protection System or by manual intervention in response to a Protection System failure to operate, (2) regardless of whether the owner owns all or part of the Protection System component(s), and (3) the owner identified ~~that~~ its Protection System component(s) as causing the BES interrupting device operation.

Since most Misoperations result in the operation of one or more BES interrupting devices, these operations initiate a review to identify any Misoperation. If an Element is manually isolated in response to a failure to operate, the manual isolation of the Element triggers a review for Misoperation.

> **Example R1a:** The failure of a loss of field relay on a generating unit where an operator takes action to isolate the unit.

Manual intervention may indicate a Misoperation has occurred, thus requiring the initiation of an investigation by the BES interrupting device owner.

For the case, BES interrupting device did not operate and remote clearing occurs due to the failure of a Composite Protection System to operate, Requirement R2, Part 2.2 requires the entity that had the BES interrupting device operation to notify the other owner(s) to review its portion of Composite Protection System for Misoperation.

Protection Systems are made of many components. These components may be owned by different entities. For example, a Generator Owner may own a current transformer that sends information to a Transmission Owner's differential relay. All of these components and many more are part of a Protection System. It is expected that all of the owners will communicate with each other, sharing information freely, so that Protection System operations can be analyzed, Misoperations identified, and corrective actions taken.

Each entity is expected to use judgment to identify those Protection System operations that meet the definition of Misoperation regardless of the level of ownership. A combination of available information from resources such as counters, relay targets, Supervisory Control and Data Acquisition (SCADA) systems, or Disturbance Monitoring Equipment (DME) would typically be used to determine whether or not a Misoperation occurred. The intent of the standard is to classify an operation as a Misoperation if the available information leads to that conclusion. The standard also allows an entity to classify an operation as a Misoperation if entity is not sure, it may decide to identify the operation as a Misoperation and continue its investigation until the entity determines otherwise. If the continued investigative actions are inconclusive, the entity may declare no cause found and end its investigation. The entity is allotted 120 calendar days from the date of its BES interrupting device operation to identify whether or not a Misoperation of its Protection System component(s) occurred.

The Protection System operation may be documented in a variety of ways such as in a report, database, spreadsheet, or list. The documentation may be organized in a variety of ways such as by BES interrupting device, protected Element, or Composite Protection System.

Repeated operations which occur during the same automatic reclosing sequence do not need a separate identification under requirement R1. This is consistent with NERC SPCS guidance.

Repeated Misoperations which occur during the same 24 hour period do not need a separate identification under requirement R1. This is consistent with NERC PSMTF guidance.

When Elements are isolated from the BES and undergoing maintenance, they are not subject to the standard, provided they do not result in the operation of any interrupting devices that are part of the BES.

Requirement R2

~~For~~ Requirement R2 ~~(i.e.,~~ensures notification of those who have a role in identifying Misoperations, but were not accounted for within Requirement R1. In the case of multi-entity ownership~~),~~, the entity that owns the BES interrupting device that operated is expected to use judgment to identify those Protection System operations that meet the definition of Misoperation under Requirement R1; however, if the entity that owns a BES interrupting device determines that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation, it must notify the other Protection System owner(s) that share Misoperation identification responsibility when the criteria in Requirement R2 is met.

This requirement does not preclude the Protection System owners from initially communicating and working together to determine whether a Misoperation occurred and, if so, the cause. The BES interrupting device owner is only required to officially notify the other owners when it: (1) shares the Composite Protection System ownership with other entity(ies), (2) determines that a

Misoperation occurred or cannot rule out a Misoperation, and (3) determines its Protection System component(s) did not cause a Misoperation or is unsure. Officially notifying the other owners without performing a preliminary review may unnecessarily burden the other owners with compliance obligations, redirect valuable resources, and add little benefit to reliability. The BES interrupting device owner should officially notify other owners when appropriate within the established time period.

The following is an example of a notification to another Protection System owner:

> **Example R2a:** Circuit breakers A and B at the Charlie station tripped from directional comparison blocking ~~or (~~DCB) relaying on 03/03/2014 at 15:43 UTC during an external fault. As discussed last week, the fault records indicate that a problem with your equipment (failure to transmit) caused the operation.
>
> **Example R2b:** A generator unit tripped out immediately upon synchronizing to the grid due to a Misoperation of its overcurrent protection. The Transmission Owner owns the 230 kV generator breaker that operated. The Transmission Owner, as the owner of the BES interrupting device after determining that its Protection System components did not cause the Misoperation, was required to notify the Generator Owner of the operation. The Generator Owner investigated to determine if its Protection System components caused the Misoperation. In this example, the Generator Owner's Protection System components did cause the Misoperation. As the owner of the Protection System components that caused the Misoperation, the Generator Owner is responsible for creating and implementing the CAP.

A Composite Protection System owned by different functional entities within the same registered entity does not necessarily satisfy the notification criteria in part 2.1.1 of Requirement R2. For example, if the same personnel within a registered entity perform the Misoperation identification for both the GO and TO functions, then the Misoperation identification would be completely covered in Requirement R1, and therefore notification would not be required. However, if the Misoperation identification is handled by different groups, then notification would be required because the Misoperation identification would not necessarily be covered in Requirement R1.

Requirement R3

For Requirement R3 (i.e., notification received), the entity that also owns a portion of the Composite Protection System is expected to use judgment to identify whether the Protection System operation is a Misoperation. A combination of available information from resources such as counters, relay targets, SCADA, DME, and information from the other owner(s) would typically be used to determine whether or not a Misoperation occurred. The intent of the standard is to classify an operation as a Misoperation if the available information leads to that conclusion. The standard also allows an entity to classify an operation as a Misoperation if an entity is not sure, it may decide to identify the operation as a Misoperation and continue its investigation under Requirement R4. If the continued investigative actions are inconclusive, the entity may declare no cause found and end its investigation.

The entity that is notified by the BES interrupting device owner is allotted the later of 60 calendar days from receipt of notification or 120 calendar days from the BES interrupting device operation date to determine if its portion of the Composite Protection System caused the

Protection System operation. It is expected that in most cases of a jointly owned Protection System, the entity making notification would have been in communication with the other owner(s) early in the process. This means that the shorter 60 calendar days only comes into play if the notification occurs in the latter half of the 120 calendar days allotted to the BES interrupting device owner.

The Protection System review may be organized in a variety of ways such as in a report, database, spreadsheet, or list. The documentation may be organized in a variety of ways such as by BES interrupting device, protected Element, or Composite Protection System. The BES interrupting device owner's notification received may be documented in a variety of ways such as an email or a facsimile.

Requirement R4

The entity in Requirement R4 (i.e., cause identification), whether it is the entity that owns the BES interrupting device or an entity that was notified, ~~the entity~~ is expected to use due diligence in taking investigative action(s) to determine the cause(s) of an identified Misoperation for its portion of the Composite Protection System. The SMEs developing this standard recognize there will be cases where the cause(s) of a Misoperation will not be revealed during the allotted time periods in Requirements R1 or R3; therefore, Requirement R4 provides the entity a mechanism to continue its investigative work to determine the cause(s) of the Misoperation when the cause is not known.

A combination of available information from resources such as counters, relay targets, SCADA, DME, test results, and studies would typically be used to determine the cause of the Misoperation. At least one investigative action must be performed every two full calendar quarters until the investigation is completed.

The following is an example of investigative actions taken to determine the cause of an identified Misoperation:

> **Example R4a**: A Misoperation was identified on 03/18/2014. A line outage to test the Protection System was scheduled on 03/24/2014 for 12/15/2014 (i.e., beyond the next two full calendar quarters) due to summer peak conditions. The protection engineer contacted the manufacturer on 04/10/2014 (i.e., within two full calendar quarters) to obtain any known issues. The engineer reviewed manufacturer's documents on 05/27/2014. The outage schedule was confirmed on 08/29/2014 and was taken on 12/15/2014. Testing was completed on 12/16/2014 (i.e., in the second two full quarters) revealing the microprocessor relay as the cause of the Misoperation. A CAP is being developed to replace the relay.

Periodic action minimizes compliance burdens and focuses the entity's effort on determining the cause(s) of the Misoperation while providing measurable evidence. The SMEs recognize that certain planned investigative actions may require months or years to schedule and complete; therefore, the entity is only required to perform at least one investigative action every two full calendar quarters. If an investigative action is performed in the first quarter of a calendar year, the next investigative action would need to be performed by the end of the third calendar quarter. If an investigative action is performed in the last quarter of a calendar year, the next investigative action would need to be performed by the end of the second calendar quarter of the following

calendar year. Investigative actions may include a variety of actions, such as reviewing DME records, performing or reviewing studies, completing relay calibration or testing, requesting manufacturer review, ~~or~~ requesting ~~a necessary~~an outage, or confirming a schedule.

The entity's investigation is complete when it identifies the cause of the Misoperation or makes a declaration that no cause was determined. The declaration is intended to be used if the entity determines that investigative actions have been exhausted or have not provided direction for identifying the Misoperation cause. Historically, approximately 12% of Misoperations are unknown or unexplainable.[6]

Although the entity only has to document its specific investigative actions taken to determine the cause(s) of an identified Misoperation, the entity should consider the benefits of formally organizing (e.g., in a report or database) its actions and findings. Well documented investigative actions and findings may be helpful in future investigations of a similar event or circumstances. A thorough report or database may contain a detailed description of the event, information gathered, investigative actions, findings, possible causes, identified causes, and conclusions. Multiple owners of a Composite Protection System might consider working together to produce a common report for their mutual benefit.

The following are examples of a declaration where no cause was determined:

> **Example R4b**: A Misoperation was identified on 04/11/2014. All relays at station A and B functioned properly during testing on 08/26/2014. The carrier system functioned properly during testing on 08/27/2014. The carrier coupling equipment functioned properly during testing on 08/28/2014. A settings review completed on 09/03/2014 indicated the relay settings were proper. Since the equipment involved in the operation functioned properly during testing, the settings were reviewed and found to be correct, and the equipment at station A and station B is already monitored. The investigation is being closed because no cause was found.
>
> **Example R4c:** A Misoperation was identified on 03/22/2014. The protection scheme was replaced before the cause was identified. The power line carrier or PLC based protection was replaced with fiber-optic based protection with an in-service date of 04/16/2014. The new system will be monitored for recurrence of the Misoperation.

Requirement R5

Resolving the causes of Protection System Misoperations benefits BES reliability by preventing recurrence. The Corrective Action Plan ~~or (~~CAP) is an established tool for resolving operational problems. The NERC Glossary defines a Corrective Action Plan as, *"A list of actions and an associated timetable for implementation to remedy a specific problem."* Since a CAP addresses specific problems, the determination of what went wrong needs to be completed before developing a CAP. When the Misoperation cause is identified in Requirement R1, R3 or R4, Requirement R5 requires Protection System owner(s) to develop a CAP, or explain why corrective actions are beyond the entity's control or would not improve BES reliability. The entity must create the CAP or make a declaration why additional actions are beyond the entity's

[6] NERC System Protection and Control Subcommittee. Misoperations Report. April 1, 2013: http://www.nerc.com/docs/pc/psmtf/PSMTF_Report.pdf, Figure 15: NERC Wide Misoperations by Cause Code, pg. 22 of 40.

control or would not improve BES reliability and that no further corrective actions will be taken within 60 calendar days of first determining a cause.

The SMEs developing this standard recognize there may be multiple causes for a Misoperation; in these circumstances, the CAP would include a remedy for the identified causes. The CAP may be revised if additional causes are found; therefore, the entity has the option to create a single or multiple CAPs to correct multiple causes of a Misoperation. The 60 calendar day period for developing a CAP (or declaration) is established on the basis of industry experience which includes operational coordination timeframes, time to consider alternative solutions, coordination of resources, and development of a schedule.

The time periods within Requirement R1, R3 and ~~Requirement~~ R5 are distinct and separate. If a cause of a Misoperation is identified quickly, the time period in Requirement R1 or R3 ends and the 60 calendar day period to develop the CAP becomes applicable. The ultimate goal is to keep all time periods as short as possible, including the correction of the cause(s) of the Misoperation. See Requirement R6 for CAP implementation. Where there are multiple Protection System owners involved in a Misoperation, each owner whose Protection System component(s) contributed to the Misoperation is subject to Requirement R5.

The development of a CAP is intended to document the specific corrective actions needed to be taken to prevent Misoperation recurrence, the timetable for executing such actions, and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations. The evaluation of these other Protection Systems aims to reduce the risk and likelihood of similar Misoperations in other Protection Systems. The Protection System owner is responsible for determining the extent of its evaluation concerning other Protection Systems and locations. The evaluation may result in the owner including actions to address Protection Systems at other locations or the reasoning for not taking any action. The CAP ~~must include~~and an evaluation of other Protection Systems including other locations ~~to~~must be developed to complete Requirement R5.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor and the evaluation of the cause at similar locations which determined capacitor replacement was not necessary.

For completion of the CAPs in examples R5a through R5d, please see examples R6a through R6d.

> **Example R5a:** Actions: Remove the relay from service. Replace capacitor in the relay. Test the relay. Return to service or replace by 07/01/2014.
>
> Applicability to other Protection Systems: This type of impedance relay has not been experiencing problems and is systematically being replaced with microprocessor relays as Protection Systems are modernized. Therefore, it was assessed that a program for wholesale preemptive replacement of capacitors in this type of impedance relay does not need to be established for the system.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor and the evaluation of the cause at similar locations which determined the capacitors need preemptive correction action.

Example R5b: Actions: Remove the relay from service. Replace capacitor~~.~~ in the relay. Test the relay. Return to service or replace by 07/01/2014.

Applicability to other Protection Systems: This type of impedance relay is suspected to have previously tripped at other locations because of the same type of capacitor issue. Based on the evaluation, a program should be established by 12/01/2014 for wholesale preemptive replacement of capacitors in this type of impedance relay.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor and the evaluation of the cause at similar locations which determined the capacitors need preemptive correction action.

Example R5c: Actions: Remove the relay from service. Replace capacitor~~.~~ in the relay. Test the relay. Return to service or replace by 07/01/2014.

Applicability to other Protection Systems: This type of impedance relay is suspected to have previously tripped at other locations because of the same type of capacitor issue. Based on the evaluation, the preemptive replacement of capacitors in this type of impedance relay should be pursued for the identified stations A through I by 04/30/2015.

A plan is being developed to replace the impedance relay capacitors at stations A, B, and C by 09/01/2014. A second plan is being developed to replace the impedance relay capacitors at stations D, E, and F by 11/01/2014. The last plan will replace the impedance relay capacitors at stations G, H, and I by 02/01/2015.

The following is an example of a CAP for a relay Misoperation that was due to a version 2 firmware problem and the evaluation of the cause at similar locations which determined the firmware needs preemptive correction action.

Example R5d: Actions: Provide the manufacturer ~~Fault~~fault records. Install new firmware pending manufacturer results by 10/01/2014.

Applicability to other Protection Systems: Based on the evaluation of other locations and a risk assessment, the newer firmware version 3 should be installed at all installations that are identified to be version 2. Twelve relays were identified across the system. Proposed completion date is 12/31/2014.

The following are examples of a declaration made where corrective actions are beyond the entity's control or would not improve BES reliability and that no further corrective actions will be taken.

Example R5e: The cause of the Misoperation was due to a non-registered entity communications provider problem.

Example R5f: The cause of the Misoperation was due to a transmission transformer tapped industrial customer who initiated a direct transfer trip to a registered entity's transmission breaker.

In situations where a Misoperation cause emanates from a non-registered outside entity, there may be limited influence an entity can exert on an outside entity and is considered outside of an entity's control.

The following ~~in an example~~are examples of ~~a declaration~~declarations made why corrective actions would not improve BES reliability.

Example R5g: The investigation showed that the Misoperation occurred due to transients associated with energizing transformer ABC at Station Y. Studies show that de-sensitizing the relay to the recorded transients may cause the relay to fail to operate as intended during power system oscillations.

Example R5h: As a result of an operation that left a portion of the power system in an electrical island condition, circuit XYZ within that island tripped, resulting in loss of load within the island. Subsequent investigation showed an overfrequency condition persisted after the formation of that island and the XYZ line protective relay operated. Since this relay was operating outside of its designed frequency range and would not be subject to this condition when line XYZ is operated normally connected to the BES, no corrective action will be taken because BES reliability would not be improved.

Example R5i: During a major ice storm, four of six circuits were lost at Station A. Subsequent to the loss of these circuits, a skywire (i.e., shield wire) broke near station A on line AB (between Station A and B) resulting in a phase-phase fault. The protection scheme utilized for both protection groups is a ~~POTT.~~permissive overreaching transfer trip (POTT). The Line AB protection at Station B tripped timed for this event (i.e., Slow Trip – During Fault) even though this line had been identified as requiring high speed clearing. A weak infeed condition was created at Station A due to the loss of 4 transmission circuits resulting in the absence of a permissive signal on Line AB from Station A during this fault. No corrective action will be taken for this Misoperation as even under N-1 conditions, there is normally enough infeed at Station A to send a proper permissive signal to station B. Any changes to the protection scheme to account for this would not improve BES reliability.

A declaration why corrective actions are beyond the entity's control or would not improve BES reliability should include the Misoperation cause and the justification for taking no corrective action. Furthermore, a declaration that no further corrective actions will be taken is expected to be used sparingly.

Requirement R6

To achieve the stated purpose of this standard, which is to identify and correct the causes of Misoperations of Protection Systems for BES Elements, the responsible entity is required to implement a CAP that addresses the specific problem (i.e., cause(s) of the Misoperation) through completion. Protection System owners are required in the implementation of a CAP to update it when actions or timetable change, until completed. Accomplishing this objective is intended to reduce the occurrence of future Misoperations of a similar nature, thereby improving reliability and minimizing risk to the BES.

The following is an example of a completed CAP for a relay Misoperation that was applying a standing trip (See also, Example R5a).

Example R6a: Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. ~~The~~A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.

CAP completed on 06/25/2014.

The following is an example of a completed CAP for a relay Misoperation that was applying a standing trip that resulted in the correction and the establishment of a program for further replacements (See also, Example R5b).

Example R6b: Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. ~~The~~A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.

A program for wholesale preemptive replacement of capacitors in this type of impedance relay was established on 10/28/2014.

CAP completed on 10/28/2014.

The following is an example of a completed CAP of corrective actions with a timetable that required updating for a failed relay~~;~~ and preemptive actions for similar installations (See also, Example R5c).

Example R6c: Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. ~~The~~A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.

The impedance relay capacitor replacement was completed at stations A, B, and C on 08/16/2014. The impedance relay capacitor replacement was completed at stations D, E, and F on 10/24/2014. The impedance relay capacitor replacement for stations G, H, and I were postponed due resource rescheduling from a scheduled 02/01/15 completion to ~~03~~04/01/2015~~. Following the timetable change, capacitor~~ completion. Capacitor replacement was completed on 03/09/2015 at stations G, H, and I. All stations identified in the evaluation have been completed.

CAP completed on 03/09/2015.

The following is an example of a completed CAP for corrective actions with updated actions for a firmware problem~~;~~ and preemptive actions for similar installations. (See also, Example R5d).

Example R6d: Actions: ~~Fault~~fault records were provided to the manufacturer on 06/04/2014. The manufacturer responded that the Misoperation was caused by a bug in version 2 firmware, and recommended installing version 3 firmware. Version 3 firmware was installed on 08/12/2014.

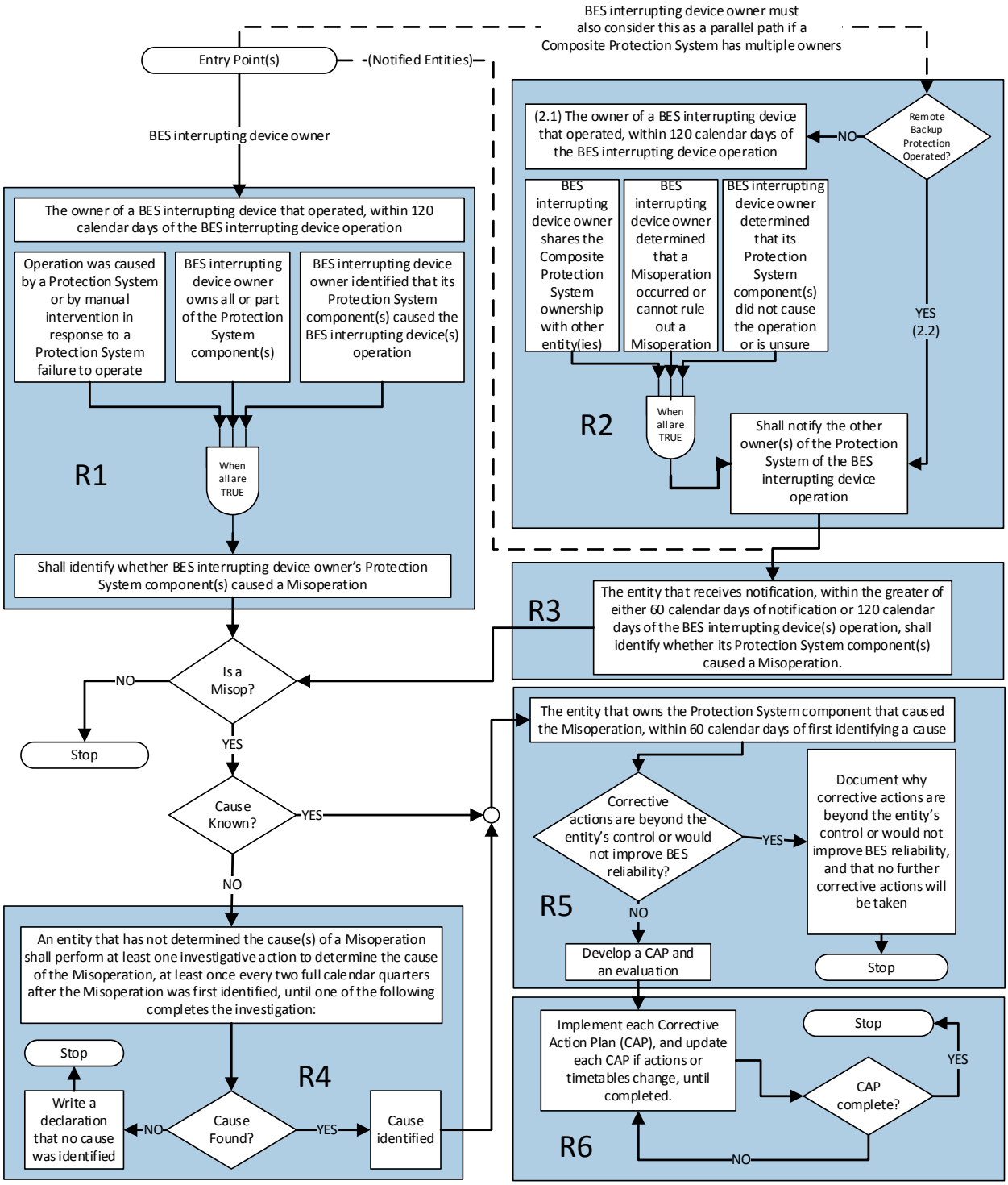
Nine of the twelve relays were updated to version 3 firmware on 09/23/2014. The manufacturer provided a subsequent update which was determined to be beneficial for the remaining relays. The remaining three of twelve relays identified as having the version 2 firmware were updated to version 3.01 firmware on 11/10/2014.

CAP completed on 11/10/2014.

The CAP is complete when all of the ~~documented~~ actions ~~to resolve~~identified within the ~~specific problem (i.e., Misoperation) are~~CAP have been completed ~~which may include those actions~~

~~resulting from the entity's evaluation of other locations, if not addressed through a separate CAP.~~.

Process Flow Chart: Below is a graphical representation ~~of the expected process created by the standard, including~~demonstrating the relationships between requirements:



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factors and Violation Severity Level Justifications

PRC-004-3 – Protection System Misoperation Identification and Correction

Project 2010-05.1 – Protection System (Misoperations)

Violation Risk Factor and Violation Severity Level Justifications

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in: PRC-004-3 — Protection System Misoperations.

Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

The Protection System Misoperations Standard Drafting Team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project.

NERC Criteria - Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

FERC Violation Risk Factor Guidelines

The standard drafting team (SDT) also considered consistency with the FERC Violation Risk Factor Guidelines for setting VRFs:[1]

Guideline (1) — Consistency with the Conclusions of the Final Blackout Report

The Commission seeks to ensure that Violation Risk Factors assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System.

In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System: [2]

[1] North American Electric Reliability Corp., 119 FERC ¶ 61,145, order on reh'g and compliance filing, 120 FERC ¶ 61,145 (2007) ("VRF Rehearing Order").
[2] Id. at footnote 15.

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief

Guideline (2) — Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

Guideline (3) — Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) — Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) — Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to

reflect the lower risk level associated with the less important objective of the Reliability Standard.

VRF Discussion

The following discussion addresses how the SDT considered FERC's VRF Guidelines 1 through 5. PRC-004-3 – Protection System Misoperation Identification and Correction is a revision of PRC-004-2.1a – Analysis and Mitigation of Transmission and Generation Protection System Misoperations. " The Reliability Standard PRC-003-1 – Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems requires Regional Entities to establish procedures for analysis of Misoperations. In FERC Order No. 693, the Commission identified PRC-003-0 as a "fill-in-the-blank" standard. The Order stated that because the regional procedures had not been submitted, the Commission proposed not to approve or remand PRC-003-0. Because PRC-003-0 (now PRC-003-1) is not enforceable, there is not a mandatory requirement for Regional Entity procedures to support the requirements of PRC-004-2.1a. This is a potential reliability gap; consequently, PRC-004-3 combines the reliability intent of the two legacy standards PRC-003-1 and PRC-004-2.1a.

The proposed PRC-004-3 Reliability Standard has six (6) discrete requirements that incorporate and enhance the intent of the requirements of PRC-004-2.1a and PRC-003-1. First, the revised standard requires the Transmission Owner, Generator Owner, and Distribution Provider to review each BES interrupting device operation meeting the criteria in Requirement R1, which includes: when caused by a Protection System operation or by manual intervention in response to a Protection System failure to operate and identify each that is a Misoperation; regardless of whether the BES interrupting device owner owns all or part of the Composite Protection System; and when BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation.

Second, the BES interrupting device owner is required to notify the other Composite Protection System component owner(s) when the criteria in Requirement R2 are met, which includes: Composite Protection System ownership is shared with another ~~entity~~owner; the BES interrupting device owner determined that a Misoperation occurred or cannot rule out a Misoperation; and the BES interrupting device owner determined that its Protection System component(s) did not cause the BES interrupting device(s) operation or is unsure.

Third, if a Transmission Owner, Generator Owner, or Distribution Provider is notified by a BES interrupting device owner that the Composite Protection System operated, it must review the operation according to Requirement R3. In most cases, Requirement R1 or R3 will reveal the cause of the Misoperation. If not, Requirement R4 mandates the entity perform investigative action(s) to determine the cause(s) as the fourth discrete ~~requirement~~Requirement. If a cause is not identified, the entity either may continue its investigation until a cause is identified or the

entity may write a declaration that no cause was identified. If a cause is identified, the entity advances to the fifth ~~requirement~~Requirement.

In Requirement R5, the entity whose Protection System component was identified as the cause of the Misoperation must either develop a Corrective Action Plan (CAP) or explain in a declaration why it cannot correct the cause of the Misoperation. In developing a Corrective Action Plan (CAP) for the identified Protection System component(s), the entity must perform an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations. If the entity determines that corrective actions are beyond the entity's control or would not improve BES reliability, ~~the entity~~it must ~~make~~explain this in a declaration why ~~and that~~ no further corrective actions will be taken.

In the last ~~of the requirements,~~ Requirement R6, the entity must implement and complete the CAP. The entity must update the CAP during implementation when actions or timetables change.

The requirements of the proposed PRC-004-3 do not map, one-to-one, with the ~~requirements~~Requirements of the two legacy standards, PRC-003-1 and PRC-004-2.1a. The new ~~requirements~~Requirements comingle various reliability attributes of the legacy standards with precise reliability objectives, thus a ~~requirement~~Requirement-to-~~requirement~~Requirement comparison of VRFs is not possible. In developing the new VRFs for the ~~requirements~~Requirements of PRC-004-3, the Standard Drafting Team carefully considered the NERC criteria for developing VRFs, as well as the FERC VRF guidelines. The VRFs of the FERC approved PRC-004-2.1a – Analysis and Mitigation of Transmission and Generation Protection System Misoperations~~,~~ (R1 & R2 – High VRF), PRC-004-WECC-1 – Protection System and Remedial Action Scheme Misoperation~~,~~ (R1 – Lower VRF), PRC-016-0.1 – Special Protection System Misoperation~~,~~ (R2 – Medium VRF), and PRC-022-1 – Under-Voltage Load Shedding Program Performance~~, R1~~ (R1 & R1.5 – Medium VRF), all influenced (citing FERC VRF Guideline 3) the drafting team's VRF decisions, as such, the VRFs for PRC-004-3 Requirements R1 through R6 are assigned a VRF of Medium.

NERC Criteria - Violation Severity Levels

Violation Severity Levels (VSLs) define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

Violation severity levels should be based on the guidelines shown in the table below:

Lower	Moderate	High	Severe
Missing a minor element (or a small percentage) of the required performance The performance or product measured has significant value as it almost meets the full intent of the requirement.	Missing at least one significant element (or a moderate percentage) of the required performance. The performance or product measured still has significant value in meeting the intent of the requirement.	Missing more than one significant element (or is missing a high percentage) of the required performance or is missing a single vital component. The performance or product has limited value in meeting the intent of the requirement.	Missing most or all of the significant elements (or a significant percentage) of the required performance. The performance measured does not meet the intent of the requirement or the product delivered cannot be used in meeting the intent of the requirement.

FERC Order on Violation Severity Levels

In its June 19, 2008 Order on Violation Severity Levels, FERC indicated it would use the following four guidelines for determining whether to approve VSLs:

Guideline 1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior Levels of Non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when Levels of Non-compliance were used.

Guideline 2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

Guideline 2a: A violation of a "binary" type requirement must be a "Severe" VSL.

Guideline 2b: Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline 4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF and VSL Justifications – PRC-004-3, R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A Violation Risk Factor of Medium is consistent with the NERC VRF Guidelines. Failure to review each BES interrupting device operation caused by a Protection System operation or by manual intervention in response to a Protection System failure to operate for Misoperation could in the planning time frame, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. Composite Protection System operations reviewed for proper operation by ~~their~~an owner~~(s)~~ is the first step in preventing the future severity of disturbances affecting a wider area, or potential equipment damage. However, violation of this requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	Guideline 1- Consistency w/ Blackout Report: The blackout report and subsequent technical analysis noted that zone 3 relays increased the severity of the blackout. Reviewing Protection ~~System~~Systems for Misoperation, identifying an unnecessary operation and taking corrective actions would reduce the likelihood of reoccurrence. This requirement is consistent with Recommendation 8: Improve System Protection to Slow or Limit the Spread of Future Cascading Outages.
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard:

VRF and VSL Justifications – PRC-004-3, R1	
	~~The~~This requirement has a single reliability activity associated with the reliability objective and no sub-Requirement(s) which allows a single VRF to be assigned; therefore no conflict(s) exist.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards: This requirement replaces one of the three performance components of PRC-004-2a, R1 (TO & DP) and R2 (GO). The three performance components (paraphrased) are "analyze Protection System Misoperations," "develop a Correction Action Plan," and "implement a Corrective Action Plan" which both have a VRF of High. This ~~proposed~~ Requirement R1, to "review" (similar to "analyze"), comports with Reliability Standards PRC-016-0.1 – Special Protection System Misoperations, R1 ("…shall analyze its SPS operations and maintain a record of all misoperations…") and PRC-022-1 – Under-Voltage Load Shedding Program Performance, R1 ("…shall analyze and document all UVLS operations and Misoperations.") which both have a VRF of Medium. ~~The proposed~~A VRF of Medium ~~is~~does not inadvertently ~~lowering~~lower the ~~identified~~current VRF of High in the former PRC-004-2.1a, Requirements R1 and R2, because ~~the proposed~~this Requirement now provides a clear and concise single reliability activity whereas the former Requirement contained multiple activities and is ambiguous. The VRF assignment also comports with the currently effective standards PRC-016-0.1 and PRC-022-1.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs:

VRF and VSL Justifications – PRC-004-3, R1	
	Failure to review each BES interrupting device operation caused by a Protection System operation or by manual intervention in response to a Protection System failure to operate for Misoperation could in the planning time frame, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. Protection System operations reviewed for proper operation by their owner(s) is the first step in preventing the future severity of disturbances affecting a wider area, or potential equipment damage. However, violation of this requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation: This requirement does not co-mingle reliability objectives of differing risk; therefore, the assigned VRF of Medium is consistent.

VRF and VSL Justifications – PRC-004-3, R1			
Proposed VSL			
Lower	**Moderate**	**High**	**Severe**
The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 120 calendar days and less than or equal to 150 calendar days of the BES interrupting device operation.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 150 calendar days and less than or equal to 165 calendar days of the BES interrupting device operation.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 165 calendar days and less than or equal to 180 calendar days of the BES interrupting device operation.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 180 calendar days of the BES interrupting device operation. OR The responsible entity failed to identify whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1.
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to the VSL for tardiness and a binary aspect for failure. The VSL is entity size-neutral because performance is event-driven and not by individual assets.		

VRF and VSL Justifications – PRC-004-3, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement replaces one of the three performance components of PRC-004-2a, R1 (TO & DP) and R2 (GO). The three performance components (paraphrased) are "analyze Protection System Misoperations," "develop a Correction Action Plan," and "implement a Corrective Action Plan." The VSLs are based on the three components and not individually as presented in the proposed PRC-004-3 standard. ~~The proposed~~This VSL does not lower the current level of compliance because the former VSL was comingled with the other activities. The ~~proposed~~ VSLs appropriately assess the severity of the violation with the failure to perform a review for Misoperation as Severe.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: This requirement is not binary; therefore, this criterion does not apply. Guideline 2b: ~~The proposed~~This VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – PRC-004-3, R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	~~The proposed~~This VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with ~~the requirement.~~this Requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justifications – PRC-004-3, R2	
Proposed VRF	**Medium**
NERC VRF Discussion	A Violation Risk Factor of Medium is consistent with the NERC VRF Guidelines. Failure to notify ~~a joint~~the other owner(s) of a Composite Protection System when the initiating owner determined its Protection System components did not cause a Misoperation or it did not rule out a Misoperation, could in the planning time frame, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. Unresolved Misoperations of ~~jointly~~Composite Protection Systems owned ~~equipment or operations~~by others that are not ruled out as a Misoperation could contribute to the severity of future disturbances affecting a wider area, or potential equipment damage. However, violation of this requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	Guideline 1- Consistency w/ Blackout Report:

VRF and VSL Justifications – PRC-004-3, R2	
	This is consistent with Recommendation 8: Improve System Protection to Slow or Limit the Spread of Future Cascading Outages. A lack of coordination on system protection was one of eight factors common to substantive outages prior to and including the August 14, 2003 Blackout. The initiating entity in the planning time frame is required to notify the other owner(s) of the Composite Protection System ~~components~~component(s) when it determines that (or is unsure whether)its ~~components~~component(s) did not cause a Misoperation or when it is unable to rule out a Misoperation of the ~~jointly owned~~ Composite Protection System~~.~~ owned by others. This ensures that all ~~parties~~owners review their equipment for proper operation which may include checking for proper coordination depending on the circumstances.
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard: ~~The~~This requirement has a single reliability activity associated with the reliability objective and no sub-Requirement(s) which allows a single VRF to be assigned; therefore no conflict(s) exist.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards: This requirement replaces one of the three performance components of PRC-004-2a, R1 (TO & DP) and R2 (GO). The three performance components (paraphrased) are "analyze Protection System Misoperations," "develop a Correction Action Plan," and "implement a Corrective Action Plan" which ~~as~~both have a VRF of High. ~~The~~This requirement and VRF of Medium is consistent with Reliability Standards FAC-008-3 – Facility Ratings, R7 ("…shall provide Facility Ratings (for its solely and jointly owned Facilities~~…") and …"~~), MOD-012-0 – Dynamics Data for Modeling and Simulation of the Interconnected Transmission System, R2 ("…shall provide appropriate equipment characteristics and system data~~…") which both~~…"), and IRO-015-1 – NAME, R1.1 ("…shall make notifications to other Reliability Coordinators of conditions in its Reliability Coordinator Area that may impact other Reliability Coordinator Areas.") which all have a VRF of Medium.

VRF and VSL Justifications – PRC-004-3, R2	
	Other ~~protection systems~~Protection Systems based Reliability Standards such as PRC-005-1b – Transmission and Generation Protection System Maintenance and Testing, R2 ("…shall provide documentation…"), PRC-016-0.1 – Special Protection System Misoperations, R3 ("…that owns an SPS shall provide documentation of the misoperation analyses…"), and PRC-017-0 – Special Protection System Maintenance and Testing, R2 ("…SPS shall provide documentation of the program…) all have a VRF of Lower; however, these requirements involve the administrative reporting to either the Regional Reliability Organization (now Regional Entity) or NERC and not a reliability function like the previously mentioned FAC-008-3 and MOD-012-0 Reliability Standards. As such, this Requirement R2 is assigned a VRF of Medium because it has a reliability need to be communicated to other owners.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs: Failure to notify other entities to review each Protection System operation, identify Misoperations, and determine the cause could in the planning time frame, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. Unresolved Misoperations of ~~jointly~~Composite Protection Systems owned ~~equipment or operations~~by others that are not ruled out as a Misoperation could contribute to the severity of future disturbances affecting a wider area, or potential equipment damage. However, violation of this requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation:

VRF and VSL Justifications – PRC-004-3, R2			
	This requirement does not co-mingle reliability objectives of differing risk; therefore, the assigned VRF of Medium is consistent.		
Proposed VSL			
Lower	**Moderate**	**High**	**Severe**
The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 120 calendar days and less than or equal to 150 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 150 calendar days and less than or equal to 165 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 165 calendar days and less than or equal to 180 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 180 calendar days of the BES interrupting device operation. OR The responsible entity failed to notify one or more of the other owner(s) of the Protection System component(s) in accordance with Requirement R2.
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to the VSL for tardiness and a binary aspect for failure. The VSL is entity size-neutral because performance is event-driven and not by individual assets.		

VRF and VSL Justifications – PRC-004-3, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement is new to the standard and had no previous level of compliance. Other Reliability Standards use a variety of VSLs ranging from a single severe level (i.e., binary), two levels, to four VSL levels. Some use a percentage as the failure of the number entities not notified; however, this would not be practical for this requirement as ~~joint ownership~~Composite Protection Systems that are owned by multiple entities is generally limited to one or two owners. The incremental increase in violation is consistent with the NERC Guidelines and is reasonable in consideration of the time periods provided by the Requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: This requirement is not binary; therefore, this criterion does not apply. Guideline 2b: ~~The proposed~~This VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	~~The proposed~~This VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with ~~the requirement.~~this Requirement.

VRF and VSL Justifications – PRC-004-3, R2	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justifications – PRC-004-3, R3	
Proposed VRF	**Medium**
NERC VRF Discussion	A Violation Risk Factor of Medium is consistent with the NERC VRF Guidelines. Failure of ~~a joint~~another Composite Protection System owner to review its ~~components~~component(s) for Misoperation, upon notification, for each BES interrupting device operation caused by a Protection System operation or by manual intervention in response to a Protection System failure to operate ~~for Misoperation upon notification~~ could in the planning time frame, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. Composite Protection System operations reviewed for proper operation by the other owner(s) is an important step in preventing the future severity of disturbances affecting a wider area, or potential equipment damage. However, violation of this requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	Guideline 1- Consistency w/ Blackout Report: The blackout report and subsequent technical analysis noted that zone 3 relays increased the severity of the blackout. Reviewing Protection ~~System~~Systems for Misoperation, identifying an unnecessary operation and taking corrective actions would reduce the likelihood of reoccurrence. This requirement is consistent with Recommendation 8: Improve System Protection to Slow or Limit the Spread of Future Cascading Outages.

VRF and VSL Justifications – PRC-004-3, R3	
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard: ~~The~~This requirement has a single reliability activity associated with the reliability objective and no sub-Requirement(s) which allows a single VRF to be assigned; therefore no conflict(s) exist.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards: This requirement replaces one of the three performance components of PRC-004-2a, R1 (TO & DP) and R2 (GO). The three performance components (paraphrased) are "analyze Protection System Misoperations," "develop a Correction Action Plan," and "implement a Corrective Action Plan" which ~~as~~both have a VRF of High. This ~~proposed~~ Requirement ~~R1,~~ R3, to "review" (similar to "analyze"), comports with Reliability Standards PRC-016-0.1 – Special Protection System Misoperations, R1 ("…shall analyze its SPS operations and maintain a record of all misoperations…") and PRC-022-1 – Under-Voltage Load Shedding Program Performance, R1 ("…shall analyze and document all UVLS operations and Misoperations.") which both have a VRF of Medium. ~~The proposed~~A VRF of Medium ~~is~~does not inadvertently ~~lowering~~lower the ~~identified~~current VRF of High in the former PRC-004-2.1a, Requirements R1 and R2, because ~~the proposed~~this Requirement now provides a clear and concise single reliability activity whereas the former Requirement contained multiple activities and is ambiguous.

VRF and VSL Justifications – PRC-004-3, R3	
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs: Failure of ~~a joint~~another Composite Protection System owner to review its ~~components~~component(s) for Misoperation, upon notification, for each BES interrupting device operation caused by a Protection System operation or by manual intervention in response to a Protection System failure to operate ~~for Misoperation upon notification~~ could in the planning time frame, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. Composite Protection System operations reviewed for proper operation by the other owner(s) is an important step in preventing the future severity of disturbances affecting a wider area, or potential equipment damage. However, violation of this requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation: This requirement does not co-mingle reliability objectives of differing risk; therefore, the assigned VRF of Medium is consistent.

VRF and VSL Justifications – PRC-004-3, R3			
Proposed VSL			
Lower	**Moderate**	**High**	**Severe**
The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was less than or equal to 30 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 30 calendar days and less than or equal to 45 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 45 calendar days and less than or equal to 60 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 60 calendar days late. OR The responsible entity failed to identify whether or not a Misoperation of its Protection System component(s) occurred in accordance with Requirement R3.
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to the VSL for tardiness and a binary aspect for failure. The VSL is entity size-neutral because performance is event-driven and not by individual assets.		

VRF and VSL Justifications – PRC-004-3, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement replaces one of the three performance components of PRC-004-2a, R1 (DP) and R2 (GO & TO) for the notified Protection System owner. The three performance components (paraphrased) are "analyze Protection System Misoperations," "develop a Correction Action Plan," and "implement a Corrective Action Plan." The VSLs are based on the three components and not individually as presented in the proposed PRC-004-3 standard. ~~The proposed~~A VSL does not lower the current level of compliance because the former VSL was comingled with the other activities. ~~The proposed~~This VSLs appropriately assess the severity of the violation with the failure to perform investigative actions as Severe.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: This requirement is not binary; therefore, this criterion does not apply. Guideline 2b: ~~The proposed~~This VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – PRC-004-3, R3	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	~~The proposed~~This VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with ~~the requirement.~~this Requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justifications – PRC-004-3, R4	
Proposed VRF	**Medium**
NERC VRF Discussion	A Violation Risk Factor of Medium is consistent with the NERC VRF Guidelines. Failure to identify the cause(s) of a Misoperation (if not determined in Requirements R1 or R3) could in the planning time frame, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. An Unidentified ~~causes~~cause(s) of a Misoperation could contribute to the severity of future disturbances affecting a wider area, or potential equipment damage. However, violation of this requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	Guideline 1- Consistency w/ Blackout Report: This requirement is consistent with Recommendation 8: Improve System Protection to Slow or Limit the Spread of Future Cascading Outages. The applicable entity must conduct investigative action(s) to determine the cause(s) of a Misoperation, if not determined during the course of a review as proposed in Requirements R1 and R3.
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard: ~~The~~This requirement has a single reliability activity associated with the reliability objective and no sub-Requirement(s) which allows a single VRF to be assigned; therefore no conflict(s) exist.

VRF and VSL Justifications – PRC-004-3, R4	
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards: This requirement replaces one of the three performance components of PRC-004-2a, R1 (TO & DP) and R2 (GO). The three performance components (paraphrased) are "analyze Protection System Misoperations," "develop a Correction Action Plan," and "implement a Corrective Action Plan" which ~~as~~have a VRF of High. This ~~proposed~~ Requirement R4, to perform at least one "investigative action" (similar to "analyze"), comports with Reliability Standards PRC-016-0.1 – Special Protection System Misoperations, R1 ("…shall analyze its SPS operations and maintain a record of all misoperations…") and PRC-022-1 – Under-Voltage Load Shedding Program Performance, R1 ("…shall analyze and document all UVLS operations and Misoperations.") which both have a VRF of Medium. ~~The proposed~~A VRF of Medium is not inadvertently lowering the ~~identified~~current VRF of High in the former ~~Requirement~~PRC-004-2.1a, Requirements R1 or R3, because ~~the proposed~~this Requirement now provides a clear and concise single reliability activity whereas the former Requirement contained multiple activities and is ambiguous. This VRF of Medium comports with the VRF assignment of Medium for PRC-004-3, Requirements R1 and R3, which will generally reveal the cause(s) of an identified Misoperation.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs: Failure to identify the cause(s) of a Misoperation could in the planning time frame, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

VRF and VSL Justifications – PRC-004-3, R4			
	Unidentified causes of a Misoperation could contribute to the severity of future disturbances affecting a wider area, or potential equipment damage. However, violation of this requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation: This requirement does not co-mingle reliability objectives of differing risk; therefore, the assigned VRF of Medium is consistent.		
Proposed VSL			
Lower	**Moderate**	**High**	**Severe**
The responsible entity performed at least one investigative action in accordance with Requirement R4, but was less than or equal to one calendar quarter late.	The responsible entity performed at least one investigative action in accordance with Requirement R4, but was greater than one calendar quarter and less than or equal to two calendar quarters late.	The responsible entity performed at least one investigative action in accordance with Requirement R4, but was greater than two calendar quarters and less than or equal to three calendar quarters late.	The responsible entity performed at least one investigative action in accordance with Requirement R4, but was more than three calendar quarters late. OR The responsible entity failed to perform investigative action(s) in accordance with Requirement R4.

VRF and VSL Justifications – PRC-004-3, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to the VSL for tardiness and a binary aspect for failure. The VSL is entity size-neutral because performance is event-driven and not by individual assets.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement replaces one of the three performance components of PRC-004-2a, R1 (TO & DP) and R2 (GO). The three performance components (paraphrased) are "analyze Protection System Misoperations," "develop a Correction Action Plan," and "implement a Corrective Action Plan." The VSLs are based on the three components and not individually as presented in the proposed PRC-004-3 standard. ~~The proposed~~This VSL does not lower the current level of compliance because the former VSL was comingled with the other activities. ~~The proposed~~This VSLs appropriately assess the severity of the violation with the failure to perform investigative actions as Severe.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent	Guideline 2a: This requirement is not binary; therefore, this criterion does not apply. Guideline 2b: ~~The proposed~~This VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – PRC-004-3, R4	
Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	~~The proposed~~This VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with ~~the requirement.~~this Requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justifications – PRC-004-3, R5	
Proposed VRF	**Medium**
NERC VRF Discussion	A Violation Risk Factor of Medium is consistent with the NERC VRF Guidelines. Failure to develop a CAP for a Misoperation with an identified cause could in the planning time frame, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. An unresolved cause of a Misoperation or failing to consider other locations with similar Protection System components could contribute the severity of future disturbances affecting a wider area, or potential equipment damage. However, violation of this requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	Guideline 1- Consistency w/ Blackout Report: The blackout report and subsequent technical analysis resulted in entities performing corrective actions; however, there were no negative reliability outcomes concerning the development of a Corrective Action Plan (CAP) associated with Protection Systems.
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard: ~~The~~This requirement has a single reliability activity associated with the reliability objective and no sub-Requirement(s) which allows a single VRF to be assigned; therefore no conflict(s) exist.

VRF and VSL Justifications – PRC-004-3, R5	
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards: This requirement replaces one of the three performance components of PRC-004-2a, R1 (TO & DP) and R2 (GO). The three performance components (paraphrased) are "analyze Protection System Misoperations," "develop a Correction Action Plan," and "implement a Corrective Action Plan" which have ~~varying VSLs.~~ ~~The proposed VSL does not lower the current level of compliance because the former VSL was comingled with the other activities. The former Requirement for the CAP was limited to a High VSL; however, the proposed Requirement R5 is now expanded to the Severe VSL. The lesser VSLs are based on tardiness and are practical and reasonable for the amount of time allotted for completion.~~a VRF of High. This requirement is consistent with Reliability Standards PRC-016-0.1, R2 ("…shall take corrective actions to avoid future Misoperations"), PRC-022-1, R1.5 ("For any Misoperation, a Corrective Action Plan…"), FAC-003, R5 ("…Transmission Owner or applicable Generator Owner shall take corrective action to ensure continued vegetation management") all three of which have a VRF of Medium.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs: Failure to develop a CAP for a Misoperation with an identified cause or failing to consider other locations with similar components could in the planning time frame, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. An unresolved cause of a Misoperation could contribute the severity of future disturbances affecting a wider area, or potential equipment damage. However, violation of this requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.

VRF and VSL Justifications – PRC-004-3, R5			
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation: This requirement does not co-mingle reliability objectives of differing risk; therefore, the assigned VRF of Medium is consistent.		
Proposed VSL			
Lower	**Moderate**	**High**	**Severe**
The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 60 calendar days and less than or equal to 70 calendar days of first identifying a cause of the Misoperation. OR The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 60 calendar days and less than or equal to 70 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 70 calendar days and less than or equal to 80 calendar days of first identifying a cause of the Misoperation. OR The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 70 calendar days and less than or equal to 80 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 80 calendar days and less than or equal to 90 calendar days of first identifying a cause of the Misoperation. OR The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 80 calendar days and less than or equal to 90 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 90 calendar days of first identifying a cause of the Misoperation. OR The responsible entity failed to develop a CAP or explain in a declaration in accordance with Requirement R5. OR

VRF and VSL Justifications – PRC-004-3, R5			
			The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 90 calendar days of first identifying a cause of the Misoperation. OR The responsible entity failed to develop an evaluation in accordance with Requirement R5.
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to the VSL for tardiness and a binary aspect for failure. Varying VSLs are provided for the omission of the evaluation when developing the Corrective Action Plan and for failure to develop the evaluation.		
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement replaces one of the three performance components of PRC-004-2a, R1 (TO & DP) and R2 (GO). The three performance components (paraphrased) are "analyze Protection System Misoperations," "develop a Correction Action Plan," and "implement a Corrective Action Plan" which have varying VSLs. ~~The proposed~~This VSL does not lower the current level of compliance because the former VSL in PRC-004-2.1a was comingled with the other activities. ~~The proposed~~This Requirement ~~is~~has a Severe VSL for failure to develop the CAP with the ~~Lower VSL~~other VSLs being based on tardiness of the development.		

VRF and VSL Justifications – PRC-004-3, R5	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: This requirement is not binary; therefore, this criterion does not apply. Guideline 2b: ~~The proposed~~This VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	~~The proposed~~This VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with ~~the requirement.~~this Requirement.
FERC VSL G4	The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justifications – PRC-004-3, R5	
Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	

VRF and VSL Justification – PRC-004-3, R6	
Proposed VRF	**Medium**
NERC VRF Discussion	A Violation Risk Factor of Medium is consistent with the NERC VRF Guidelines. Failure to implement a CAP for a Misoperation with an identified cause could in the planning time frame, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. An uncorrected cause of a Misoperation~~, through~~ as a result of not implementing a Corrective Action Plan, could contribute to the severity of future disturbances affecting a wider area, or potential equipment damage. However, violation of this requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.

VRF and VSL Justification – PRC-004-3, R6	
FERC VRF G1 Discussion	Guideline 1- Consistency w/ Blackout Report: The blackout report and subsequent technical analysis resulted in entities performing corrective actions; however, there were no negative reliability outcomes concerning the implementation of a Corrective Action Plan (CAP) associated with Protection Systems.
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard: ~~The~~This requirement has a single reliability activity associated with the reliability objective and no sub-Requirement(s) which allows a single VRF to be assigned; therefore no conflict(s) exist.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards: This requirement replaces one of the three performance components of PRC-004-~~2a~~2.1a, R1 (TO & DP) and R2 (GO). The three performance components (paraphrased) are "analyze Protection System Misoperations," "develop a Correction Action Plan," and "implement a Corrective Action Plan" which ~~as~~both have a VRF of High. ~~The~~This requirement is consistent with Reliability Standards PRC-016-0.1, R2 ("…shall take corrective actions to avoid future misoperations.") and PRC-022-1, R1.5 ("For any Misoperation, a Corrective Action Plan…") which both have a VRF of Medium. The proposed VRF of Medium ~~is~~does not inadvertently ~~lowering~~lower the ~~identified~~current VRF of High in the former ~~Requirement~~PRC-004-2.1a, Requirements R1 and R2, because ~~the proposed~~this Requirement now provides a clear and concise single reliability activity whereas the former Requirement contained multiple activities and is ambiguous.

VRF and VSL Justification – PRC-004-3, R6	
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs: Failure to implement a Corrective Action Plan for a Misoperation with an identified cause could in the planning time frame, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. An uncorrected cause of a Misoperation could contribute to the severity of future disturbances affecting a wider area, or potential equipment damage. However, violation of this requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation: This requirement does not co-mingle reliability objectives of differing risk; therefore, the assigned VRF of Medium is consistent.

VRF and VSL Justification – PRC-004-3, R6			
Proposed VSL			
Lower	**Moderate**	**High**	**Severe**
The responsible entity implemented, but failed to update a CAP, when actions or timetables changed, in accordance with Requirement R6.	N/A	N/A	The responsible entity failed to implement a CAP in accordance with Requirement R6.
NERC VSL Guidelines	Meets NERC's VSL Guidelines—The VSLs cover aspects of ~~the requirement~~this Requirement that are not equal in importance and performance.		
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 3- Consistency among Reliability Standards: This requirement replaces one of the three performance components of PRC-004-2a, R1 (TO & DP) and R2 (GO). The three performance components (paraphrased) are "analyze Protection System Misoperations," "develop a Correction Action Plan," and "implement a Corrective Action Plan." The VSLs are based on the three components and not individually as presented in the proposed PRC-004-3 standard. The proposed VSL does not lower the current level of compliance because the former VSL was comingled with the other activities. The proposed Requirement is a Severe VSL for failure to implement the CAP with the Lower VSL being based on the failure of updating the CAP when actions or timetables change which is administrative in nature.		

VRF and VSL Justification – PRC-004-3, R6	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: This requirement is not binary; therefore, this criterion does not apply. Guideline 2b: The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with ~~the requirement.~~this Requirement.
FERC VSL G4	The VSL is based on a single violation and not cumulative violations.

VRF and VSL Justification – PRC-004-3, R6	
Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	

Introduction to GMD Studies

A Planner's summary roadmap for TPL007-1 GMD planning studies

DRAFT

Prepared by L. Marti

Hydro One Networks, Toronto, Ontario, Canada

Last revision May 2014

Introduction to GMD studies

NERC Draft Standard TPL007-1 requires that applicable entities such as transmission planners and generator owners carry out studies and establish mitigating measures (if any) to meet the reliability performance criteria established by the Geomagnetic Disturbance (GMD) benchmark event. The draft standard and its associated white papers provide references to resources that a planning engineer can use as guidance to carry out GMD assessment studies. This document provides an introduction and single-source information summary to familiarize the planning engineer with the salient steps needed to carry out a GMD assessment.

Organization

This document is organized to answer the following questions:

- What is a GMD event and how does it interact with the interconnected power system
- What is the TPL007-1 GMD benchmark event
- What are the steps required to carry out the studies needed to meet TPL007-1 requirements
- What are the data required for these studies

This guide does not replace the modelling and application guides produced by NERC's Geomagnetic Disturbance Task Force [1-2], but rather provides a "lighter" guide focused on the requirements of TPL007-1. The reader is directed to these guides for a more in-depth treatment of various elements of the subject matter as needed.

Space weather and the power system

A geomagnetic disturbance (GMD) event is a consequence of the interaction of the cloud of charged particles produced by the Sun's Coronal Mass Ejections (CME) and the Earth's magnetic field. Unlike terrestrial weather, which is local, CMEs that cross the earth's path are global events.

The Sun undergoes an 11-year cycle, where the polarities of its north and south poles reverse (see Fig. 1). Most solar storms and CMEs occur during a 4-6 year period referred to as "solar maximum" (see Fig. 2). However, the largest historical solar storms have not occurred at the peak of the "solar maximum." Although the probability of a solar storm occurrence is greater during the peak of the solar cycle, severe solar storms and CMEs can occur at any time in the cycle.

DRAFT

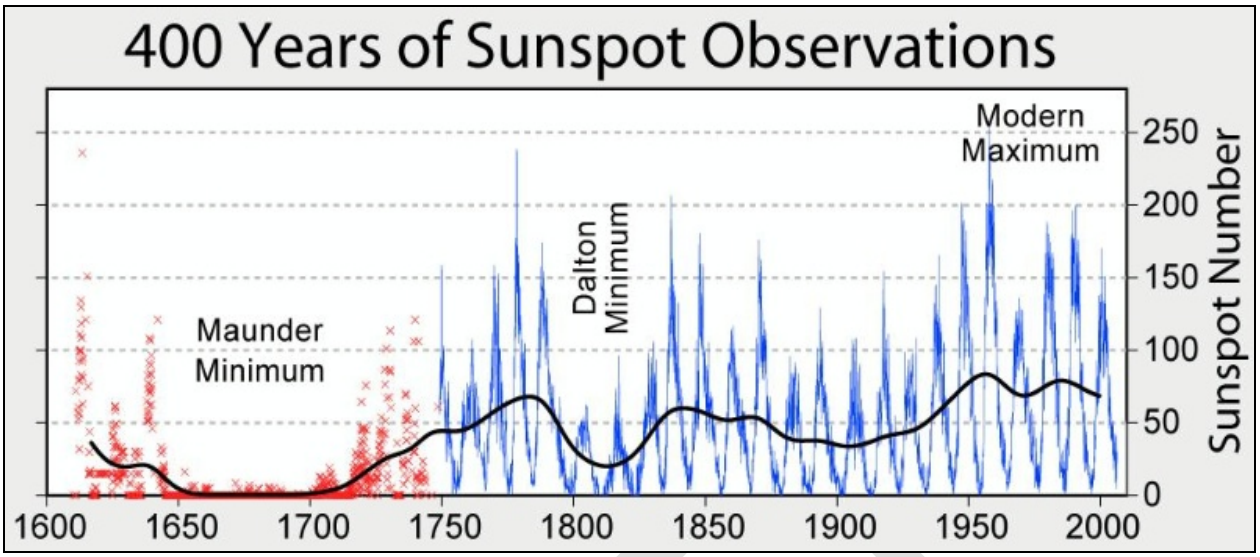


Fig. 1: Solar sunspot cycle

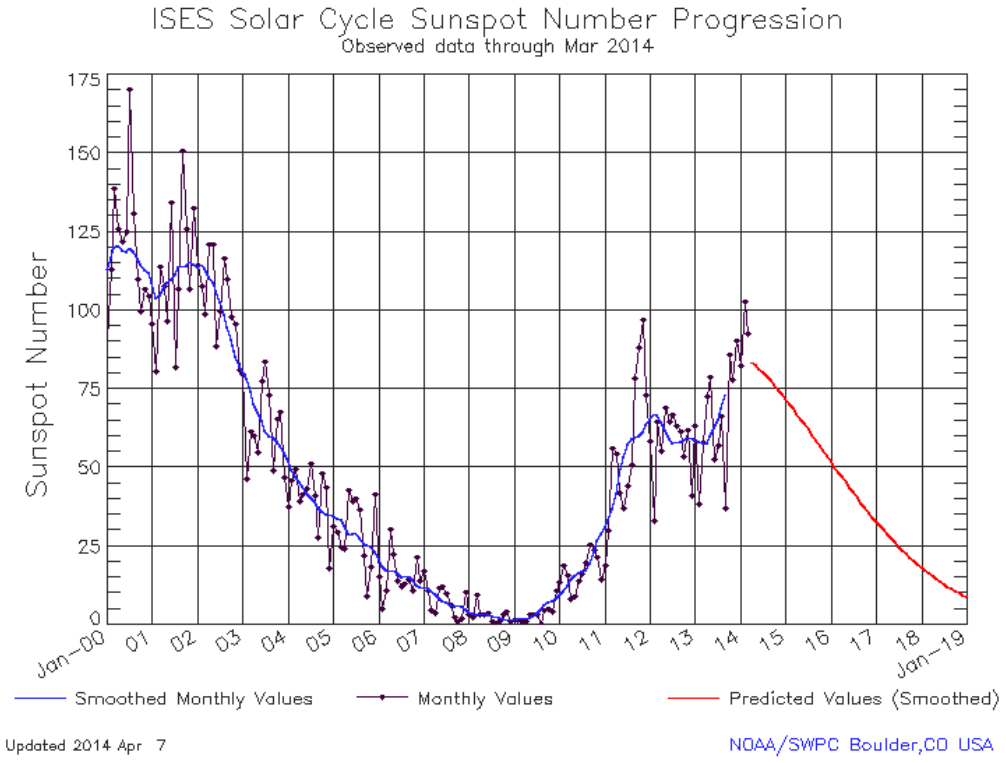


Fig. 2: Solar Sunspot Number Progression through October 2011

Geomagnetic disturbances occur on Earth one to four days after a flare or other eruption on the Sun.takes place. A CME, which is a cloud of solar material and magnetic fields that ejects from the Sun

and moves at a rate of about one to five million miles-per-hour, is usually associated with a large flare (see Fig. 3). If CMEs are Earth-directed, they interact with the Earth's magnetosphere and,

- Increase in the magnitude electroject currents as well as its width. From a power engineer's point of view, the electrojects (auroral/north and boreal/south) can be viewed as a large conductor about 100 km above the earth's surface carrying currents that can exceed 1,000,000 A.
- The interaction of the CME with the electroject causes slow fluctuations in the electrojet currents which in turn translate into changes in the magnetic field at ground level.

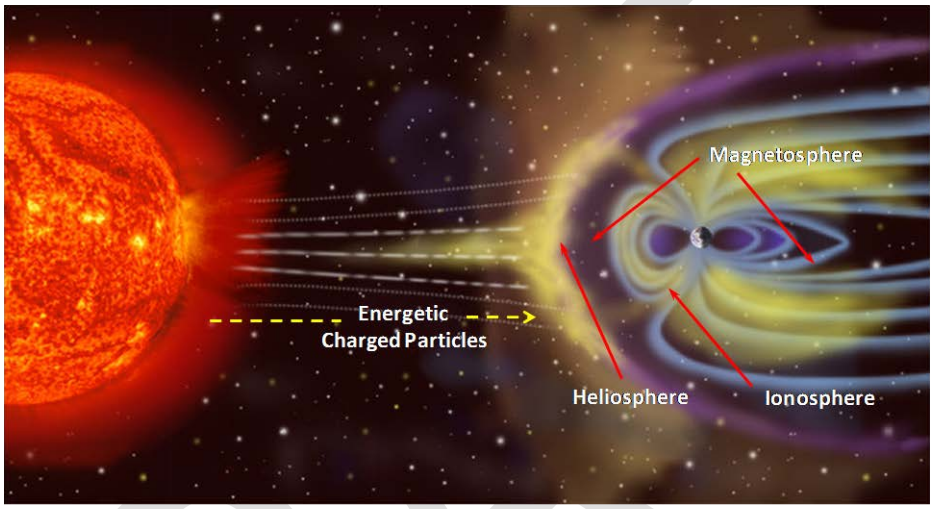


Fig. 3: Coronal Mass Ejection

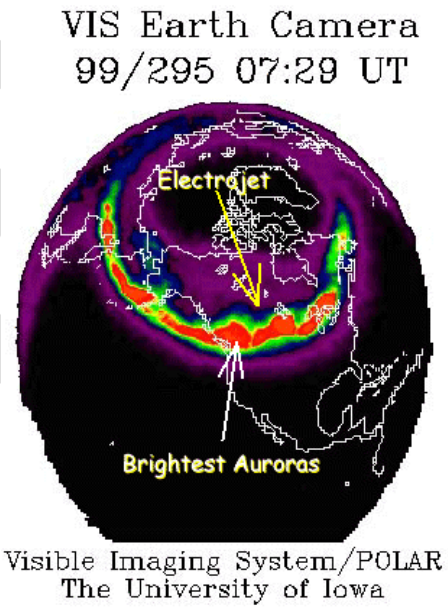


Fig. 4: Auroral electrojet.

Interaction of Geomagnetic Disturbances with the power system

A CME interacts with the earth's magnetic field and increases the magnitude and size of the electroject. The electroject can be visualized as a conductor 100 km above the earth carrying slow-varying currents (10 microHertz to 100 milliHertz). The electroject is magnetically coupled with transmission lines at ground level (see Fig. 5). The stronger the magnetic coupling between two conductors, the larger their coupling factor. The earth resistivity determines the coupling factor (high resistivity means large coupling factor) After the coupling factor is taken into consideration, the earth is assumed to be a zero resistance return path.

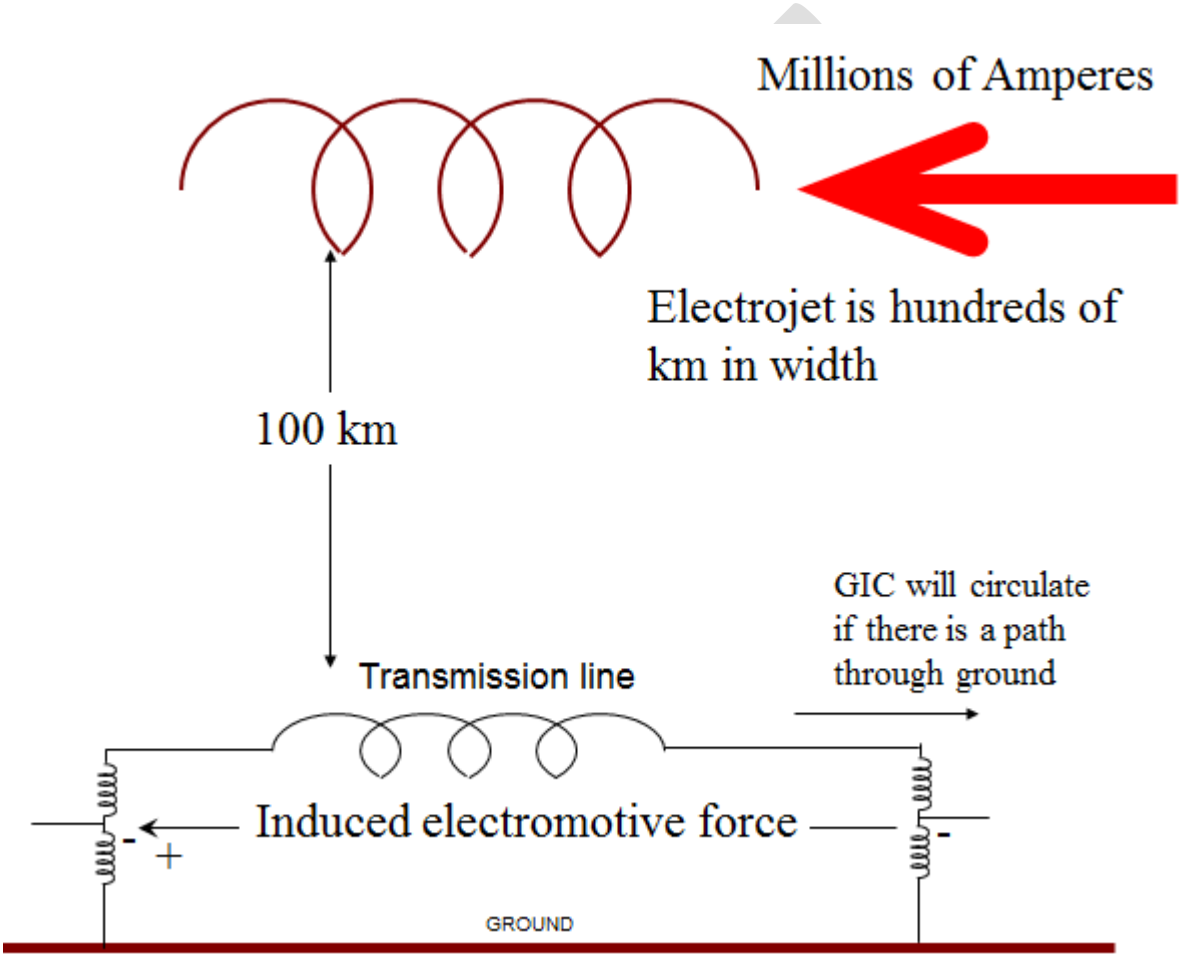


Fig. 5: Magnetic coupling between the electroject and HV transmission circuits.

Magnetic coupling induces a longitudinal voltage on transmission circuits. If there is a closed path through ground, this induced voltage will cause the circulation of Geomagnetically Induced Currents (GIC).

The notion of "coupling factor" is strictly a power engineering concept. The TPL007-1 standard uses the space science terminology of "earth model" effects, which account for earth structure and resistivity to depths of hundreds of km and determines how strongly the electrojet and transmission

circuits are coupled. The longitudinal induced voltage is referred to as the induced geoelectric field. In an HV and EHV transmission network, wye-grounded transformers provide a path to ground so that so that GIC can flow through the loop formed by lines, transformer windings station grounding system and earth return (see Fig. 6). In principle, a transformer with a zig-zag connection can also provide a path to ground for GIC. However, this type of connection is not normally used for voltages above 200 kV, which is the applicability voltage level of TPL007-1. HV-connected (as opposed to tertiary-connected) shunt reactors can also provide a path for GIC.

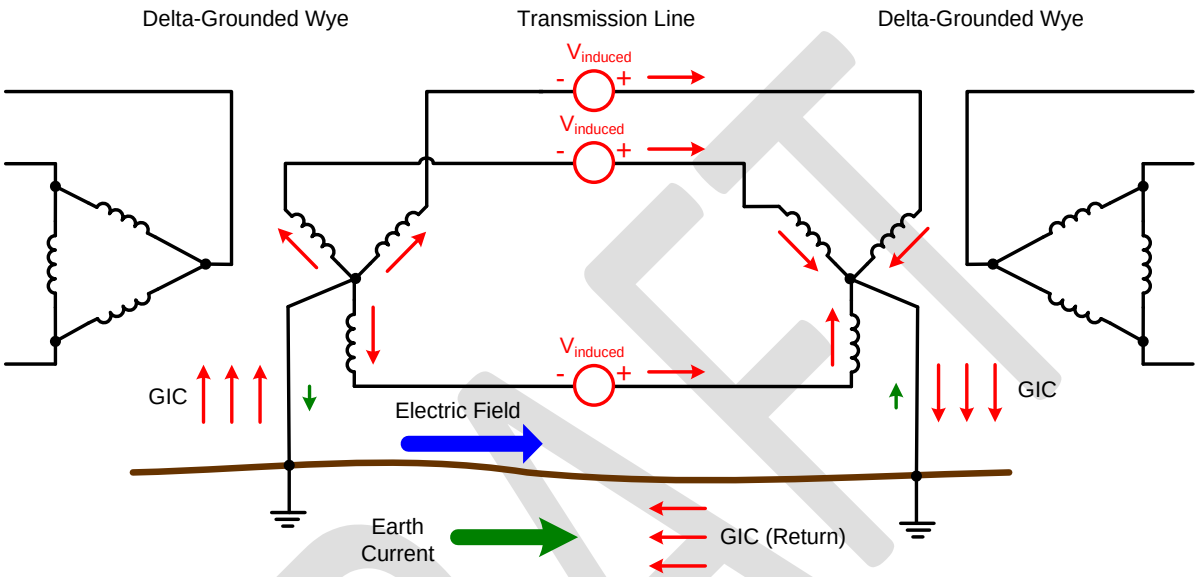


Fig. 6: GIC flow in the power system.

When GIC flows through a transformer winding there is a nearly constant flux offset (from a 60 Hz frame of reference) which causes asymmetrical or half-cycle saturation. Half cycle saturation causes persistent large magnetizing currents similar to inrush currents during transformer energization. These magnetizing currents are rich in even and odd harmonics. The 60 Hz component of these large magnetizing currents are seen by the system as transformer reactive power absorption.

Another effect of half-cycle saturation is hot spot heating of the transformer windings, which causes undue ageing of paper-oil insulation. Additionally, there is hot spot heating of the tank and other structural parts, which causes gassing, which in turn can result in dielectric breakdown.

Harmonics caused by half-cycle saturation can interfere with the operation of protective relaying. Shunt capacitor banks are harmonic sinks and experience harmonic overcurrents. This means that the shunt capacitor banks can either fail or trip on protection, depending on the protection scheme.

DRAFT

Effects of GIC in the power system

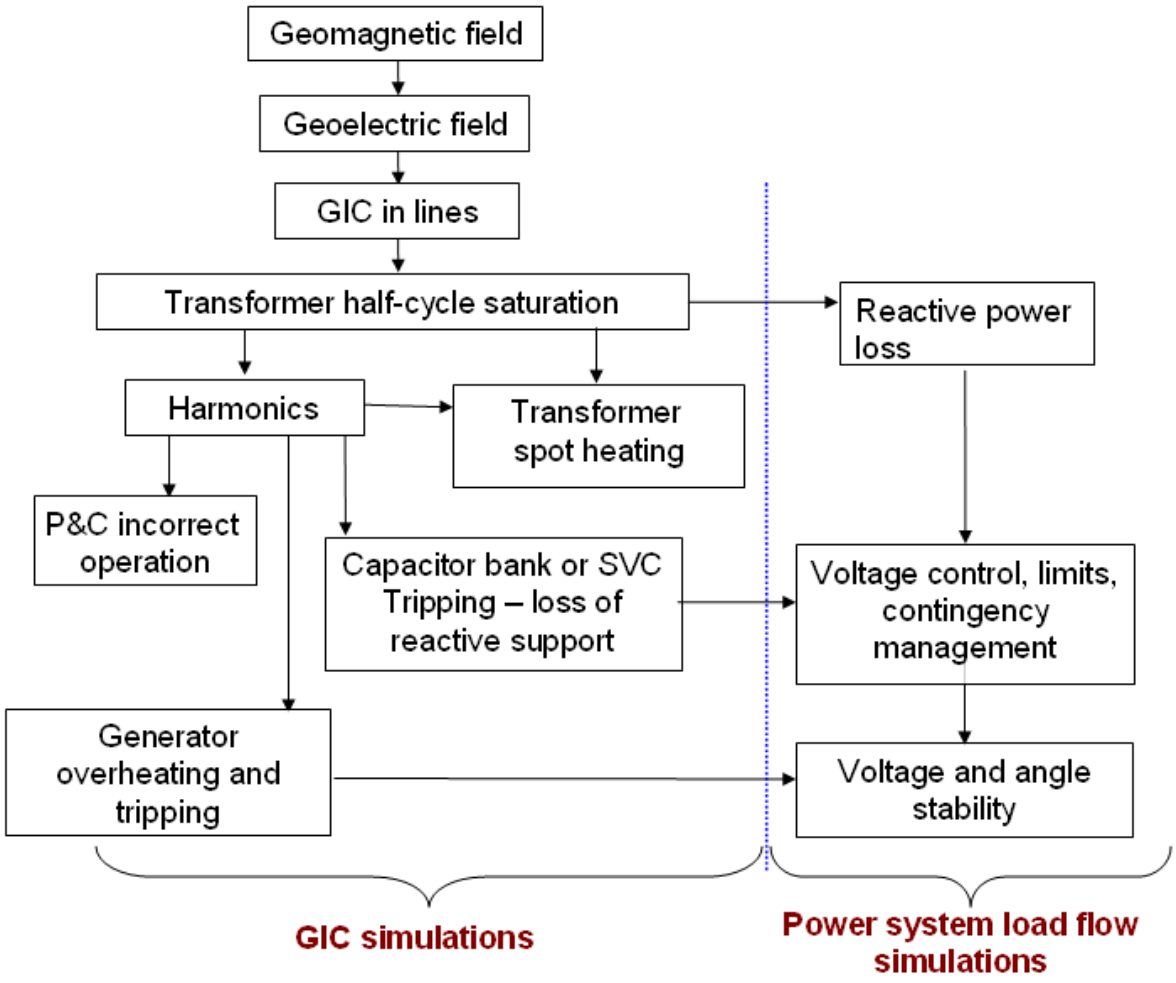


Fig. 7: Effects of GIC on the power system.

To summarize: GIC flow through the windings of HV and EHV transformer has the following consequences:

- Half-cycle saturation takes place. Half-cycle saturation causes
    - Even and odd current harmonics, which may
        - cause incorrect P&C operation;
        - exceed harmonic current ratings of shunt capacitor banks;
        - cause generator overheating due to negative sequence-like currents caused by even harmonics

- Additional transformer var absorption, which in turn can
  - reduce var reserves in the system;
  - violation of voltage and thermal limits;
  - contribute to voltage and angle instability.
- Transformer winding and structural part hot spot heating, which can lead to
  - Undue ageing of paper-oil insulation
  - Gassing that can lead to dielectric failure.

Benchmark GMD Event Description

The TPL007-1 GMD benchmark event is composed of the following elements: (1) a reference peak geoelectric field amplitude E_{peak} in V/km derived from statistical analysis of historical magnetometer data; (2) scaling factor α to account for local geomagnetic latitude; (3) scaling factor β to account for local earth resistivity; and (4) a reference geomagnetic field time series or waveshape to facilitate transformer thermal impact studies.

The statistical analysis predicts a peak geoelectric field amplitude of approximately 5.2 V/km. TPL007-1 selected a conservative 8V/km after accounting for some 20% margin as shown in equation (1) below.

$$E_{peak} = 8 \times \alpha \times \beta \ \text{(V/km)} \qquad (1)$$

Tables for scaling factor are provided in the Appendix of TPL007-1. A planner is permitted to use a technically-justified factor β on the basis of availability of more accurate earth models within the service territory.

The reference geomagnetic field time series is used to calculate GIC(t) in every applicable transformer in the network in order to carry out thermal vulnerability assessments.

DRAFT

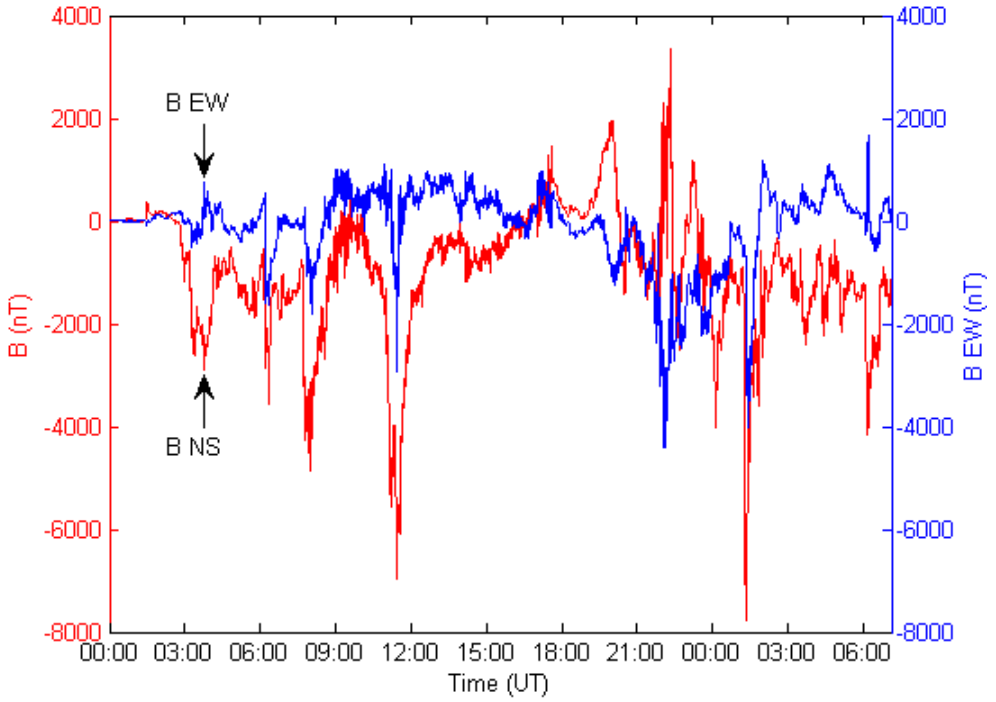


Fig. 8: Benchmark geomagnetic field waveshape. Red Bn (Northward), Blue Be (Eastward).

Studies required in a GMD assessment

The GMD assessment studies required in TPL007-1 generally follow the following sequence (see Fig. 9)

- GIC Study
  - Calculate GIC flow in every applicable transformer of the system using a peak geoelectric field of E_{peak}, as determined by the GMD benchmark event
  - Calculate var absorption in every applicable transformer of the system
- Load flow Study
  - Evaluate the performance of the system taking into consideration transformer var absorption calculated in the GIC Study.
- Thermal assessment study
  - Calculate GIC(t) for every applicable transformer in the system using the results of the GIC Study and the GMD benchmark reference geomagnetic field waveshape.
  - Determine if GIC(t) exceeds the allowable hot spot thermal limits of every applicable transformer in the system.

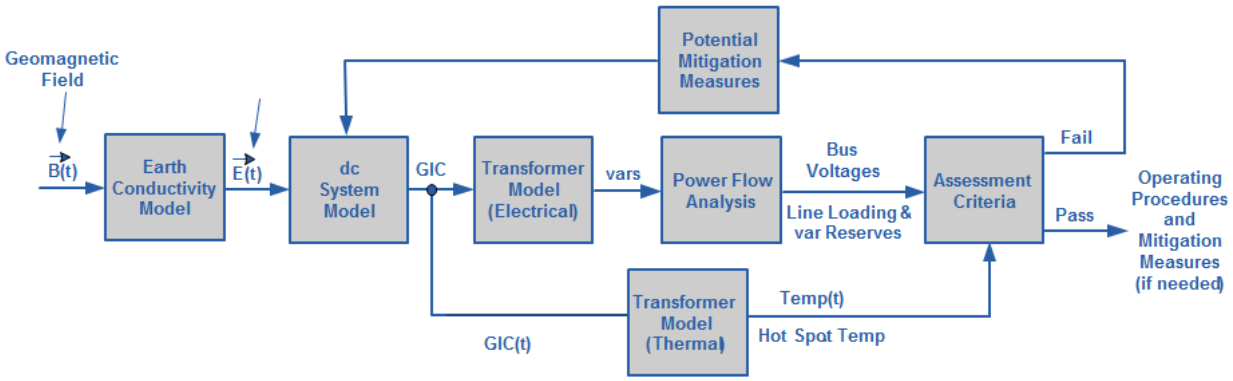


Fig. 9: GMD studies

1. **GIC study.** The purpose is to calculate the distribution of GIC in the network assuming a peak geoelectric field defined by E_{peak} in the GMD benchmark event (see equation (1)).
    a. GIC System model: Transmission lines are represented as a resistance in series with a voltage source. The magnitude of the voltage source depends on (a) line length and its orientation with respect to the direction of the geoelectric field; (b) Peak amplitude of the geoelectric field, which is defined by the benchmark GMD event. Transformers are represented as resistances. The effective grounding of a station is also modelled as a resistance.
    b. Transformer model: This is a curve that relates effective GIC in a transformer to reactive power absorption in the transformer (see Fig. 10).

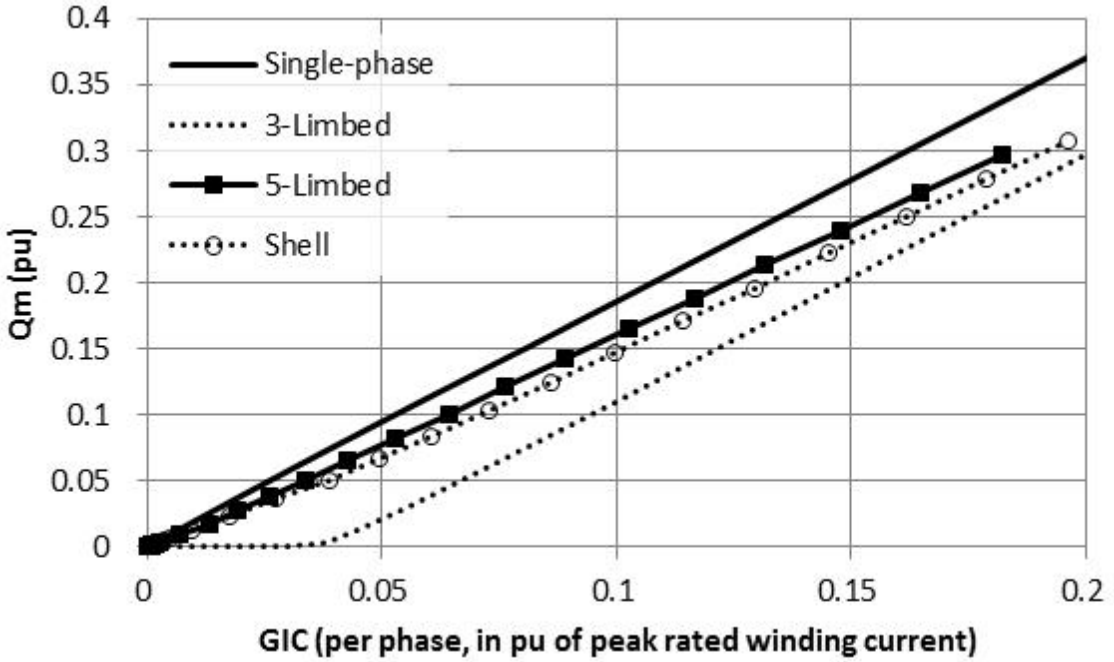


Fig. 10: Example of of GIC and var loss curves

DRAFT

c. Data sources:
    i. Station GPS coordinates. This determines the relative orientation of the transmission circuits and the geoelectric field.
    ii. Earth model or β factor from the GMD benchmark event. This determines the magnitude of the dc voltage sources in series with the transmission lines.
    iii. Transmission line dc resistance
    iv. Transformer winding dc resistance from test sheet, not from load flow model.
    v. Station grounding equivalent resistance, including the effect of shield wires.
    vi. Peak amplitude of the geoelectric field defined by the benchmark GMD event. This peak amplitude depends on geographical latitude (α factor) and local deep earth resistivity (β factor).
d. Results. The GIC study produces the following results for a given geoelectric field orientation, or the maximum GIC for the worst possible geoelectric field orientation:
    i. Distribution of GIC in every transformer in the system
    ii. 60 Hz reactive power absorption in every transformer.

2. **Load flow study.** The purpose of this study is to evaluate the effect to the ac network of transformer reactive power absorption computed by the GIC Study.
    a. System model:
        i. Standard ac base case load flow model to reflect the network operating conditions expected at the time a severe GMD event. For example, the load flow model may be modified to account for safe posture operational procedures that could be triggered on the basis of GMD coarse forecast (time window of 1 to 3 days).
        ii. Transformer reactive power absorption computed by the GIC Study is represented in the load flow model in the form of a constant var sink/source.
    b. Data sources
        i. Transformer reactive power absorption calculated with the GIC study
    c. Results:
        i. Load flow reflecting results with the reactive power absorption at the transformers reflected.
        ii. Identification of limit violations and situations of voltage instability

3. **Thermal assessment study**. The purpose is to assess if a transformer will withstand the benchmark GMD event.
    a. Transformer thermal model. This model relates GIC as a function of time (GIC(t)) to hot spot heating. Since transformer hot spot heating due to half-cycle saturation depends on magnitude and duration of GIC, the GMD benchmark provides a reference geoelectric field as a function of time from which GIC(t) can be calculated.
    b. Data sources:
        i. Transformer thermal model in the form of transformer capability curves provided by transformer manufacturers

DRAFT

ii. Generic or measured thermal transfer functions
    1. Manufacturer-provided
    2. From the NERC GMD Task Force reports.
iii. Peak GIC seen by a transformer as calculated in the GIC study.

c. Results:
    i. Hot spot temperature as a function of time for the GMD benchmark event. If temperatures exceed IEEE Std. 57.91 permissible emergency overloading hot spot limits the transformer may age unduly or eventually fail due to gassing.

Mitigating measures and corrective actions.

If load flow studies identify limit violations, a corrective plan must be put in place. If the plan involves changes in the system configuration, GIC, load flow and thermal assessment studies must be carried out to assess the effectiveness of the corrective plan.

If thermal assessment studies identify unacceptable hot spot limit violations, a corrective plan must be put in place. If the plan involves changes in the system configuration, GIC, load flow and thermal assessment studies must be carried out to assess the effectiveness and potentially unintended consequences of the corrective plan.

Calculation of GIC(t)

The calculation of GIC(t) required to perform a transformer thermal assessment is a new requirement for power engineers. The process to make this calculation from the time series of the GMD reference event is described in [3] and the general technical considerations are further discussed in [1]. A simplified step-by-step guide is presented here for completeness.

The GMD benchmark event specifies a reference geomagnetic field time series in the form of a comma-delimited ASCII file.

B_EW(t) and B_NS(t) are the components of geomagnetic field in the Eastward and Northward directions, respectively. The geomagnetic field is normalized to a 60° geomagnetic latitude (α=1.0).

E_EW(t) and E_NS(t) are the components of the geoelectric field in the Eastward and Northward directions, respectively. The geoelectric field is calculated using the reference earth model (β=1.0). Emag is the vectorial magnitude of the geoelectric field.

DRAFT

Time	B_EW(nT)	B_NS(nT)	E_EW(mV/km)	E_NS(mV/km)	Emag (mV/km)
1.00E+01	6.58E+00	-3.29E+00	1.92E+01	3.84E+01	4.29E+01
2.00E+01	9.87E+00	-3.29E+00	1.52E+01	4.97E+01	5.20E+01
3.00E+01	6.58E+00	-6.58E+00	2.84E+01	1.44E+01	3.18E+01
4.00E+01	0.00E+00	-6.58E+00	2.16E+01	-3.17E+01	3.84E+01
5.00E+01	6.58E+00	-6.58E+00	1.40E+01	1.48E+01	2.04E+01
6.00E+01	6.58E+00	-6.58E+00	1.03E+01	1.84E+01	2.10E+01
7.00E+01	3.29E+00	-9.88E+00	2.73E+01	-8.08E+00	2.85E+01
8.00E+01	6.58E+00	-6.58E+00	2.75E+00	1.21E+01	1.24E+01
9.00E+01	6.58E+00	-9.88E+00	1.89E+01	1.26E+01	2.27E+01
1.00E+02	6.58E+00	-9.88E+00	1.76E+01	8.25E+00	1.94E+01
1.10E+02	6.58E+00	-1.32E+01	3.14E+01	6.35E+00	3.21E+01
1.20E+02	9.87E+00	-9.88E+00	5.71E+00	2.44E+01	2.51E+01
1.30E+02	6.58E+00	-9.88E+00	2.03E+00	6.07E-01	2.12E+00

Process to calculate GIC(t)

1. Using the GIC Study software, calculate GIC_E in steady-state for the transformer under consideration assuming a uniform Eastward geoelectric field E_E = 1 V/km, GIC_E , and a zero Northward geoelectric field.
2. Using the GIC Study software, calculate GIC_N in steady-state for the transformer under consideration assuming a uniform Northward geoelectric field E_N = 1 V/km, GIC_E , and a zero Eastward geoelectric field.
3. Calculate GIC(t) using the formula

$$GIC(t) = \alpha \times \beta \times \left\{ GIC_E \cdot E_EW(t) + GIC_N \cdot E_NS(t) \right\}$$

If a technically justifiable earth model is known, use software to calculate the geoelectric field from the geomagnetic field using B_EW(t) and B_NS(t) as input to obtain $E_N(t)$ and $E_E(t)$. Calculate GIC(t) with the formula

$$GIC(t) = \alpha \times \left| E(t) \right| \times \left\{ GIC_E \cdot \sin(\theta(t)) + GIC_N \cdot \cos(\theta(t)) \right\}$$

where

$$\left| E(t) \right| = \sqrt{E_N^2(t) + E_E^2(t)}$$

$$\theta(t) = \tan^{-1}\left(\frac{E_E(t)}{E_N(t)} \right)$$

DRAFT

References

[1] NERC Application Guide, 2013

[2] NERC Planning guide, 2013

[3] TPL007-1 Thermal assessment white paper, 2014

[4] TPL007-1 Benchmark white paper, 2014

DRAFT

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

BES Cyber Asset (BCA): A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. ~~(~~A Transient Cyber Asset is not a BES Cyber Asset. ~~if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)~~

Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Transient Cyber Asset is not a Protected Cyber Asset. ~~if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.~~

Removable Media: Portable media, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media.

Transient Cyber Asset: A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-~~5~~6

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

6. Background:

Standard CIP-003-~~5~~ exists as part of a suite of CIP Standards related to cyber security, which ~~. CIP-002-5.1~~ require~~s~~ the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~ This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement~~ ~~**, in a manner that identifies, assesses, and corrects deficiencies, . . .**~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes,

but ~~they~~ it must address the applicable requirements. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to ~~its~~ low impact BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements by CIP Senior Manager approval of the policies specified in Part 2.1.

The language in Requirement R2, Part 2.~~3~~ 4 "~~. . . for~~ external routable protocol ~~connections~~ paths" and "Dial-up Connectivity~~. . .~~" was included to acknowledge the support given in FERC Order No. 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.~~3~~ 4 uses the phrase "external routable protocol ~~connections~~paths" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems. The Standard Drafting Team (SDT) intent in using the phrase "external routable protocol paths" is to focus only on the paths to the low impact BES Cyber Systems and not the paths to other networks (e.g., corporate paths).

The additions to Requirement R2, in particular the processes required under Parts 2.2-2.6, address FERC Order No. 791 paragraphs 106-110, which require the standard to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for low impact assets. The SDT pulled language and concepts from CIP-004, CIP-005, CIP-006, and CIP-008 in order to add objective criteria to each of the previous policy topic areas in CIP-003, Requirement R2.

In FERC Order No. 791 paragraphs 111-112, FERC upheld that creating and maintaining an inventory of low impact assets for audit purposes would be unduly burdensome, so the inventory statements remain unchanged.

R2. Each Responsible Entity for its assets ~~identified in CIP-002-5, Requirement R1, Part R1.3~~containing low impact BES Cyber Systems~~),~~ shall perform each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* ~~implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months:~~. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~Cyber security awareness;~~

~~Physical security controls;~~

~~Electronic access controls for external routable protocol connections and Dial-up Connectivity; and~~

~~Incident response to a Cyber Security Incident.~~

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence must include each of the applicable documented policies and processes that collectively include each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* and any additional evidence to demonstrate implementation as described in the Measures column of the table~~. If any asset locations have been identified per R2 of this Standard, then the following bulleted evidence may be included~~.

~~Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.~~

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	Low Impact BES Cyber Systems	Review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the topics in CIP-003-6, Requirement R2, Parts 2.2 – 2.6.	An example of evidence may include, but is not limited to, one or more documented cyber security policies that address each of the areas in Requirement R2, Parts 2.2 – 2.6 and includes evidence of review and CIP Senior Manager approval at least every 15 calendar months.
2.2	Low Impact BES Cyber Systems	Implement one or more documented processes that include operational or procedural control(s) to restrict physical access.	An example of evidence may include, but is not limited to, documentation of the operational or procedural control(s).
2.3	Low Impact BES Cyber Systems at Control Centers	Implement one or more documented processes that collectively include the following: 2.3.1. Escorted access of visitors; and 2.3.2. For Control Centers with external routable protocol paths, monitoring physical access point(s).	Examples of evidence may include, but are not limited to: • For 2.3.1, documentation of visitor escort procedure(s) at Control Centers. • For 2.3.2, documentation describing how the Responsible Entity monitors physical access points into Control Centers that have

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
			external routable protocol paths.
2.4	Low Impact BES Cyber Systems	Implement one or more documented processes that collectively include the following: 2.4.1. All external routable protocol paths, if any, must be through one or more identified access point(s). 2.4.2. For each identified access point, if any, require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. 2.4.3. Authentication when establishing Dial-up Connectivity, per Cyber Asset capability.	Examples of evidence may include, but are not limited to: • For 2.4.1, documentation of external routable protocol paths through identified access points. • For 2.4.2, a representative sample of a list of restrictions (e.g., firewall rules, access control lists, data diode, etc.) that demonstrates that only permitted access is allowed and that each access rule has a reason documented individually or by group. • For 2.4.3, documentation of authentication controls applied to dial-up access connections.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	Low Impact BES Cyber Systems	Implement one or more Cyber Security Incident response plan(s) that collectively include the following: 2.5.1. Identification, classification, and response to Cyber Security Incidents. 2.5.2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident. 2.5.3. Notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. 2.5.4. The roles and responsibilities of Cyber Security Incident response groups or individuals. 2.5.5. Incident handling procedures for Cyber Security Incidents. 2.5.6. Testing of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to: • One or more documented cyber security incident response plans that include the requirement parts. • Dated evidence that shows the testing or execution of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Low Impact BES Cyber Systems	Implement a security awareness program that reinforces cyber security practices at least quarterly. Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.	An example of evidence may include, but is not limited to, one or more documents describing how the Responsible Entity is implementing its cyber security awareness program per 2.6.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager

may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1)	the previous approval. (R1)		months of the previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only three~~one of the topics as required by Requirement R2, Part 2.1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (~~R2~~2.1) ~~OR~~ ~~The Responsible Entity documented and implemented one or more cyber~~	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only~~ two of the topics as required by Requirement R2, Part 2.1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (~~R2~~2.1) ~~OR~~ ~~The Responsible Entity documented and implemented~~	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only one~~three of the topics as required by Requirement R2, Part 2.1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (~~R2~~2.1) ~~OR~~ ~~The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2~~	The Responsible Entity did not ~~document or implement~~have any documented cyber security policies for assets with a low impact rating that address the topics as required by Requirement R2, Part 2.1. (~~R2~~2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~security policies for assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the	~~one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of	~~but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (~~R2~~2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by	Part 2.1 within 18 calendar months of the previous review. (~~R2~~2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 18 calendar months of the previous approval. (~~R2~~2.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			previous review. (~~R2~~2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (~~R2~~2.1) OR	the previous review. (~~R2~~2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (~~R2~~2.1)	Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (~~R2~~2.1) OR The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.3. (2.3) OR The Responsible Entity documented and implemented one or	The Responsible Entity did not document or implement any processes for assets with a low impact rating to include the operational or procedural control(s) to restrict physical access as required by Requirement R2, Part 2.2. (2.2) OR The Responsible Entity did not document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.3. (2.3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity did not reinforce cyber security practices at least quarterly but did reinforce cyber security practices at least every two quarters. (2.6) OR The Responsible Entity did not	OR The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include two of the topics as required by Requirement R2, Part 2.5. (2.5) OR	more processes for assets with a low impact rating but failed to include two of the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include three of the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices	The Responsible Entity did not document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity did not implement any Cyber Security Incident response plans for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.5 for assets with a low impact rating in less than or equal to 16 calendar months. (2.6)	The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices at least quarterly but failed to include one of the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security practices every three quarters. (2.6) OR	at least quarterly but failed to include two of the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security practices every three quarters. (2.6) OR The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 for assets with a low impact rating in more than 17 calendar months but less than or equal to 18 calendar months. (2.6)	implement a security awareness program for assets with a low impact rating that collectively included the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not implement a security awareness program for assets with a low impact rating that reinforced cyber security practices at least every 15 months. (2.6) OR The Responsible Entity did not implement a security awareness program for assets with a low

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 in more than 16 calendar months but less than or equal to 17 calendar months. (2.6)		impact rating that reinforced the topics within 18 calendar months as required by Requirement R2, Part 2.6. (2.6)
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				50 calendar days of the change. (R3)		Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	~~The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and has Identified deficiencies but did not assess or correct the deficiencies.(R4)~~ ~~OR~~ ~~The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or~~	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~correct the deficiencies.(R4)~~ ~~OR~~ The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-6~~5~~, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-6~~5~~, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-6~~5~~, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

~~As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not~~

~~necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.~~

The intent of the requirement is to outline a set of protections designed for all low impact BES Cyber Systems. The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do meet the definition of having a 15-minute adverse impact so some protections are needed. The intent is that such protections are part of a program that covers the low impact BES Cyber Systems collectively either at a programmatic or site level, not an individual device or system level.

There are four main areas that must be covered by this security program: physical security, electronic access controls for all external routable protocol paths or Dial-up Connectivity, a security awareness program, and cyber security incident response plans.

The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not necessary.

2.1 - As with Requirement R1, the number of policies and the specific language used in them would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas in CIP-003-6, Requirement R2, Parts 2.2 through 2.6. The Responsible Entity has flexibility in the number and structure of its policies to meet its needs and organization. Examples include developing a single comprehensive cyber security policy covering these topics for all in-scope assets, several comprehensive cyber security policies based on asset type, or a single high-level umbrella policy with additional policy detail in lower level documents in its documentation hierarchy.

2.2 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at a BES asset. The Responsible Entity has flexibility in the controls used and the granularity of those controls. The entity is to document its operational or physical controls that restrict access to the low impact BES Cyber Systems at the asset. Entities may utilize perimeter controls (fences with locked gates, guards, site access policies, etc.) and/or more granular areas of access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. Lists of authorized users are not required.

2.3 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at Control Centers. For Control Centers, the entity should further describe the process for handling escorted access of visitors. For Control Centers that have external routable connectivity, monitoring of physical access points is also required. Monitoring does not imply logging and maintaining logs, but monitoring that access has been

granted through an access point (door alarm, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the level as determined by the entity's controls.

2.4 – The Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. The electronic access controls should address the risk of using the asset's external connectivity to gain access to the low impact BES Cyber Systems. The entity should be able to describe how its electronic access controls on the external connectivity paths protect the collection of low impact BES Cyber Systems at the site. The intent is to reduce the risk of aggregation of numerous low impact BES Cyber Systems at the site or across multiple sites through external connectivity.

Examples of sufficient access controls may include:

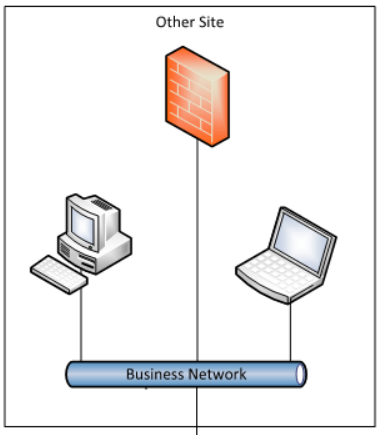
- All the external routable protocol connectivity paths to the asset pass through a firewall that denies all traffic by default with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are shielded from or to the world-wide-web (e.g. IP addresses, ports, services, and data diode) for scenarios representative of the Responsible Entity's sites having Low Impact BES Cyber Systems.
- Dialup Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dialup Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has dialup connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset which has a default password. There is no access control in this instance.
- An asset has external routable connectivity due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier which allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.

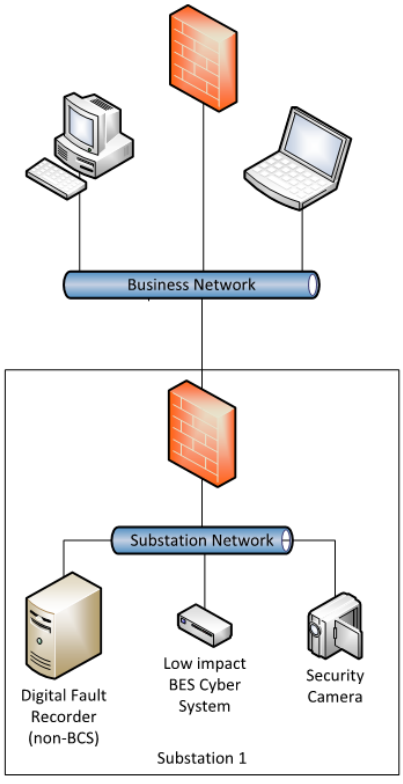
The SDT also notes that in topic 2.4, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

The following diagrams explain the SDT's rationale.



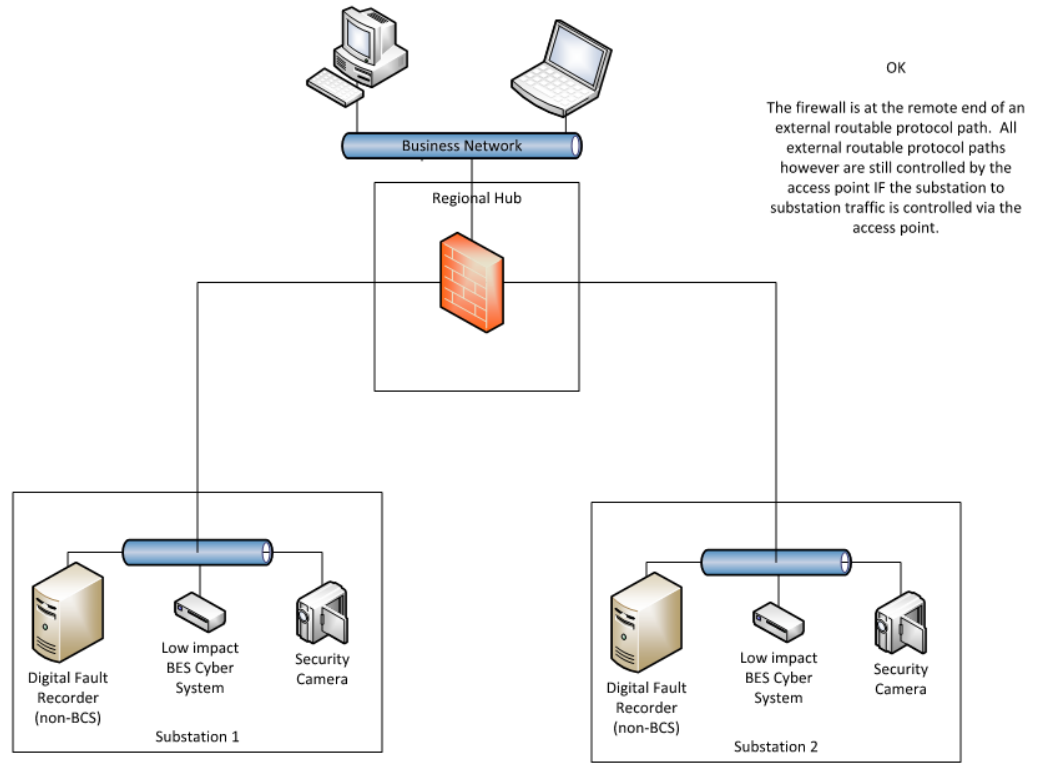
NOT OK

The BES Cyber System is behind an access point, however all external routable protocol paths to the BES Cyber System are not controlled by an access point if they originate on the business network.



OK

All the external traffic to the BES Cyber System is controlled by an access point.



2.5 - The entity should have a documented cyber security incident response plan that includes each of the topics listed. For assets that have limited or no connectivity, it is not the intent to increase their risk by increasing the level of connectivity in order to have real-time monitoring. The intent is if in the normal course of business suspicious activities are noted at an asset containing low impact BES Cyber Systems, there is a cyber security incident response plan that will guide the entity through responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident. The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as well as other forms of tabletop exercises or paper drills. NERC-led exercises such as GridEx participation would also count as an exercise if the entity's response plan is followed.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

2.6 - The intent of the security awareness program is for entities to reinforce good cyber security practices with their personnel on at least a quarterly basis. The physical security, electronic access controls, and the cyber security incident response plan should be covered at least every 15 months. It is up to the entity as to the topics and how it schedules these topics. It should be sufficient for an entity to produce the awareness material that it delivered quarterly and the delivery method(s) (posters, emails, topics at staff meetings, etc.). The intent is that tracking of reception of the messages by personnel is not required.

Requirement R3:

The intent of CIP-003-6~~5~~, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-6~~5~~, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-~~5.1~~6

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~5.1~~6:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-004-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is six calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-004 ~~5.1~~ exists as part of a suite of CIP Standards related to cyber security, which ~~CIP-002-5~~ requires the initial identification and categorization of BES Cyber Systems ~~CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards.*~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement **in a manner that identifies, assesses, and corrects deficiencies, . . .~~**

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements~~

~~described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~ 6Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for

CIP-004-~~5.1~~6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ ~~a~~ one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-~~5~~6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-~~5~~ 6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the~~	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the~~	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	~~deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical	~~deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical	implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)	access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)	(2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date~~, and did not identify, assess and correct the deficiencies~~. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals~~, and did not identify, assess, and correct the deficiencies~~.	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals~~, and did not identify, assess, and correct the deficiencies~~.	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual~~, and did not identify, assess, and correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)	calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date ~~and has identified deficiencies, and did not identify, assess, and correct the deficiencies~~. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter~~, and did not identify, assess and correct the deficiencies~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	BES Cyber System Information is located~~, and did not identify, assess, and correct the deficiencies~~. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is	calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)	calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies~~. (4.4)			were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3) OR The Responsible Entity has implemented	complete the removal within 24 hours of the termination action but did not initiate those removals for one individual~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that~~-~~ an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that ~~-~~an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that ~~-~~an individual no longer

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.4) OR The Responsible Entity has implemented one or more process(es) to	day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3)	day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3)	requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.5) OR The Responsible			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances~~, and did not~~			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~identify, assess, and correct the deficiencies~~. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the

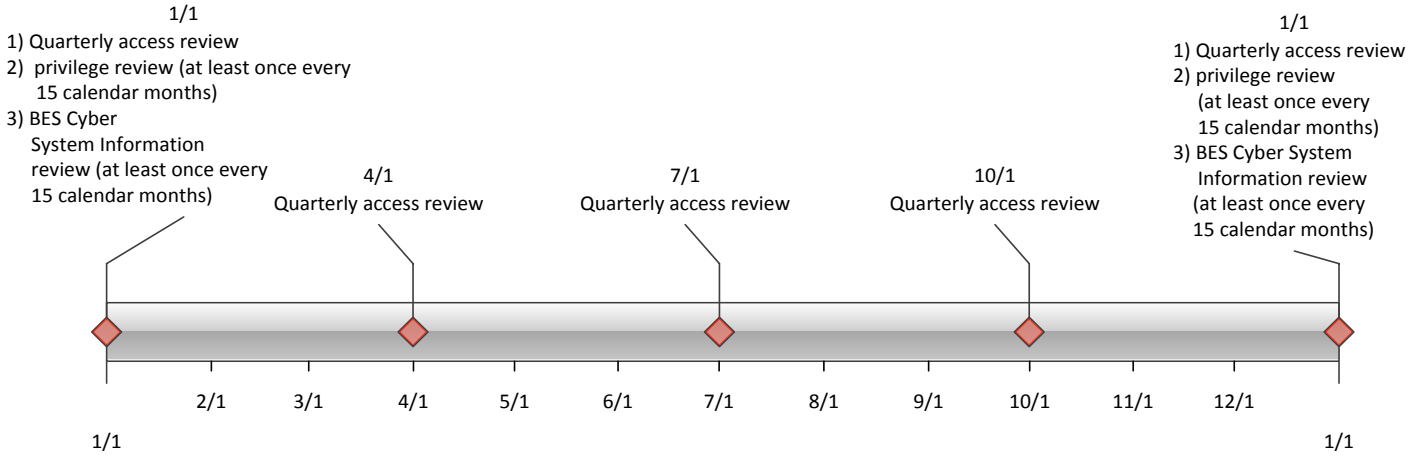
criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to



perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to

or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-~~5~~6

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

6. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security, which ~~, CIP-002-5~~ requires the initial identification and categorization of BES Cyber Systems~~, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies, . . .~~**

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of

300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access

authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6~~7~~ and 1.7~~8~~ beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-~~5~~ 6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-~~5~~ 6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-~~5~~ 6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~5~~ 6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-~~5~~6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~5~~ 6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	N/A The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR The	N/A The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to	N/A The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5) OR	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8)~~ ~~OR~~ ~~The Responsible Entity has a process to retain physical access logs for 90 calendar~~	~~identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7)~~ ~~OR~~ ~~The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)~~	~~The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not~~	~~documented and implemented operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1)~~ OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) ~~OR~~ ~~The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~days and identified deficiencies but did not assess or correct the deficiencies. (1.9)~~ ~~OR~~ ~~The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)~~		~~assess or correct the deficiencies. (1.6)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)~~	~~correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2)~~ OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) ~~OR~~ ~~The Responsible Entity documented and~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3)~~ OR The Responsible Entity does not have a process

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or correct the deficiencies. (1.4)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~identify, assess, or correct the deficiencies. (1.4)~~ OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical ~~security~~ Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-65)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)
R2	**Same-Day Operations**	**Medium**	N/A	N/A ~~The Responsible Entity included a visitor~~	N/A ~~The Responsible Entity included a visitor~~	The Responsible Entity has failed to include or implement a visitor control program that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~control program that requires logging of each of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or correct the deficiencies. (2.2)~~ ~~OR~~ ~~The Responsible Entity included a visitor~~	~~control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)~~	requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)~~		
R3	**Long Term Planning**	**Lower**	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete	The Responsible Entity ~~has~~ did not document~~ed and~~ or implement~~ed~~ a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6~~7~~ and 1.7~~8~~ beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-3 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-~~5~~6

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-007-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-6, Requirement R1, Part 1.2 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until six calendar months after the effective date of Reliability Standard CIP-007-6.

6. Background:

Standard CIP-007 ~~-5~~ exists as part of a suite of CIP Standards related to cyber security, which~~. CIP-002-5.1~~ requires the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ 2 and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on~~

~~*whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies,** . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is

specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-~~5~~ 6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or ~~removable~~ Removable ~~media~~Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-~~5~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-~~5~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-~~5~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-~~5~~ 6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-~~5~~ 6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

Rationale for Requirement R5 (continued):

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or ~~removable~~ Removable ~~media~~Media ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (1.2) ~~OR~~ ~~The Responsible Entity has~~	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (1.1) ~~OR~~ ~~The Responsible Entity has implemented and documented processes for determining~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R1) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R1 but did not identify, assess, or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)~~	~~necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)~~	~~the deficiencies. (R1)~~
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R2 ~~and has identified deficiencies but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but~~	sources, for tracking or evaluating cyber security patches for applicable Cyber Assets ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1)~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or~~	applicable Cyber Assets ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1)~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)~~ OR The Responsible Entity has documented and	~~not assess or correct the deficiencies~~. (R2)~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R2 but did not identify, assess, or correct the deficiencies. (R2)~~ OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35	~~correct the deficiencies. (2.1)~~ OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2)	implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for~~	security patches for applicable Cyber Assets~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1) ~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but less than 50 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation~~	OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct~~	~~applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation	The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.4)~~OR~~ ~~The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)~~	~~the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess,~~	plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an~~	~~not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4)~~ OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.4) ~~OR~~ ~~The Responsible Entity documented~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~or correct the deficiencies. (2.3)~~	~~existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)~~	~~a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the deficiencies. (2.4)~~
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns ~~and has identified deficiencies but did~~	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code ~~and has identified deficiencies but did not assess or correct~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R3 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R3) ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~not assess or correct the deficiencies~~. (3.3) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)~~	~~the deficiencies~~. (3.2)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and did not identify, assess, or correct the deficiencies. (3.2)~~ OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used,	~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R3 and did not identify, assess, or correct the deficiencies. (R3)~~ OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code~~ and has identified deficiencies but did not assess or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					the Responsible Entity did not update malicious code protections ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (3.3)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies.~~ ~~(3.3)~~	~~the deficiencies~~. (3.1) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.4) ~~The Responsible Entity has documented and~~	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2~~and has identified deficiencies but did not assess or correct the deficiencies~~. (4.2)~~OR~~ ~~The Responsible Entity has documented and~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R4 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R4)~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R4 and did not identify, assess, or correct the deficiencies. (R4)~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4~~	~~implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2)~~ OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3~~and has identified deficiencies but did not assess or correct the deficiencies~~. (4.1) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to log events for the~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.3) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional~~	~~Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3)~~OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals~~ and has identified deficiencies but did~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~not assess or correct the deficiencies~~. (4.4)~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)~~	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented	The Responsible Entity has implemented one or more documented	The Responsible Entity has implemented one or more documented	The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for~~	process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~The Responsible Entity has implemented one or more documented process(es) for password-only~~	process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the~~	more process(es) that included the applicable items in *CIP-007-~~5~~ 6 Table R5 ~~and has identified deficiencies but did not assess or correct the deficiencies~~*. (R5) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5)~~OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2)~~OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts~~ and has identified deficiencies but did~~	process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~not assess or correct the deficiencies~~. (5.3) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)~~OR The Responsible Entity has implemented one or more documented process(es) for password-only	authentication of interactive user access~~ and did not identify, assess, or correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.4) ~~OR~~ ~~The Responsible Entity has~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce	~~implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4)~~OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					one of the two password parameters as described in 5.5.1 and 5.5.2~~ and did not identify, assess, or correct the deficiencies~~. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months	described in 5.5.1 and 5.5.2~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.5) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify, assess,~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password~~	~~or correct the deficiencies. (5.5)~~ OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.7)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)~~

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for

individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, ~~portable storage media policies,~~ Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code

cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement but do not meet the additional obligations for transient devices.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible

Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of R~~r~~emovable M~~m~~edia in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor.

Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-~~5~~6

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-009 ~~-5~~ exists as part of a suite of CIP Standards related to cyber security, which ~~. CIP-002-5.1~~ require~~s~~ the initial identification and categorization of BES Cyber Systems ~~. CIP-003-5~~6, CIP-004-56, CIP-005-5, CIP-006-56, CIP-007-56, CIP-008-5, CIP-009-56, CIP-010-12, and CIP-011-1 2 and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies,** . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications*.

CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-~~5~~ 6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-6 5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-~~5~~ 6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-~~5~~ 6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-~~5~~ 6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-~~5~~ 6 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-~~5~~ 6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-~~5~~ 6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.
R2	**Operations**	**Lower**	The Responsible	The Responsible	The Responsible	The Responsible

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning **Real-time Operations**		Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests~~, and when tested, any~~	Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests~~, and when tested, any deficiencies were~~	Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests~~, and when tested, any~~	Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1)~~ ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)~~ ~~OR~~ The Responsible

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~deficiencies were identified, assessed, and corrected~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.3)	~~identified, assessed, and corrected~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.3)	~~deficiencies were identified, assessed, and corrected~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.3)	Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) ~~OR~~ ~~The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)~~ ~~OR~~ ~~The Responsible Entity has tested a~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified deficiencies, but did not assess or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~the deficiencies. (2.3)~~ ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)~~
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

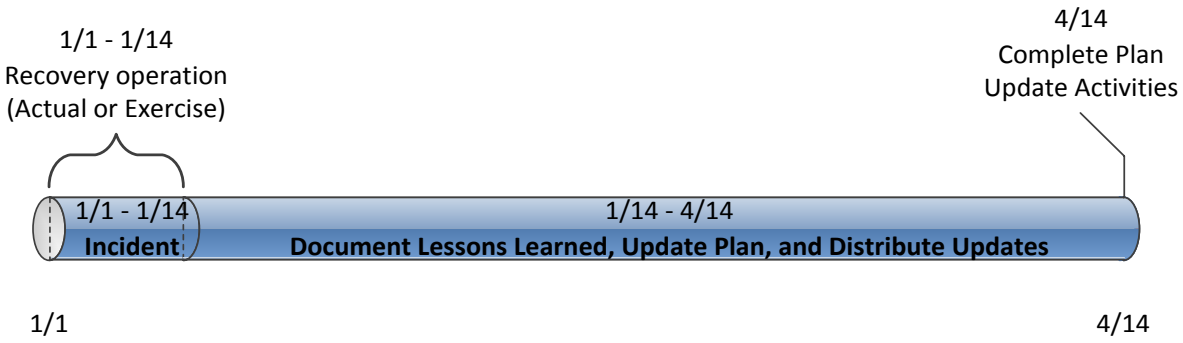


Figure 1: CIP-009-~~5~~ 6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

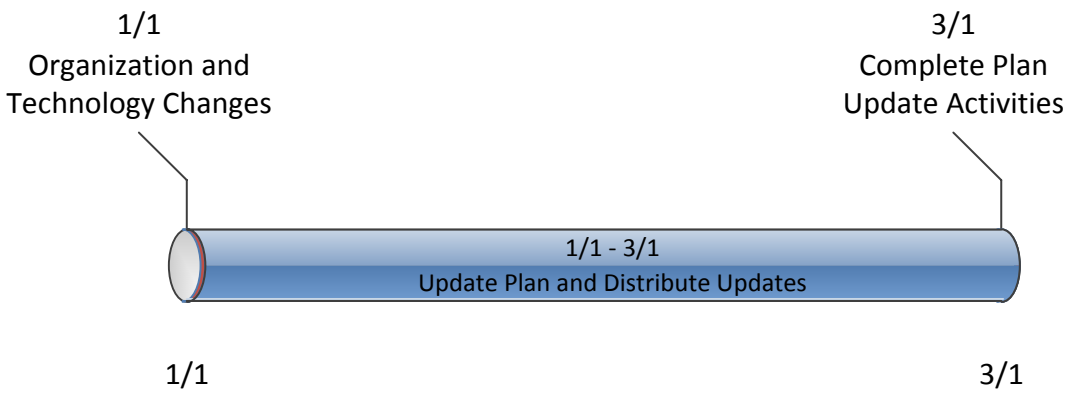


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-~~1~~2

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-~~1~~2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

6. Background:

Standard CIP-010 -1 exists as part of a suite of CIP Standards related to cyber security, which. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter. The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to

~~change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~ 2 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-~~1~~ 2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-~~1~~ 2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-~~1~~ 2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~ 2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~ 2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~1~~ 2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~1~~ 2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

Rationale for R4:

Requirement R4 is to address FERC Order No. 791 Paragraphs 6 and 136, which require the standards to address security-related issues associated with tools specifically used for data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To that end, the requirement goals are as follows:

(1) Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and

(2) Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

The SDT has incorporated the concepts of other requirements from FERC-approved CIP-010-1 and CIP-007-5 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: This is a new requirement. All requirements related to Transient Devices and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. While the requirements are similar, they are not to the same rigor of those found in CIP-007 protecting the permanent assets identified by an entity. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances. Authorization shall include: 4.1.1. Users, individually or by group/role; 4.1.2. Locations, individually or by group/role; 4.1.3. Defined acceptable use; and 4.1.4. Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the authorized software for each Transient Cyber Asset, individually or by group; or • A record in an asset management system that identifies the authorized configuration for each Transient Cyber Asset individually or by group.
4.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability).	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus hardening, policies, verification of method(s) employed by vendors, etc.).

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to detect malicious code on Removable Media prior to use on applicable systems.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus scanning techniques, verification of method(s) employed by vendors, etc.).
4.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
4.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.6	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4. For a modification that deviates from the state in Part 4.1.4, either: • Remediate by returning the Transient Cyber Asset to the state in Part 4.1.4; or • Update Part 4.1.4.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any remediation activities.
4.7	High Impact BES Cyber Systems and associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, within 35 calendar days prior to use, to ensure security patches are up-to-date. For security patches that are not up-to-date, take one of the following actions: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any mitigation activities.

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

b. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints Text

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified~~	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible	identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required	deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for	implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct~~	~~security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1)~~	~~changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to update~~	update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~the deficiencies in the verification documentation. (1.4.3)~~		~~baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the~~	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to verify that required security controls in~~	configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2)~~ ~~OR~~ ~~The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencie~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~(1.5.1)~~ ~~OR~~ ~~The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1)~~ ~~OR~~ ~~The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~identified deficiencies but did not assess or correct the deficiencies. (1.5.2)~~ ~~OR~~ ~~The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)~~OR~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~not identify, assess, or correct the deficiencies. (2.1)~~
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity did not document or implement process(es) that collectively address the requirement

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of Transient Cyber Assets, but failed to include one of the required items listed in 4.1.1 through 4.1.4. (4.1)	of Transient Cyber Assets, but failed to include two of the required items listed in 4.1.1 through 4.1.4. (4.1)	of Transient Cyber Assets, but failed to include three of the required items listed in 4.1.1 through 4.1.4. (4.1) OR The Responsible Entity documented and implemented a process to evaluate Transient Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 but did not take one of the actions required by Requirement R4, Part 4.6. (4.6) OR The Responsible Entity documented and implemented a process to evaluate	parts as required by Requirement R4. (R4) OR The Responsible Entity did not use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability) as required by Requirement R4, Part 4.2. (4.2) OR The Responsible Entity did not use method(s) to detect malicious code on Removable Media prior to use on applicable systems as required by Requirement R4, Part 4.3. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Transient Cyber Assets within 35 calendar days prior to use but did not take one of the actions required by Requirement R4, Part 4.7. (4.7)	OR The Responsible Entity did not mitigate the threat of detected malicious code for Transient Cyber Assets or Removable Media as required by Requirement R4, Part 4.4. (4.4) OR The Responsible Entity did not update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns as required by Requirement R4, Part 4.5. (4.5) OR The Responsible Entity did not evaluate Transient

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 as required by Requirement R4, Part 4.6. (4.6) OR The Responsible Entity did not evaluate Transient Cyber Assets within 35 calendar days prior to use as required by Requirement R4, Part 4.7. (4.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-~~5~~6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-~~5~~ 6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT

believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.

2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

This Requirement applies to any transient devices (i.e. Transient Cyber Assets and Removable Media) that will be connected temporarily to an applicable system. Examples of these devices include, but are not limited to:

- Hardware/software diagnostic test equipment
- Hardware/software packet sniffers
- Hardware/software used for BES Cyber System maintenance
- Hardware/software used for BES Cyber System configuration
- Hardware/software used to perform vulnerability assessments

Transient Cyber Assets can be in the form of a laptop, desktop, or tablet. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

This requirement does not cover hardware/software components that may support information system maintenance yet are a part of the system, for example the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of a switch.

Requirement Parts 4.1, 4.3, 4.6, and 4.7 refer to the term “prior to use” related to when specific actions must occur. For purposes of this standard, "use" is considered to be the interaction between transient devices and applicable systems. The interaction between transient devices and multiple applicable systems within the same ESP or PSP would be considered a single use. For example, a technician would need to have a laptop evaluated only once according to Part 4.6 when working in the same PSP. The technician would not need to have the evaluation performed each time it connects to a different Cyber Asset.

Requirement Part 4.1:

Requirement Part 4.1 requires the entity to document and implement its process to authorize the use of Transient Cyber Assets. This allows entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1. User(s), individually or by group/role, allowed to use Transient Cyber Assets. This is intended to provide assurance around who has physical proximity to the Transient Cyber Assets. These user(s) must have authorized electronic and unescorted physical access to the applicable system in accordance with CIP-004.
2. Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group/role of locations. Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e. high impact, medium impact, low impact). These impact areas have differing levels of protection under the CIP Requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. It may be reasonable to have separate Transient Cyber Assets for each impact level.
3. The intended or approved use of each Transient Cyber Asset. Activities not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals on the activities or uses that are not allowed (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).
4. The operating system, firmware, and intentionally installed software. All of this information may not be available or relevant to each Transient Cyber Asset. Having this information facilitates the review in Part 4.6. The use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The Standard Drafting Team does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included.

CAUTION: Entities should exercise caution when using Transient Cyber Assets and ensure they do not have wireless or Bluetooth features enabled in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber

Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Requirement Parts 4.2, 4.3, 4.4, and 4.5:

Requirement Parts 4.2 and 4.3 address the protection against the introduction of malicious code by Transient Cyber Assets or Removable Media. For Transient Cyber Assets, the entity may either pre-authorize an inventory of Cyber Assets or authorize devices at the time of connection. Pre-authorized Transient Cyber Assets may have the malicious code prevention maintained on the device and do not require specific actions for each use.

It is the responsibility of the entity to ensure that the Transient Cyber Assets it owns and manages have methods deployed to deter, detect, or prevent malicious code. It is also the entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not own or manage, including vendor assets.

For Removable Media and Transient Cyber Assets authorized at the time of connection, the detection of malicious code must be addressed prior to use. This can be performed by scanning the Transient Cyber Assets or Removable Media in an environment outside of the Electronic Security Perimeter (ESP). Entities should use caution not to place kiosks or other scanning devices used to comply with this Requirement inside the ESP.

For Requirement R4, Part 4.4, if malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Part 4.5 requires a process to update signatures or patterns, where applicable. This process is to be documented in the overarching program. As with CIP-007-6, Requirement R3, the process is to include testing and installing of updated signatures or patterns.

Requirement Parts 4.6 and 4.7:

Requirement R4, Part 4.6 requires the entity to evaluate Transient Cyber Assets to ensure that no unauthorized modifications have been made to the operating system, firmware, or software. This is a review of the current state against what is currently documented pursuant to Part 4.1.4. If there are differences, the modified code may be removed or the documentation updated to align to the authorized or current state.

Similarly, Requirement R4, Part 4.7 requires the entity to evaluate Transient Cyber Assets to ensure that patches are up-to-date. This is a review of the patches currently installed against what is currently documented. If there are missing patches, these should be tested and applied or a mitigation plan should be created to mitigate the vulnerabilities addressed by each uninstalled security patch. This should be performed prior to connecting the Transient Cyber Asset to an applicable system. For a device that the entity does not manage (i.e. vendor laptop), this can be performed immediately prior to connecting the Transient Cyber Asset to an applicable system. For an entity-managed device, the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-~~1~~2

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-~~1~~2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-011-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-011 ~~-1~~ exists as part of a suite of CIP Standards related to cyber security, which~~. CIP-002-5~~ require~~s~~ the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies, . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it~~-~~ believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-~~1~~ 2 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~1~~ 2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~1~~ 2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-~~1~~ 2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify,~~	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~assess, or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~but did not identify, assess, or correct the deficiencies. (1.2)~~	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset, Transient Cyber Asset, or Removable Media is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
Laura.Hussey@nerc.net
For questions about this form or for assistance in completing the form, call Laura Hussey at 404-446-2579.

NERC welcomes suggestions for improving the reliability of the Bulk-Power System through improved Reliability Standards. Please use this form to submit your proposal for a new NERC Reliability Standard or a revision to an existing standard.

Request to propose a new or a revision to a Reliability Standard			
Proposed Standard:	Project 2014-03 Revisions to the TOP/IRO Reliability Standards		
Date Submitted:	February 12, 2014		
SAR Requester Information			
Name:	David Souder		
Organization:	PJM		
Telephone:	610-666-4795	E-mail:	souder@pjm.com
SAR Type (Check as many as applicable)			
☒ New Standard ☒ Revision to existing Standard		☐ Withdrawal of existing Standard ☐ Urgent Action	

SAR Information
Industry Need (What is the industry problem this request is trying to solve?):
On April 16, 2013, NERC submitted two petitions requesting Commission approval of TOP and IRO standards. One petition addresses three revised TOP Reliability Standards: TOP-001-2 (Transmission Operations), TOP-002-3 (Operations Planning), TOP-003-2 (Operational Reliability Data), and one Protection Systems (PRC) Reliability Standard, PRC-001-2 (System Protection Coordination) (collectively, the "TOP Standards") to replace the eight currently-effective TOP standards. The second petition addresses four revised IRO Reliability Standards: IRO-001-3 (Responsibilities and Authorities), IRO-002-3 (Analysis Tools), IRO-005-4 (Current Day Operations), and IRO-014-2 (Coordination Among Reliability Coordinators) (collectively, the "IRO Standards") to replace six currently-effective IRO standards. On November 21, 2013, the Commission issued a NOPR in response to these petitions. The NOPR proposed to remand the proposed TOP and IRO Standards. In the NOPR, the Commission raises a concern that NERC "has removed critical reliability aspects that are included in the currently-effective standards without adequately addressing these aspects in the proposed standards." For example, the Commission cites the fact that the proposed TOP standards do not require Transmission Operators to plan and operate within all System Operating Limits ("SOLs"), which is a requirement in the currently effective standards. On December 20, 2013, NERC filed a motion requesting that the Commission defer action on the NOPR until January 31, 2015 to provide NERC and the industry the opportunity to thoroughly examine the technical concerns raised in the NOPR. This deferral would provide an opportunity for the industry, NERC, and FERC to work toward a common understanding and afford time to review the proposed TOP and IRO standards through the NERC standards development process to address the concerns set forth in the NOPR. That motion to defer action was granted by the Commission on January 14, 2014.
SAR Information
Purpose or Goal (How does this request propose to address the problem described above?):
The primary goal of this SAR is to allow the Standard Drafting Team (SDT) for Project 2014-03 Revisions to TOP/IRO Reliability Standards to address the concerns expressed in the NOPR while fulfilling the goals of the original projects: Project 2006-06 Reliability Coordination and Project 2007-03 Real-time Operations. In addition, the SDT should review the goals of Project 2009-02 Real-time Monitoring and Analysis Capabilities and consider whether to incorporate revisions to the TOP and/or IRO standards to address those goals in Project 2014-03.

SAR Information
Identify the Objectives of the proposed standard's requirements (What specific reliability deliverables are required to achieve the goal?):
Provide clear, unambiguous requirements and standards to allow Reliability Coordinators, Transmission Operators, and Balancing Authorities to operate the interconnected transmission system in a safe and reliable manner.
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The SDT shall modify the TOP and IRO Reliability Standards to address the issues raised in the NOPR, while ensuring that the revisions continue to address directives previously assigned to the TOP and IRO standards under Projects 2007-03 and 2006-06. If it is decided to handle the goals of Project 2009-02 within Project 2014-03, then the directives assigned to Project 2009-02 will be addressed as well. In addition, the ~~suggestions~~ recommendations from the Independent Expert Review Project and the SW Outage Report will be reviewed, a directive dealing with monitoring responsibilities for the Reliability Coordinator will be resolved, and other IRO standards will be examined for consistency purposes.
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
The SDT shall: 1. Revise the TOP/IRO Reliability Standards to address concerns expressed in the NOPR a. ~~Use~~ Consider the inputs from technical conferences ~~to advise actions~~ 2. Consider the ~~comments and suggestions~~ recommendations in the Independent Expert Review Report and the SW Outage Report 3. Review the IRO Reliability Standards not included in the original Project 2006-06 for coordination with any changes made for this project (see list of related standards) 4. Preserve the intent of the reliability objectives in the current, approved standards so that no reliability gaps are created ~~4.~~5. Decide whether to handle the goals of Project 2009-02 within Project 2014-03; and if it does so decide, then also address the directives assigned to Project 2009-02. 6. Address the directives from Order 693 originally assigned to Projects 2006-06 and 2007-03.

SAR Information
~~5.~~7. Address the following directive from Order 693, paragraph 1855 ~~so that all monitoring responsibilities for the Reliability Coordinator are included in the IRO family of standards~~: "*Since a reliability coordinator is the highest level of authority overseeing the reliability of the Bulk-Power System, the Commission believes that it is important to include the reliability coordinator as an applicable entity to assure that adequate voltage and reactive resources are being maintained. As MISO points out, other Reliability Standards address responsibilities of reliability coordinators, but we agree with EEI that it is important to include reliability coordinators in VAR-001-1 as well. Reliability coordinators have responsibilities in the IRO and TOP Reliability Standards, but not the specific responsibilities for voltage levels and reactive resources addressed by VAR-001-1, which have a great impact on system reliability. For example, voltage levels and reactive resources are important factors to ensure that IROLs are valid and operating voltages are within limits, and that reliability coordinators should have responsibilities in VAR-001-1 to monitor that sufficient reactive resources are available for reliable system operations. Accordingly, the ERO should modify VAR-001-1 to include reliability coordinators as applicable entities and include a new requirement(s) that identifies the reliability coordinator's monitoring responsibilities*." 8. Modify the measures, Violation Risk Factors (VRF), and Violation Severity Levels (VSL) as necessary to address modified requirements. 9. Address the issue of outage coordination as pointed out by the Independent Experts Review Panel through the creation of a new standard. ~~6.~~10. Address the recommendations of the IRO Five Year Review Team (Project 2012-09) for the IRO standards revised in this project.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.

Reliability Functions		
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☒	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☒	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☒	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.

Reliability Functions	
☐ Market Operator	Interface point for reliability functions with commercial functions.
☒ Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.
Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to	Yes

Reliability and Market Interface Principles	
access commercially non-sensitive information that is required for compliance with reliability standards.	

Related Standards	
Standard No.	Explanation
IRO-003-2 IRO-004-2	May n~~N~~eed~~s~~ to be reviewed for language and terminology consistency with revisions made in this project.
IRO-006-5	
IRO-008-1	
IRO-009-1	
IRO-010-1a	
IRO-015-1	
IRO-016-1	

Related SARs	
SAR ID	Explanation
N/A	N/A

Regional Variances	
Region	Explanation
ERCOT	N/A
FRCC	N/A
MRO	N/A
NPCC	N/A

Regional Variances	
RFC	N/A
SERC	N/A
SPP	N/A
WECC	N/A

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-03 Revisions to TOP and IRO Standards

Formal Comment Period Now Open through July 2, 2014
Ballot Pools Forming Now through June 17, 2014

Upcoming:

Ballots and Non-Binding Polls: June 23 – July 2, 2014

Now Available

A 45-day formal comment period for the **TOP/IRO Reliability Standards** is open through **8 p.m. Eastern on Wednesday, July 2, 2014.** The join ballot pool windows are currently open through **8 p.m. Eastern on Tuesday, June 17, 2014.**

If you have questions please contact Ed Dobrowolski via email or by telephone at (609) 947-3673.

Background information for this project can be found on the project page.

Instructions for Commenting

Please use the electronic form to submit comments on the standards. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Instructions for Joining Ballot Pool

Two ballots pools are being formed for Project 2014-03 – one for the TOP and IRO Reliability Standards and one for the associated non-binding polls on this project. Registered Ballot Body members must join the ballot pools to be eligible to vote in the balloting and submittal of an opinion for the non-binding poll of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs). Registered Ballot Body members may join the ballot pools at the following page: Join Ballot Pool

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list servers for this project are:

Ballot: bp-2014-03 TOP/IRO_STDS_in@nerc.com
Non-Binding Poll: bp-2014-03 TOP/IRO_NB_in@nerc.com

Next Steps

Ballots for the standards and non-binding polls of the associated VRFs and VSLs will be conducted **June 23 – July 2, 2014.**

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
1	Project 2007-24	Request for Interpretation - TPL-002 and TPL-003 - Ameren_in	Initial Ballot	4/25/2008	5/7/2008	Quorum: 82.61% Approval: 80.73%			
2	Project 2007-26	Request for Interpretation - TPL-002 and TPL-003 - MISO_in	Initial Ballot	4/25/2008	5/7/2008	Quorum: 83.01% Approval: 79.89%			
3	Project 2008-04	FAC-010_FAC-011_FAC-014_Order_705_in	Initial Ballot	6/2/2008	6/11/2008	Quorum: 88.83% Approval: 95.43%			
4	Project 2008-07	Interpretation Request - EOP-002 - Brookfield_in	Initial Ballot	6/2/2008	6/11/2008	Quorum: 89.67% Approval: 76.47%			
5	Project 2008-04	FAC-010_FAC-011_FAC-014_Order_705_rc	Recirculation Ballot	6/13/2008	6/22/2008	Quorum: 89.36% Approval: 95.21%			
6	Project 2008-09	Request for Interpretation - EOP-001-0 - RECM_in	Initial Ballot	6/19/2008	7/2/2008	Quorum: 84.82% Approval: 85.79%			
7	Project 2007-24	Request for Interpretation - TPL-002 and TPL-003 - Ameren_rc	Recirculation Ballot	6/27/2008	7/7/2008	Quorum: 83.57% Approval: 79.13%			
8	Project 2007-26	Request for Interpretation - TPL-002 and TPL-003 - MISO_rc	Recirculation Ballot	6/27/2008	7/7/2008	Quorum: 83.98% Approval: 78.31%			
9	Pre-2006	IROL Standard - IRO-010_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 92.71% Approval: 88.40%			
10	Pre-2006	IROL Standard - IRO-009_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 92.63% Approval: 89.44%			
11	Pre-2006	IROL Standard - IRO-008_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 92.67% Approval: 91.71%			
12	Project 2006-07	ATC et al Standard - MOD-030_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.37% Approval: 56.56%			
13	Project 2006-07	ATC et al Standard - MOD-029_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.67% Approval: 92.62%			
14	Project 2006-07	ATC et al Standard - MOD-028_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.64% Approval: 79.47%			
15	Project 2006-07	ATC et al Standard - MOD-008_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.27% Approval: 80.44%			
16	Project 2006-07	ATC et al Standard - MOD-001_in	Initial Ballot	7/21/2008	7/30/2008	Quorum: 94.02% Approval: 75.97%			
17	Project 2008-10	Request for Interpretation - CIP-006-1 - Progress Energy_in	Initial Ballot	8/7/2008	8/16/2008	Quorum: 88.18% Approval: 21.52%			
18	Pre-2006	IROL Standard - IRO-008_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 93.72% Approval: 89.49%			
19	Pre-2006	IROL Standard - IRO-009_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 93.68% Approval: 86.53%			
20	Pre-2006	IROL Standard - IRO-010_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 93.75% Approval: 85.95%			
21	Project 2006-07	ATC et al Standards - MOD-001_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 94.87% Approval: 76.83%			
22	Project 2006-07	ATC et al Standard - MOD-008_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 95.15% Approval: 81.49%			
23	Project 2006-07	ATC et al Standard - MOD-028_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 95.54% Approval: 79.34%			
24	Project 2006-07	ATC et al Standard - MOD-029_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 95.56% Approval: 92.24%			
25	Project 2006-07	ATC et al Standard - MOD-030_rc	Recirculation Ballot	8/12/2008	8/21/2008	Quorum: 95.24% Approval: 74.26%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
26	Project 2008-11	Request for Interpretation - VAR-002-1 - ICF Consulting_in	Initial Ballot	9/9/2008	9/17/2008	Quorum: 85.78% Approval: 90.37%			
27	Project 2006-07	ATC et al Standard - MOD-004_in	Initial Ballot	9/11/2008	9/21/2008	Quorum: 79.26% Approval: 66.29%			
28	Project 2007-14	Permanent Changes to CI Timing Tables_in	Initial Ballot	9/12/2008	9/22/2008	Quorum: 79.74% Approval: 100.00%			
29	Project 2008-07	Request for Interpretation - Brookfield Power - EOP-002_rb	Re-ballot	10/6/2008	10/24/2008	Quorum: 82.61% Approval: 74.67%			
30	Project 2008-13	Request for Interpretation - TOP-002-2 - Orlando Utilities Commission_in	Initial Ballot	10/21/2008	10/30/2008	Quorum: 83.33% Approval: 96.94%			
31	Project 2006-01	Project 2006-01 - PER-005-1_in	Initial Ballot	10/27/2008	11/5/2008	Quorum: 90.13% Approval: 82.47%			
32	Project 2006-09	Project 2006-09 - FAC-008-2 - Facility Ratings_in	Initial Ballot	10/27/2008	11/5/2008	Quorum: 89.13% Approval: 70.01%			
33	Project 2006-07	ATC et al Standard - MOD-004_rc	Recirculation Ballot	10/28/2008	11/6/2008	Quorum: 91.49% Approval: 83.71%			
34	Project 2006-07	Project 2006-07 (ATC) MOD-030-2_in	Initial Ballot	12/1/2008	12/10/2008	Quorum: 83.77% Approval: 86.51%			
35	Project 2006-09	Project 2006-09 - FAC-008-2 - Facility Ratings_rc	Recirculation Ballot	12/10/2008	12/19/2008	Quorum: 93.04% Approval: 57.37%			
36	Project 2008-13	Request for Interpretation - TOP-002-2 - Orlando Utilities Commission_rc	Recirculation Ballot	12/10/2008	12/19/2008	Quorum: 87.62% Approval: 97.47%			
37	Project 2006-01	Project 2006-01 - PER-005-1_rc	Recirculation Ballot	12/12/2008	12/22/2008	Quorum: 91.48% Approval: 80.63%			
38	Project 2008-15	Request for Interpretation - CIP-006-1a - US Army COE_in	Initial Ballot	1/5/2009	1/14/2009	Quorum: 91.15% Approval: 97.39%			
39	Project 2008-16	TOP-004-2 VSL Revisions_in	Initial Ballot	1/5/2009	1/14/2009	Quorum: 91.20% Approval: 93.93%			
40	Project 2008-11	Request for Interpretation - VAR-002-1 - ICF Consulting_rc	Recirculation Ballot	1/6/2009	1/15/2009	Quorum: 91.47% Approval: 91.21%			
41	Project 2006-07	Project 2006-07 (ATC) MOD-030-2_rc	Recirculation Ballot	1/20/2009	1/29/2009	Quorum: 85.86% Approval: 86.39%			
42	Project 2008-16	TOP-004-2 VSL Revisions_rc	Recirculation Ballot	1/28/2009	2/6/2009	Quorum: 92.59% Approval: 96.06%			
43	Project 2008-15	Request for Interpretation - CIP-006-1a - US Army COE_rc	Recirculation Ballot	2/6/2009	2/16/2009	Quorum: 93.81% Approval: 99.12%			
44	Project 2008-09	Interpretation Request - EOP-001 - R1 - RECM_in	Initial Ballot	2/27/2009	3/9/2009	Quorum: 89.67% Approval: 89.03%			
45	Project 2008-18	Project 2008-18 Interpretation-Manitoba Hydro_in	Initial Ballot	3/19/2009	3/30/2009	Quorum: 89.78% Approval: 92.62%			
46	Project 2008-06	Project 2008-06: CIP-002-1-CIP-009-1 Revisions_in	Initial Ballot	4/1/2009	4/10/2009	Quorum: 91.90% Approval: 84.06%			
47	Project 2009-10	Project 2009-10 Interpretation - CMPWG - PRC-005-1 R1_in	Initial Ballot	4/8/2009	4/17/2009	Quorum: 92.70% Approval: 92.71%			
48	Project 2006-03	Project 2006-03 EOP-001_EOP-005_EOP-006 System Restoration and Blackstart_in	Initial Ballot	4/14/2009	4/23/2009	Quorum: 89.81% Approval: 76.63%			
49	Project 2008-06	Project 2008-06: CIP-002-1-CIP-009-1 Revisions_rc	Recirculation Ballot	4/17/2009	4/27/2009	Quorum: 94.37% Approval: 88.32%			
50	Project 2008-18	Project 2008-18 Interpretation-Manitoba Hydro_rc	Recirculation Ballot	4/17/2009	4/27/2009	Quorum: 95.56% Approval: 92.81%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
51	Project 2009-11	Project 2009-11 Interpretation WECC Reliability Coordination Subcommittee IRO-10-1_in	Initial Ballot	4/22/2009	5/1/2009	Quorum: 88.64% Approval: 84.77%			
52	Project 2006-03	Project 2006-03 EOP-001_EOP-005_EOP-006 System Restoration and Blackstart_rc	Recirculation Ballot	5/6/2009	5/18/2009	Quorum: 92.08% Approval: 75.39%			
53	Project 2009-15	Project 2009-15 Interpretation - NYISO - MOD-001-1, MOD-029-1_in	initial Ballot	5/25/2009	6/4/2009	Quorum: 85.13% Approval: 82.10%			
54	Project 2009-11	Project 2009-11 Interpretation WECC Reliability Coordination Subcommittee IRO-10-1_rc	Recirculation Ballot	5/26/2009	6/5/2009	Quorum: 90.45% Approval: 85.76%			
55	Project 2009-14	Project 2009-14 Interpretation - PacifiCorp - TPL-002-0a_in	Initial Ballot	6/1/2009	6/11/2009	Quorum: 87.10% Approval: 95.71%			
56	Project 2009-08	Project 2009-08 - Nuclear Plant Interface Coordination for Order 716_in	Initial Ballot	6/12/2009	6/22/2009	Quorum: 81.72% Approval: 94.09%			
57	Project 2008-14	Project 2008-14 VSLs for CIP-002-1 through CIP-009-1_in	Initial Ballot	6/15/2009	6/24/2009	Quorum: 87.23% Approval: 83.94%			
58	Project 2008-14	Project 2008-14 VSLs for CIP-002-1 through CIP-009-1_rc	Recirculation Ballot	7/7/2009	7/16/2009	Quorum: 92.77% Approval: 84.96%			
59	Project 2009-15	Project 2009-15 Interpretation - NYISO - MOD-001-1, MOD-029-1_rc	Recirculation Ballot	7/8/2009	7/17/2009	Quorum: 90.26% Approval: 82.25%			
60	Project 2009-08	Project 2009-08 - Nuclear Plant Interface Coordination for Order 716_rc	Recirculation Ballot	7/10/2009	7/20/2009	Quorum: 87.10% Approval: 96.94%			
61	Project 2009-10	Project 2009-10 Interpretation - CMPWG - PRC-005-1 R1_rc	Recirculation Ballot	7/24/2009	8/6/2009	Quorum: 95.26% Approval: 95.62%			
62	Project 2009-14	Project 2009-14 Interpretation - PacifiCorp - TPL-002-0a_rc	Recirculation Ballot	7/24/2009	8/6/2009	Quorum: 91.24% Approval: 98.85%			
63	Project 2007-23	Project 2007-23 TPL Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 85.71% Approval: 90.46%			
64	Project 2007-23	Project 2007-23 TOP Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.40% Approval: 89.14%			
65	Project 2007-23	Project 2007-23 PRC Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.32% Approval: 88.26%			
66	Project 2007-23	Project 2007-23 IRO Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.16% Approval: 90.15%			
67	Project 2007-23	Project 2007-23 INT, PER, and NUC Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 85.71% Approval: 88.63%			
68	Project 2007-23	Project 2007-23 FAC and MOD Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.64% Approval: 87.63%			
69	Project 2007-23	Project 2007-23 CIP, COM, and VAR Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.50% Approval: 85.78%			
70	Project 2007-23	Project 2007-23 BAL Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 86.28% Approval: 89.56%			
71	Project 2008-08	Project 2008-08 EOP Violation Severity Levels_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 87.98% Approval: 87.31%			
72	Project 2009-17	Project 2009-17 Interpretation - Y-W Electric and Tri-State - PRC-004-1 and PRC-005-1_in	Initial Ballot	7/31/2009	8/10/2009	Quorum: 90.32% Approval: 62.15%			
73	RSDP V7	Reliability Standards Development Procedure - Version 7 - June 2009_rb	Re-ballot	7/27/2009	8/14/2009	Quorum: 84.65% Approval: 74.79%			
74	Project 2009-09	Project 2009-09 - Interpretation - Covanta Energy - CIP-001-1_in	Initial Ballot	8/6/2009	8/17/2009	Quorum: 84.68% Approval: 68.92%			
75	Project 2007-23	Project 2007-23 TPL Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 91.96% Approval: 89.28%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
76	Project 2007-23	Project 2007-23 BAL Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.04% Approval: 89.41%			
77	Project 2007-23	Project 2007-23 CIP, COM, and VAR Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.41% Approval: 84.64%			
78	Project 2007-23	Project 2007-23 FAC and MOD Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.67% Approval: 88.04%			
79	Project 2007-23	Project 2007-23 INT, PER, and NUC Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.17% Approval: 88.73%			
80	Project 2007-23	Project 2007-23 IRO Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 91.96% Approval: 90.77%			
81	Project 2007-23	Project 2007-23 PRC Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.31% Approval: 86.93%			
82	Project 2007-23	Project 2007-23 TOP Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.11% Approval: 88.26%			
83	Project 2008-08	Project 2008-08 EOP Violation Severity Levels_rc	Recirculation Ballot	8/17/2009	8/27/2009	Quorum: 92.70% Approval: 85.80%			
84	Order 706-B	Order 706-B Nuclear Implementation Plan_in	Initial Ballot	8/19/2009	8/28/2009	Quorum: 81.96% Approval: 97.37%			
85	Project 2008-07	Request for Interpretation - Brookfield Power - EOP-002_rc	Recirculation Ballot	8/20/2009	8/31/2009	Quorum: 86.96% Approval: 70.85%			
86	Project 2009-12	Project 2009-12 - Interpretation - PacifiCorp - CIP-005-1_in	Initial Ballot	8/27/2009	9/8/2009	Quorum: 84.68% Approval: 80.37%			
87	Project 2009-13	Project 2009-13 - Interpretation - PacifiCorp - CIP-006-1_in	Initial Ballot	8/27/2009	9/8/2009	Quorum: 84.92% Approval: 79.04%			
88	Project 2009-18	Project 2009-18 - Withdraw Three Midwest ISO Waivers_in	Initial Ballot	8/27/2009	9/8/2009	Quorum: 85.28% Approval: 99.62%			
89	Order 706-B	Order 706-B Nuclear Implementation Plan_rc	Recirculation Ballot	9/1/2009	9/10/2009	Quorum: 87.11% Approval: 97.18%			
90	RSDP V7	Reliability Standards Development Procedure - Version 7 - June 2009_rc	Recirculation Ballot	9/2/2009	9/14/2009	Quorum: 86.31% Approval: 76.09%			
91	Project 2008-06	Project 2008-06 Cyber Security (VRFs and VSLs for Version 2 CIP Standards)_in	Initial Ballot	9/10/2009	9/21/2009	Quorum: 87.45% Approval: 94.18%			
92	Project 2009-16	Project 2009-16 - Interpretation - WECC - CIP-007-1_in	Initial Ballot	9/9/2009	9/21/2009	Quorum: 85.31% Approval: 100.00%			
93	Project 2006-04	Project 2006-04 - Back-up Facilities - EOP-008-1_in	Initial Ballot	9/16/2009	9/28/2009	Quorum: 82.69% Approval: 72.86%			
94	Project 2009-09	Project 2009-09 - Interpretation - Covanta Energy - CIP-001-1_rc	Recirculation Ballot	9/29/2009	10/9/2009	Quorum: 89.92% Approval: 68.31%			
95	Project 2008-10	Project 2008-10 - Interpretation of CIP-006-1 Revised R1 for Progress Energy	Initial Ballot	9/30/2009	10/12/2009	Quorum: 79.92% Approval: 74.47%			
96	Project 2009-12	Project 2009-12 - Interpretation - PacifiCorp - CIP-005-1_rc	Recirculation Ballot	10/16/2009	10/26/2009	Quorum: 86.29% Approval: 83.25%			
97	Project 2008-06	Project 2008-06 Cyber Security (VRFs and VSLs for Version 2 CIP Standards)_rc	Recirculation Ballot	11/2/2009	11/12/2009	Quorum: 88.70% Approval: 94.24%			
98	Project 2008-09	Project 2008-09 - Interpretation - RECM - Revision 2_in	Initial Ballot	11/5/2009	11/16/2009	Quorum: 85.97% Approval: 98.07%			
99	Project 2009-21	Project 2009-21 - Cyber Security Ninety-day Response_in	Initial Ballot	11/20/2009	11/30/2009	Quorum: 89.58% Approval: 88.07%			
100	Project 2009-17	Project 2009-17 - Interpretation Y-W Electric and Tri-State (Revision 1)_in	Initial Ballot	11/19/2009	12/7/2009	Quorum: 85.83% Approval: 58.91%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
101	Project 2009-20	Project 2009-20 - Interpretation - BAL-003-0 - Energy Mark, Inc. in	Initial Ballot	11/20/2009	12/7/2009	Quorum: 87.11% Approval: 93.40%			
102	Project 2009-21	Project 2009-21 - Cyber Security Ninety-day Response rc	Recirculation Ballot	12/3/2009	12/14/2009	Quorum: 93.33% Approval: 85.55%			
103	Project 2009-23	Project 2009-23 - Interpretation - CIP-004-2 - U.S. Army Corps of Engineers in	Initial Ballot	12/1/2009	12/14/2009	Quorum: 86.13% Approval: 72.11%			
104	Project 2009-13	Project 2009-13 - Interpretation - PacifiCorp - CIP-006-1 rc	Recirculation Ballot	12/11/2009	12/23/2009	Quorum: 90.08% Approval: 78.77%			
105	Project 2009-24	Project 2009-24 - Interpretation - FMPA - EOP-005-1 in	Initial Ballot	1/5/2010	1/15/2010	Quorum: 87.68% Approval: 17.79%			
106	Project 2009-25	Project 2009-25 - Interpretation - BPA - BAL-001-01.a and BAL-002-0 in	Initial Ballot	1/5/2010	1/15/2010	Quorum: 88.00% Approval: 34.28%			
107	Project 2009-26	Project 2009-26 - Interpretation - WECC - CIP-004-1 in	Initial Ballot	1/6/2010	1/19/2010	Quorum: 84.21% Approval: 42.24%			
108	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-2	Initial Ballot	1/12/2010	1/22/2010	Quorum: 89.16% Approval: 75.16%			
109	Project 2009-27	Project 2009-27 - Interpretation - TOP-002-2a for FMPAA in	Initial Ballot	2/10/2010	2/22/2010	Quorum: 84.98% Approval: 90.82%			
110	Project 2009-28	Project 2009-28 - Interpretation - EOP-001-1 and EOP-001-2 for FMPP in	Initial Ballot	2/10/2010	2/22/2010	Quorum: 87.36% Approval: 91.79%			
111	Project 2009-29	Project 2009-29 - Interpretation - TOP-002-2a for FMPP in	Initial Ballot	2/11/2010	2/22/2010	Quorum: 84.34% Approval: 84.56%			
112	Project 2009-19	Project 2009-19 - Interpretation - BAL-002-0 Northwest Power Pool RSG in	Initial Ballot	2/15/2010	2/26/2010	Quorum: 89.83% Approval: 48.60%			
113	Project 2009-20	Project 2009-20 - Interpretation - BAL-003-0 - Energy Mark, Inc. rc	Recirculation Ballot	2/16/2010	2/26/2010	Quorum: 92.44% Approval: 91.90%			
114	Project 2009-30	Project 2009-30 - Interpretation - PRC-001-1 for WPSC in	Initial Ballot	2/15/2010	2/26/2010	Quorum: 89.51% Approval: 48.74%			
115	Project 2006-02	Project 2006-02 - Assess Transmission Future Needs - TPL-001-1 in	Initial Ballot	2/19/2010	3/1/2010	Quorum: 91.38% Approval: 35.36%			
116	Project 2009-31	Project 2009-31 - Interpretation - TOP-001-1 for FMPP in	Initial Ballot	3/3/2010	3/16/2010	Quorum: 88.24% Approval: 98.27%			
117	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-2	Recirculation Ballot	3/8/2010	3/18/2010	Quorum: 93.71% Approval: 78.15%			
118	Project 2009-32	Project 2009-32 - Interpretation - EOP-003-1 for FMPP rb	Re-ballot	3/10/2010	3/31/2010	Quorum: 91.37% Approval: 77.66%			
119	Project 2009-23	Project 2009-23 - Interpretation - CIP-004-2 - U.S. Army Corps of Engineers (Revision 1) in	Initial Ballot	3/29/2010	4/8/2010	Quorum: 88.52% Approval: 63.43%			
120	Project 2008-09	Project 2008-09 - Interpretation - RECM - Revision 3 in	Initial Ballot	4/15/2010	4/26/2010	Quorum: 81.97% Approval: 98.64%			
121	SPM	Standards Process Manual Revisions in	Initial Ballot	4/19/2010	4/29/2010	Quorum: 87.82% Approval: 80.48%			
122	Project 2009-17	Project 2009-17 - Interpretation Y-W Electric and Tri-State (Revision 2) in	Initial Ballot	4/28/2010	5/10/2010	Quorum: 83.15% Approval: 74.55%			
123	SPM	Standards Process Manual Revisions rc	Recirculation Ballot	4/30/2010	5/10/2010	Quorum: 93.73% Approval: 86.69%			
124	Project 2010-11	Project 2010-11 SAR for TPL Table 1 Order in	Initial Ballot	5/17/2010	5/27/2010	Quorum: 84.41% Approval: 63.75%			
125	Project 2010-09	Project 2010-09: NUC Implementation Plans for CIP Version 2 and Version 3 in	Initial Ballot	5/19/2010	6/1/2010	Quorum: 84.83% Approval: 90.83%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
126	Project 2010-09	Project 2010-09: NUC Implementation Plans for CIP Version 2 and Version 3_rc	Recirculation Ballot	6/22/2010	7/2/2010	Quorum: 89.10% Approval: 87.24%			
127	Project 2006-04	Project 2006-04 - Backup Facilities - Revision 1_in	Initial Ballot	6/23/2010	7/6/2010	Quorum: 89.05% Approval: 79.45%			
128	Project 2006-08	Project 2006-08 - Reliability Coordination - Transmission Loading Relief_in	Initial Ballot	6/23/2010	7/6/2010	Quorum: 87.04% Approval: 84.98%			
129	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Initial Ballot	7/7/2010	7/17/2010	Quorum: 86.94% Approval: 43.13%			
130	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005-2	Initial Ballot	7/8/2010	7/17/2010	Quorum:91.12 % Approval: 22.91%			
131	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005-2	Non-binding Poll	7/8/2010	7/17/2010	Quorum: 86.00% Approval: 28.00%			
132	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: Protection System definition	Initial Ballot	7/8/2010	7/17/2010	Quorum: 87.85% Approval: 39.35%			
133	Project 2007-07	Project 2007-07 Vegetation Management: FAC-003-2	Initial Ballot	7/9/2010	7/19/2010	Quorum: 86.18% Approval: 65.93%			
134	Project 2006-04	Prokect 2006-04 - Backup Facilities - Revision 1_rc	Recirculation Ballot	7/16/2010	7/26/2010	Quorum: 93.43% Approval: 85.22%			
135	Project 2007-17	Project 2007-17 Protection System Maintenance: Protection System definition	Successive Ballot	7/23/2010	8/2/2010	Quorum: 94.70% Approval: 58.61%			
136	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Successive Ballot	7/24/2010	8/3/2010	Quorum: 92.99% Approval: 49.61%			
137	Project 2006-08	Project 2006-08 - Reliability Coordination - Transmission Loading Relief_rc	Recirculation Ballot	8/20/2010	8/30/2010	Quorum: 88.26% Approval: 93.93%			
138	Project 2007-04	Project 2007-04 - Certifying System Operators: PER-003-1	Initial Ballot	9/14/2010	9/24/2010	Quorum: 92.73% Approval: 79.17%			
139	Project 2010-15	Project 2010-15 - Urgent Action Revisions to CIP-005-3	Initial Ballot	9/17/2010	9/27/2010	Quorum: 96.46% Approval: 21.77%			
140	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Successive Ballot	9/24/2010	10/4/2010	Quorum: 85.71% Approval: 81.72%			
141	Project 2007-17	Project 2007-17 Protection System Maintenance: Protection System definition	Successive Ballot	10/2/2010	10/14/2010	Quorum: 84.11% Approval: 84.52%			
142	Project 2008-09	Project 2008-09 - Interpretation - RECM - Revision 3_rc	Recirculation Ballot	10/4/2010	10/14/2010	Quorum: 88.11% Approval: 99.14%			
143	Project 2009-28	Project 2009-28 - Interpretation - EOP-001-1 and EOP-001-2 for FMPP_rc	Recirculation Ballot	10/5/2010	10/15/2010	Quorum: 92.19% Approval: 94.78%			
144	Project 2009-27	Project 2009-27 - Interpretation - TOP-002-2a for FMPAA_rc	Recirculation Ballot	10/6/2010	10/16/2010	Quorum: 91.21% Approval: 93.44%			
145	Project 2007-01	Project 2007-01 Underfrequency Load Shedding: PRC-006-1 and EOP-003-1	Recirculation Ballot	10/18/2010	10/28/2010	Quorum: 89.84% Approval: 84.67%			
146	Project 2008-06	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards)_in	Initial Ballot	10/20/2010	11/3/2010	Quorum: 93.66% Approval: 43.33%			
147	Project 2010-10	Project 2010-10 FAC-013-2 Planning Transfer Capability_in	Initial Ballot	10/20/2010	11/3/2010	Quorum: 88.54% Approval: 39.85%			
148	2010 SPM	2010 Standard Processes Manual (Proposed Changes)_in	Initial Ballot	10/28/2010	11/7/2010	Quorum: 81.61% Approval: 93.72%			
149	Project 2007-17	Project 2007-17 Protection System Maintenance: Protection System definition	Recirculation Ballot	11/1/2010	11/11/2010	Quorum: 89.41% Approval: 86.83%			
150	2010 SPM	2010 Standard Processes Manual (Proposed Changes)_rc	Recirculation Ballot	11/9/2010	11/13/2010	Quorum: 87.00% Approval: 92.88%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
151	Project 2009-17	Project 2009-17 - Interpretation Y-W Electric and Tri-State (Revision 2)_rc	Recirculation Ballot	11/19/2010	12/3/2010	Quorum: 87.81% Approval: 82.41%			
152	Project 2008-06	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards)_sb_in	Initial Ballot	12/1/2010	12/10/2010	Quorum: 87.07% Approval: 77.06%			
153	Project 2010-15	Project 2010-15 - Expedited Action Revisions to CIP-005-3	Initial Ballot	12/2/2010	12/11/2010	Quorum: 84.46% Approval: 42.89%			
154	Project 2007-04	Project 2007-04 - Certifying System Operators: PER-003-1	Recirculation Ballot	12/2/2010	12/13/2010	Quorum: 95.50% Approval: 86.91%			
155	Project 2010-13	Project 2010-13 - Relay Loadability Order - PRC-023	Initial Ballot	12/7/2010	12/16/2010	Quorum: 88.00% Approval: 51.51%			
156	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005-2	Successive Ballot	12/10/2010	12/20/2010	Quorum: 79.88% Approval: 44.65%			
157	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005-2	Non-binding Poll	12/10/2010	12/20/2010	Quorum: 78.00% Approval: 53.00%			
158	Project 2008-06	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards)_sb_rc	Recirculation Ballot	12/20/2010	12/30/2010	Quorum: 90.49% Approval: 80.56%			
159	Project 2010-11	Project 2010-11 TPL Table 1 Footnote B SAR_in	Recirculation Ballot	12/27/2010	1/5/2011	Quorum: 90.42% Approval: 83.33%			
160	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.62% Approval: 22.09%	Oppose 12/16/11		
161	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.62% Approval: 33.49%	Oppose 12/16/11		
162	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.60% Approval: 26.82%	Oppose 12/16/11		
163	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.60% Approval: 28.04%	Oppose 12/16/11		
164	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 29.60%	Oppose 12/16/11		
165	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 24.15%	Oppose 12/16/11		
166	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 94.02% Approval: 34.30%	Oppose 12/16/11		
167	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 27.28%	Oppose 12/16/11		
168	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 26.61%	Oppose 12/16/11		
169	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Initial Ballot	12/16/2011	1/6/2011	Quorum: 93.61% Approval: 29.88%	Oppose 12/16/11		
170	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation	Initial Ballot	12/16/2011	1/6/2011	Quorum: 92.15% Approval: 42.06%	Oppose 12/16/11		
171	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Initial Ballot	12/16/2011	1/6/2011	Quorum: 92.56% Approval: 25.34%	Oppose 12/16/11		
172	Project 2010-10	Project 2010-10: FAC Order 729_in	Initial Ballot	12/30/2010	1/8/2011	Quorum: 83.23% Approval: 58.16%			
173	Project 2010-10	Project 2010-10: FAC Order 729_rc	Recirculation Ballot	1/14/2011	1/23/2011	Quorum: 86.65% Approval: 68.98%			
174	Project 2010-11	Project 2010-11 TPL Table 1 Footnote B SAR_rc	Recirculation Ballot	1/26/2011	2/5/2011	Quorum: 93.29% Approval: 86.79%	Support 1/5/11		
175	Project 2010-13	Project 2010-13 - Relay Loadability Order - PRC-023	Successive Ballot	1/24/2011	2/14/2011	Quorum: 83.95% Approval: 65.71%	Support 2/11/11		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
176	Project 2007-23	Project 2007-23 - Violation Severity Levels	Non-binding Poll	2/9/2011	2/22/2011	Quorum: 78.00% Approval: 72.00%	Support 10/28/10		
177	Project 2007-07	Project 2007-07 Vegetation Management: FAC-003-2	Successive Ballot	2/18/2011	2/28/2011	Quorum: 79.28% Approval: 79.34%	Support 2/22/11		
178	Project 2010-13	Project 2010-13 - Relay Loadability Order - PRC-023	Recirculation Ballot	2/24/2011	3/6/2011	Quorum: 87.35% Approval: 68.83%	Support 2/11/11		
179	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002, IRO-001, and IRO-014	Initial Ballot	2/25/2011	3/7/2011	Quorum: 87.10% Approval: 49.54%	Support 3/2/11		
180	Project 2010-15	Project 2010-15 - Expedited Action Revisions to CIP-005-4	Successive Ballot	4/19/2011	4/28/2011	Quorum: 79.66% Approval: 38.00%	Oppose 4/19/11		
181	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-3	Initial Ballot	4/21/2011	5/2/2011	Quorum: 86.01% Approval: 48.74%	Abstain 4/26/11		
182	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-3	Non-binding Poll	4/21/2011	5/2/2011	Quorum: 75.58% Approval: 73.00%			
183	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing: PRC-005	Successive Ballot	5/3/2011	5/12/2011	Quorum: 78.33% Approval: 67.00%	No Recommendation		
184	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing: PRC-005	Non-binding Poll	5/3/2011	5/12/2011	Quorum: 75.00% Approval: 66.00%			
185	Project 2009-06	Project 2009-06 - Facility Ratings: FAC-008-3	Recirculation Ballot	5/12/2011	5/23/2011	Quorum: 91.25% Approval: 78.92%	Support 5/12/11		
186	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs - TPL-001 through TPL-006	Successive Ballot	5/18/2011	5/31/2011	Quorum: 92.07% Approval: 73.99%			
187	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs - TPL-001 through TPL-006	Non-binding Poll	5/18/2011	5/31/2011	Quorum: 86.79% Approval: 71.9%			
188	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2, TOP-002-2 and TOP-003-2	Initial Ballot	5/31/2011	6/9/2011	Quorum: 88.47% Approval: 48.64%	Oppose 5/31/11		
189	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2, TOP-002-2 and TOP-003-2	Non-binding Poll	5/31/2011	6/9/2011	Quorum: 84.18% Approval: 41.00%			
190	Project 2007-17	Project 2007-17 – Protection System Maintenance and Testing – PRC-005	Recirculation Ballot	6/20/2011	6/30/2011	Quorum: 82.97% Approval: 64.76%	Support 6/28/11		
191	Project 2007-17	Project 2007-17 – Protection System Maintenance and Testing – PRC-005	Non-binding Poll	6/20/2011	6/30/2011	Quorum: 52.63% Approval: 60.00%			
192	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs	Recirculation Ballot	7/13/2011	7/22/2011	Quorum: 94.33% Approval: 75.37%			
193	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-002-3	Recirculation Ballot	7/15/2011	7/25/2011	Quorum: 94.13% Approval: 76.99%	Support 7/22/11		
194	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-005-4	Recirculation Ballot	7/15/2011	7/25/2011	Quorum: 94.13% Approval: 75.17%	Support 7/22/11		
195	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-014-2	Recirculation Ballot	7/15/2011	7/25/2011	Quorum: 94.13% Approval: 76.27%	Support 7/22/11		
196	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-002-3	Non-binding Poll	7/15/2011	7/25/2011	Quorum: 75.37% Approval: 93.00%			
197	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-005-4	Non-binding Poll	7/15/2011	7/25/2011	Quorum: 75.66% Approval: 93.00%			
198	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-014-2	Non-binding Poll	7/15/2011	7/25/2011	Quorum: 75.37% Approval: 89.00%			
199	Project 2007-09	Project 2007-09 – Generator Verification: MOD-026-1	Initial Ballot	7/22/2011	8/1/2011	Quorum: 90.25% Approval: 46.53%	No Consensus 7/28/11		
200	Project 2007-09	Project 2007-09 – Generator Verification: MOD-026-1	Non-binding Poll	7/22/2011	8/1/2011	Quorum: 88.75% Approval: 56.00%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
201	Project 2007-09	Project 2007-09 – Generator Verification: PRC-024-1	Initial Ballot	7/22/2011	8/1/2011	Quorum: 90.82% Approval: 18.23%	No Consensus 7/28/11		
202	Project 2007-09	Project 2007-09 – Generator Verification: PRC-024-1	Non-binding Poll	7/22/2011	8/1/2011	Quorum: 88.35% Approval: 20.79%			
203	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing: PRC-005	Initial Ballot	9/19/2011	9/29/2011	Quorum: 84.86% Approval: 61.10%	Support 9/21/11		
204	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing: PRC-005	Non-binding Poll	9/19/2011	9/29/2011	Quorum: 83.13% Approval: 68.68%			
205	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System: Definition of BES	Initial Ballot	9/30/2011	10/10/2011	Quorum: 92.97% Approval: 71.68%	No Consensus 10/3/11		
206	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System: Detailed Information to Support BES Exceptions Request	Initial Ballot	9/30/2011	10/10/2011	Quorum: 89.53% Approval: 64.03%	No Consensus 10/7/111		
207	Project 2007-07	Project 2007-07 Vegetation Management: FAC-003-2	Recirculation Ballot	10/4/2011	10/13/2011	Quorum: 87.17% Approval: 86.25%	Support 2/22/11		
208	Project 2011-INT-01	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	Initial Ballot	11/7/2011	11/16/2011	Quorum: 88.05% Approval: 85.53%	Support 11/8/11		
209	Project 2009-22	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Initial Ballot	11/8/2011	11/17/2011	Quorum: 91.20% Approval: 95.05%	Support 11/8/11		
210	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-001-1	Initial Ballot	11/9/2011	11/18/2011	Quorum: 88.22% Approval: 86.94%	Support 11/10/11		
211	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-3	Initial Ballot	11/9/2011	11/18/2011	Quorum: 85.08% Approval: 85.71%	Support 11/10/11		
212	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-X	Initial Ballot	11/9/2011	11/18/2011	Quorum: 84.82% Approval: 85.31%	Support 11/10/11		
213	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: PRC-004-2.1	Initial Ballot	11/9/2011	11/18/2011	Quorum: 84.29% Approval: 96.09%	Support 11/10/11		
214	Project 2008-10	Project 2008-10 - Interpretation of CIP-006-x R1 for Progress Energy	Successive Ballot	11/11/2011	11/21/2011	Quorum: 83.53% Approval: 95.99%	Support 11/14/11		
215	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System and Implementation Plan	Recirculation Ballot	11/10/2011	11/21/2011	Quorum: 95.92% Approval: 81.32%	Support 10/3/11		
216	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System: Detailed Information to Support BES Exceptions Request	Recirculation Ballot	11/10/2011	11/21/2011	Quorum: 93.02% Approval: 81.48%	Support 10/3/11		
217	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Initial Ballot	11/30/2011	12/9/2011	Quorum: 93.92% Approval: 30.82%	Oppose 12/5/11		
218	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Non-binding Poll	11/30/2011	12/9/2011	Quorum: 89.49% Approval: 36.00%			
219	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Initial Ballot	12/2/2011	12/12/2011	Quorum: 87.97% Approval: 36.21%	Oppose 12/5/11		
220	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	12/2/2011	12/12/2011	Quorum: 85.28% Approval: 45.00%			
221	Project 2008-10	Project 2008-10 - Interpretation of CIP-006-x R1 for Progress Energy	Recirculation Ballot	12/9/2011	12/19/2011	Quorum: 88.02% Approval: 96.04%	Support 11/14/11		
222	Project 2011-INT-01	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	Recirculation Ballot	12/12/2011	12/22/2011	Quorum: 90.10% Approval: 92.49%	Support 11/8/11		
223	Project 2009-22	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 92.00% Approval: 94.58%	Support 11/8/11		
224	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-001-1	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 88.48% Approval: 90.10%	Support 11/10/11		
225	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-3	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 87.17% Approval: 85.38%	Support 11/10/11		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
226	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-X	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 86.91% Approval: 85.03%	Support 11/10/11		
227	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: PRC-004-2.1a	Recirculation Ballot	12/14/2011	12/23/2011	Quorum: 86.65% Approval: 96.43%	Support 11/10/11		
228	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Successive Ballot	1/3/2012	1/12/2012	Quorum: 82.04% Approval: 59.93%	Oppose 1/9/12		
229	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-002-3	Successive Ballot	1/3/2012	1/12/2012	Quorum: 82.04% Approval: 77.08 %	Support 1/9/12		
230	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Successive Ballot	1/3/2012	1/12/2012	Quorum: 82.04% Approval: 78.95%	Support 1/9/12		
231	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-001-1	Non-binding Poll	1/4/2012	1/13/2012	Quorum: 78.27% Approval: 93.00%			
232	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-002-3	Non-binding Poll	1/9/2012	1/18/2012	Quorum: 76.41% Approval: 71.42%			
233	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Non-binding Poll	1/9/2012	1/19/2012	Quorum: 81.50% Approval: 67.61%			
234	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Non-binding Poll	1/9/2012	1/19/2012	Quorum: 81.50% Approval: 70.28%			
235	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Successive Ballot	1/30/2012	2/9/2012	Quorum: 81.82% Approval: 54.64%	Oppose 2/7/12		
236	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-002-3	Successive Ballot	1/30/2012	2/9/2012	Quorum: 82.11% Approval: 80.62%	Support 2/7/12		
237	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-001-3	Successive Ballot	1/30/2012	2/9/2012	Quorum: 81.82% Approval: 80.21%	Support 2/7/12		
238	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Non-binding Poll	1/30/2012	2/9/2012	Quorum: 80.35% Approval: 71.35%			
239	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-002-3	Non-binding Poll	1/30/2012	2/9/2012	Quorum: 80.06% Approval: 90.86%			
240	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-001-3	Non-binding Poll	1/30/2012	2/9/2012	Quorum: 79.77% Approval: 84.69%			
241	Project 2009-26	Project 2009-26 - Interpretation of CIP-004-1 by WECC	Successive Ballot	3/14/2012	3/23/2012	Quorum: 88.55% Approval: 79.61%	Support 3/16/12		
242	Project 2010-INT-05	Interpretation 2010-INT-05 - Interpretation of CIP-002-1 R3 for Duke Energy	Initial Ballot	3/14/2012	3/23/2012	Quorum: 89.63% Approval: 94.71%	Support 3/16/12		
243	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR-002 for Constellation	Initial Ballot	3/14/2012	3/23/2012	Quorum: 86.92% Approval: 63.09%	Support 3/16/12		
244	Project 2007-09	Project 2007-09 Generator Verification: MOD-026-1	Successive Ballot	3/19/2012	3/29/2012	Quorum: 81.45% Approval: 61.21%			
245	Project 2007-09	Project 2007-09 Generator Verification: PRC-024-1	Successive Ballot	3/19/2012	3/29/2012	Quorum: 80.38% Approval: 41.09%			
246	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Successive Ballot	3/19/2012	3/29/2012	Quorum: 84.32% Approval: 73.93%	Support 3/19/12		
247	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Non-binding Poll	3/19/2012	3/29/2012	Quorum: 81.93% Approval: 66.12%			
248	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-3	Successive Ballot	3/30/2012	4/9/2012	Quorum: 80.37% Approval: 85.18%	Support 4/5/12		
249	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-X	Successive Ballot	3/30/2012	4/9/2012	Quorum: 80.10% Approval: 85.01%	Support 4/5/12		
250	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Initial Ballot	4/6/2012	4/16/2012	Quorum: 88.28% Approval: 41.09%	Oppose 4/16/12		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of “Ballot Periods” column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
251	Project 2007-09	Project 2007-09_Generator Verification: MOD-027-1	Initial Ballot	4/6/2012	4/16/2012	Quorum: 88.04% Approval: 36.84%	Oppose 4/16/12		
252	Project 2007-09	Project 2007-09_Generator Verification: PRC-019-1	Initial Ballot	4/6/2012	4/16/2012	Quorum: 88.04% Approval: 48.70%%	Oppose 4/16/12		
253	Project 2007-09	Project 2007-09_Generator Verification: MOD-025-2	Non-binding Poll	4/6/2012	4/16/2012	Quorum: 86.82% Approval: 43.72%			
254	Project 2007-09	Project 2007-09_Generator Verification: MOD-027-1	Non-binding Poll	4/6/2012	4/16/2012	Quorum: 86.04% Approval: 38.56%			
255	Project 2007-09	Project 2007-09_Generator Verification: PRC-019-1	Non-binding Poll	4/6/2012	4/16/2012	Quorum: 86.53% Approval: 46.38%			
256	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: PRC-005-1.1a	Initial Ballot	4/6/2012	4/16/2012	Quorum: 88.95% Approval: 92.41%	Support 4/16/12		
257	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Successive Ballot	4/11/2012	4/20/2012	Quorum: 78.28%% Approval: 75.44%			
258	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-002-3	Successive Ballot	4/11/2012	4/20/2012	Quorum: 78.02% Approval: 87.22%			
259	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Successive Ballot	4/11/2012	4/20/2012	Quorum: 78.28% Approval: 80.11%			
260	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Non-binding Poll	4/11/2012	4/23/2012	Quorum: 77.21% Approval: 69.84%			
261	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Non-binding Poll	4/11/2012	4/23/2012	Quorum: 77.48% Approval: 67.64%			
262	Project 2009-26	Project 2009-26 - Interpretation of CIP-004-1 by WECC	Recirculation Ballot	4/20/2012	4/30/2012	Quorum: 90.96% Approval: 80.08%	Support 3/16/12		
263	Project 2010-INT-05	Interpretation 2010-INT-05 - Interpretation of CIP-002-1 R3 for Duke Energy	Recirculation Ballot	4/20/2012	4/30/2012	Quorum: 92.68% Approval: 94.61%	Support 3/16/12		
264	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-3	Recirculation Ballot	4/24/2012	5/3/2012	Quorum: 81.72% Approval: 87.34%			
265	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: FAC-003-X	Recirculation Ballot	4/24/2012	5/3/2012	Quorum: 81.94% Approval: 87.32%			
266	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface: PRC-005-1.1b	Recirculation Ballot	4/24/2012	5/3/2012	Quorum: 90.44% Approval: 93.23%			
267	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-001-2	Recirculation Ballot	4/27/2012	5/6/2012	Quorum: 79.36% Approval: 76.84%	Abstain 4/19/12		
268	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-002-3	Recirculation Ballot	4/27/2012	5/6/2012	Quorum: 79.36% Approval: 88.11%	Support 4/19/12		
269	Project 2007-03	Project 2007-03 - Real-time Operations: TOP-003-2	Recirculation Ballot	4/27/2012	5/6/2012	Quorum: 79.36% Approval: 80.79%	Support 4/19/12		
270	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.63% Approval: 37.37%	Abstain 5/17/12		
271	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.45% Approval: 60.55%	Abstain 5/17/12		
272	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.40% Approval: 38.81%	Abstain 5/17/12		
273	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.98% Approval: 55.08%	Abstain 5/17/12		
274	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.22% Approval: 38.50%	Abstain 5/17/12		
275	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.01% Approval: 45.78%	Abstain 5/17/12		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
276	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.19% Approval: 67.19%	Abstain 5/17/12		
277	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Successive Ballot	5/11/2012	5/21/2012	Quorum: 87.01% Approval: 60.19%	Abstain 5/17/12		
278	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.39% Approval: 47.92%	Abstain 5/17/12		
279	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Successive Ballot	5/11/2012	5/21/2012	Quorum: 86.39% Approval: 58.23%	Abstain 5/17/12		
280	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation	Successive Ballot	5/11/2012	5/21/2012	Quorum: 85.12% Approval: 66.23%	Abstain 5/17/12		
281	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Successive Ballot	5/11/2012	5/21/2012	Quorum: 84.09% Approval: 47.88%	Abstain 5/17/12		
282	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Successive Ballot	5/15/2012	5/24/2012	Quorum: 84.43% Approval: 46.18%			
283	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	5/15/2012	5/24/2012	Quorum: 79.95% Approval: 52.67%			
284	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Initial Ballot	6/11/2012	6/20/2012	Quorum: 84.14% Approval: 21.11%	Oppose 6/13/12		
285	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	6/11/2012	6/20/2012	Quorum: 81.01% Approval: 28.30%			
286	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Successive Ballot	6/18/2012	6/27/2012	Quorum: 79.46% Approval: 79.00%			
287	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Non-binding Poll	6/18/2012	6/27/2012	Quorum: 75.00% Approval: 70.21%			
288	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR -002 for Constellation	Successive Ballot	6/18/2012	6/27/2012	Quorum: 85.98% Approval: 68.22%	Support 6/26/12		
289	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Initial Ballot	6/26/2012	7/5/2012	Quorum: 84.24% Approval: 23.82%	Oppose 6/27/12		
290	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Non-binding Poll	6/26/2012	7/5/2012	Quorum: 82.26% Approval: 25.19%			
291	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-002-3	Recirculation Ballot	6/27/2012	7/6/2012	Quorum: 85.34% Approval: 81.71%			
292	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-001-3	Recirculation Ballot	6/27/2012	7/6/2012	Quorum: 85.04% Approval: 81.72%			
293	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-002-3	Non-binding Poll	6/27/2012	7/6/2012	Quorum: 84.16% Approval: 79.16%			
294	Project 2006-06	Project 2006-06 - Reliability Coordination - IRO-001-3	Non-binding Poll	6/27/2012	7/6/2012	Quorum: 83.87% Approval: 86.91%			
295	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Successive Ballot	6/27/2012	7/9/2012	Quorum: 75.37% Approval: 72.16%	No Consensus 7/5/12		
296	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Non-binding Poll	6/27/2012	7/11/2012	Quorum: 75.37% Approval: 73.71%			
297	Project 2011-INT-02	Project 2011-INT-02 - Rapid Revision of VAR-002 for Constellation	Recirculation Ballot	7/18/2012	7/27/2012	Quorum: 90.97% Approval: 69.81%	Support 6/26/12		
298	Project 2011-INT-02	Project 2011-INT-02 - Rapid Revision of VAR-002 for Constellation	Non-binding Poll	7/18/2012	7/27/2012	Quorum: 81.31% Approval: 60.93%			
299	Project 2010-INT-01	Project 2010-INT-01 - Rapid Revision of TOP-006 for FMPP	Initial Ballot	7/20/2012	7/30/2012	Quorum: 80.39% Approval: 79.28%	Oppose 7/20/12		
300	Project 2010-INT-01	Project 2010-INT-01 - Rapid Revision of TOP-006 for FMPP	Non-binding Poll	7/20/2012	7/30/2012	Quorum: 78.26% Approval: 76.07%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
301	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Initial Ballot	7/24/2012	8/2/2012	Quorum: 83.11% Approval: 54.16%	Oppose 7/20/12		
302	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Successive Ballot	8/17/2012	8/27/2012	Quorum: 78.11% Approval: 80.31%	Support 6/22/12		
303	Project 2009-19	Project 2009-19 – Interpretation of BAL-002 by NWPP Reserve Sharing Group	Successive Ballot	8/23/2012	9/4/2012	Quorum: 79.21% Approval: 87.78%	Support 2/22/10		
304	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Initial Ballot	8/29/2012	9/7/2012	Quorum: 86.71% Approval: 37.68%	Support 9/5/12		
305	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Non-binding Poll	8/29/2012	9/7/2012	Quorum: 84.17% Approval: 37.36%			
306	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001-2	Recirculation Ballot	9/6/2012	9/17/2012	Quorum: 80.35% Approval: 75.01%			
307	Project 2007-02	Project 2007-02 - Operating Personnel Communication Protocols	Successive Ballot	9/11/2012	9/20/2012	Quorum: 77.70% Approval: 50.57%	Support 9/15/12		
308	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	9/11/2012	9/20/2012	Quorum: 84.05% Approval: 54.07%			
309	Project 2010-INT-01	Project 2010-INT-01 - Rapid Revision of TOP-006 for FMPP	Recirculation Ballot	9/12/2012	9/21/2012	Quorum: 85.36% Approval: 87.34%			
310	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Successive Ballot	9/18/2012	9/27/2012	Quorum: 78.54% Approval: 63.40%	No Consensus 9/27/12		
311	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	9/18/2012	9/27/2012	Quorum: 78.93% Approval: 71.04%			
312	Project 2009-19	Project 2009-19 - Interpretation of BAL-002-0 NWPP Reserve Sharing Group	Recirculation Ballot	9/28/2012	10/8/2012	Quorum: 85.11% Approval: 90.34%	Support 2/22/10		
313	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 74.85%	Support 10/4/12		
314	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.37% Approval: 89.50%	Support 10/4/12		
315	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 85.58%	Support 10/4/12		
316	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 89.46%	Support 10/4/12		
317	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 92.11%	Support 10/4/12		
318	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 87.73%	Support 10/4/12		
319	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 91.74%	Support 10/4/12		
320	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 91.73%	Support 10/4/12		
321	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 84.60%	Support 10/4/12		
322	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Successive Ballot	10/1/2012	10/10/2012	Quorum: 80.58% Approval: 92.90%	Support 10/4/12		
323	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation	Successive Ballot	10/1/2012	10/10/2012	Quorum: 78.93% Approval: 94.00%	Support 10/4/12		
324	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Successive Ballot	10/1/2012	10/10/2012	Quorum: 79.13% Approval: 91.59%	Support 10/4/12		
325	SPM-SPIG	Standard Processes Manual Revisions to Implement SPIG Recommendations	Initial Ballot	10/3/2012	10/12/2012	Quorum: 87.50% Approval: 63.25%	Support 10/4/12		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
326	VRFs and VSLs	Revisions to Outstanding VRFs and VSLs	Non-binding Poll	10/10/2012	10/23/2012	Quorum: 78.57% Approval: 73.02%			
327	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing: PRC-005	Recirculation Ballot	10/15/2012	10/24/2012	Quorum: 81.08% Approval: 80.51%	Support 6/22/12		
328	Project 2007-09	Project 2007-09 Generator Verification: MOD-026-1	Successive Ballot	10/19/2012	10/31/2012	Quorum: 75.55% Approval: 76.50%			
329	Project 2007-09	Project 2007-09 Generator Verification: PRC-024-1	Successive Ballot	10/19/2012	10/31/2012	Quorum: 75.00% Approval: 57.24%			
330	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Successive Ballot	10/19/2012	10/31/2012	Quorum: 83.61% Approval: 68.31%			
331	Project 2007-09	Project 2007-09 Generator Verification: MOD-027-1	Successive Ballot	10/19/2012	10/31/2012	Quorum: 82.34% Approval: 71.53%			
332	Project 2007-09	Project 2007-09 Generator Verification: PRC-019-1	Successive Ballot	10/19/2012	10/31/2012	Quorum: 82.07% Approval: 70.64%			
333	Project 2007-09	Project 2007-09 Generator Verification: MOD-026-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 75.88% Approval: 77.10%			
334	Project 2007-09	Project 2007-09 Generator Verification: PRC-024-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 75.40% Approval: 52.72%			
335	Project 2007-09	Project 2007-09 Generator Verification: MOD-025-2	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 77.94% Approval: 64.24%			
336	Project 2007-09	Project 2007-09 Generator Verification: MOD-027-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 78.06% Approval: 68.93%			
337	Project 2007-09	Project 2007-09 Generator Verification: PRC-019-1	Non-binding Poll	10/19/2012	10/31/2012	Quorum: 78.51% Approval: 63.63%			
338	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-002-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.33% Approval: 78.59%	Support 10/4/12		
339	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-003-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.33% Approval: 92.75%	Support 10/4/12		
340	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-004-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 89.73%	Support 10/4/12		
341	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-005-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 93.73%	Support 10/4/12		
342	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-006-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 95.53%	Support 10/4/12		
343	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-007-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 91.79%	Support 10/4/12		
344	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-008-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 95.47%	Support 10/4/12		
345	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-009-5	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.33% Approval: 94.60%	Support 10/4/12		
346	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-010-1	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 88.99%	Support 10/4/12		
347	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP-011-1	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 85.54% Approval: 95.67%	Support 10/4/12		
348	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Implementation Plan	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 83.47% Approval: 94.91%	Support 10/4/12		
349	Project 2008-06	Project 2008-06 - Cyber Security - Order 706: CIP V5 Definitions	Recirculation Ballot	10/26/2012	11/5/2012	Quorum: 83.47% Approval: 93.23%	Support 10/4/12		
350	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Recirculation Ballot	10/24/2012	11/5/2012	Quorum: 85.14% Approval: 71.39%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
351	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting: EOP-004-2	Non-binding Poll	10/24/2012	11/5/2012	Quorum: 78.93% Approval: 71.04%			
352	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Successive Ballot	10/26/2012	11/6/2012	Quorum: 82.04% Approval: 76.08%	Support 11/5/12		
353	Project 2010-11	Project 2010-11 TPL footnote b Initial Ballot October 2012_in	Initial Ballot	11/9/2012	11/19/2012	Quorum: 80.45% Approval: 56.18%			
354	Project 2012-INT-02	Interpretation 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for SPCS	Initial Ballot	11/26/2012	12/5/2012	Quorum: 84.81% Approval: 72.57%	Oppose 12/5/12		
355	Project 2013-02	Project 2013-02 - Paragraph 81	Initial Ballot	11/30/2012	12/10/2012	Quorum: 75.77% Approval: 96.45%	Support 12/10/12		
356	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Successive Ballot	12/4/2012	12/13/2012	Quorum: 76.78% Approval: 53.57%	No Consensus 12/13/12		
357	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	12/4/2012	12/13/2012	Quorum: 77.22% Approval: 57.91%			
358	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Successive Ballot	12/7/2012	12/17/2012	Quorum: 76.47% Approval: 33.23%	Oppose 12/17/12		
359	Project 2007-06	Project 2007-06 - System Protection Coordination: PRC-027-1	Non-binding Poll	12/7/2012	12/17/2012	Quorum: 75.58% Approval: 34.80%			
360	Project 2012-INT-05	Interpretation 2012-INT-05: CIP-002-3 for OGE	Initial Ballot	12/11/2012	12/20/2012	Quorum: 84.50% Approval: 95.60%	Support 12/19/12		
361	SPM-SPIG	Standard Processes Manual Revisions to Implement SPIG Recommendations	Successive Ballot	12/11/2012	12/20/2012	Quorum: 83.24% Approval: 84.48%	Support 12/19/12		
362	Project 2007-09	Project 2007-09_Generator Verification: MOD-025-2	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 86.89% Approval: 73.06%			
363	Project 2007-09	Project 2007-09_Generator Verification: MOD-026-1	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 79.00% Approval: 79.36%			
364	Project 2007-09	Project 2007-09_Generator Verification: MOD-027-1	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 86.68% Approval: 74.27%			
365	Project 2007-09	Project 2007-09_Generator Verification: PRC-019-1	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 85.87% Approval: 73.63%			
366	Project 2007-12	Project 2007-12 - Frequency Response: BAL-003-1	Recirculation Ballot	12/12/2012	12/21/2012	Quorum: 86.19% Approval: 76.53%			
367	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Successive Ballot	1/2/2013	1/11/2013	Quorum: 78.16% Approval: 60.31%	Support 1/11/13		
368	Project 2007-09	Project 2007-09 - Generator Verification - PRC-024-1	Non-binding Poll	1/2/2013	1/11/2013	Quorum: 76.38% Approval: 55.68%			
369	Project 2010-11	Project 2010-11 Successive Ballot December 2012_in	Successive Ballot	1/2/2013	1/11/2013	Quorum: 85.47% Approval: 65.77%	No Consensus 1/11/13		
370	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-012-1	Initial Ballot	1/4/2013	1/14/2013	Quorum: 83.94% Approval: 21.80%	Oppose 1/11/13		
371	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-012-1	Non-binding Poll	1/4/2013	1/14/2013	Quorum: 82.23% Approval: 24.27%			
372	Project 2013-02	Project 2013-02 - Paragraph 81	Recirculation Ballot	1/8/2013	1/17/2013	Quorum: 84.60% Approval: 95.22%	Support 12/10/12		
373	Project 2012-INT-05	Interpretation 2012-INT-05: CIP-002-3 for OGE	Recirculation Ballot	1/14/2013	1/23/2013	Quorum: 87.13% Approval: 99.09%	Support 12/19/12		
374	SPM-SPIG	Standard Processes Manual Revisions to Implement SPIG Recommendations	Recirculation Ballot	1/18/2013	1/28/2013	Quorum: 85.90% Approval: 85.57%	Support 12/19/12		
375	Project 2010-11	Project 2010-11 Recirculation Ballot Jan 2013_in	Recirculation Ballot	1/22/2013	1/31/2013	Quorum: 88.55% Approval: 69.63%	No Consensus 1/11/13		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
376	Project 2012-INT-02	Interpretation 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for SPCS	Recirculation Ballot	1/22/2013	1/31/2013	Quorum: 85.67% Approval: 77.61%	Oppose 12/5/12		
377	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Successive Ballot	2/11/2013	2/20/2013	Quorum: 77.62% Approval: 50.66%	Support 9/5/12		
378	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Non-binding Poll	2/11/2013	2/20/2013	Quorum: 75.38% Approval: 50.60%			
379	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Successive Ballot	2/15/2013	2/28/2013	Quorum: 78.80% Approval: 89.01%	Support 1/11/13		
380	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Non-binding Poll	2/15/2013	2/28/2013	Quorum: 76.38% Approval: 84.24%			
381	Project 2010-13.2	Project 2010-13.2 Phase 2 of Relay Loadability: Generation	Initial Ballot	3/1/2013	3/11/2013	Quorum: 76.36% Approval: 54.65%			
382	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Successive Ballot	3/13/2013	3/22/2013	Quorum: 77.48% Approval: 84.27%	No Consensus 3/22/13		NPCC to abstain - international nature of the ERO and BPS is not used in Reliability Standards
383	Project 2012-INT-04	Project 2012-INT-04 - Interpretation of CIP-007-3 for ITC	Initial Ballot	3/13/2013	3/22/2013	Quorum: 88.58% Approval: 97.18%	Support 3/14/13		
384	Project 2012-INT-06	Project 2012-INT-06 - Interpretation of CIP-003-3 for Consumers Energy	Initial Ballot	3/13/2013	3/22/2013	Quorum: 88.52% Approval: 98.89%	Support 3/14/13		
385	Project 2007-09	Project 2007-09 - Generator Verification: PRC-024-1	Recirculation Ballot	3/18/2013	3/27/2013	Quorum: 81.33% Approval: 89.44%	Support 1/11/13		
386	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Successive Ballot	3/27/2013	4/5/2013	Quorum: 78.39% Approval: 57.50%	No Consensus 4/4/13		The RSC did not reach a full consensus however the majority of respondents had indicated they will support the standard - see comment form for further details. Some believe the standard is not necessary and that existing whitepapers alleviate the need for it. In recognition of the NERC BOT's expectations that COM-003 will be approved by the industry and brought before them for approval, NPCC has voted affirmatively and will supply comments for the record outlining our concerns.
387	Project 2007-02	Project 2007-02 Operating Personnel Protocols: COM-003-1	Non-binding Poll	3/27/2013	4/5/2013	Quorum: 77.97% Approval: 54.28%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
388	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-001-2	Initial Ballot	4/16/2013	4/25/2013	Quorum: 88.60% Approval: 66.98%	No Consensus 4/23/13		The majority of NPCC's Balancing Authorities have indicated support for the standard, however NPCC as the Regional Entity has concerns based on results of the field trials that were conducted. These field trials have indicated the potential for an increased number of SOL violations as well as potential for increased ACE due to large inadvertent flows with the proposed BAAL limits based on frequency triggers. To be respectful of the positions of the NPCC BAs who will have to implement this new methodology and the support expressed, NPCC as the Regional Entity will cast an Abstention
389	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-002-2	Initial Ballot	4/16/2013	4/25/2013	Quorum: 88.51% Approval: 42.75%	Oppose 4/23/13		There is a lack of technical justification for the 500 MW threshold within the standard-NPCC will submit suggested improvements
390	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-013-1	Initial Ballot	4/16/2013	4/25/2013	Quorum: 88.51% Approval: 23.84%	Oppose 4/23/13		Losses of large blocks of load are typically caused by coincident transmission contingencies. Excessive and uninformed adjustments made to generation in order to bring the ACE to zero may well lead to further transmission issues. NPCC will submit suggested improvements
391	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-001-2	Non-binding Poll	4/16/2013	4/25/2013	Quorum: % Approval: %			
392	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-002-2	Non-binding Poll	4/16/2013	4/25/2013	Quorum: % Approval: %			
393	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-013-1	Non-binding Poll	4/16/2013	4/25/2013	Quorum: % Approval: %			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
394	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Recirculation Ballot	4/18/2013	4/29/2013	Quorum: 80.70% Approval: 88.15%	No Consensus 3/22/13		
395	Project 2010-13.2	Project 2010-13.2 Phase 2 of Relay Loadability: Generation	Successive ballot	5/15/2013	5/24/2013	Quorum: 81.25% Approval: 69.23%	Support 5/23/13		The Regional Standard Committee has not expressed any concerns of significance that would warrant a ballot to reject, therefore the RSC recommends a yes vote, "Affirmative", to accept the standard
396	Project 2010-13.2	Project 2010-13.2 Phase 2 of Relay Loadability: Generation	Non-binding Poll	5/15/2013	5/24/2013	Quorum: 80.17% Approval: 61.11%			
397	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-001 and PRC-027	Successive Ballot	6/24/2013	7/3/2013	Quorum: 77.65% Approval: 52.71%			
398	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-001 and PRC-027	Non-binding Poll	6/24/2013	7/3/2013	Quorum: 77.12% Approval: 52.48%			
399	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Initial Ballot	7/3/2013	7/12/2013	Quorum: 85.53% Approval: 49.73%			
400	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	Successive Ballot	7/10/2013	7/19/2013	Quorum: 76.32% Approval: 58.36%	No Consensus 7/19/13 [Due to the concerns expressed over the potential actions by the NERC BOT and FERC as well as the incremental improvement of the standard over the previous versions, NPCC as the Regional Entity will support the standard and submit comments.]		organizations support the standard as written however some members expressed concern that in order to measure compliance with R1 and R2, the standard will require all Reliability Directives to be investigated to determine if RC approved and documented communication protocols have been violated. Also it was identified that TO, BA communication protocols would have to approved by the RC potentially causing some legal issues if protocols aren't approved and casts question on the enforcement of those protocols. NPCC will be submitting some helpful comments should the standard pass and some non-substantive revision be performed prior to the "final" (previously named recirculation) ballot.
401	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	Non-binding Poll	7/10/2013	7/19/2013	Quorum: 76.20% Approval: 55.37%			
402	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	Successive Ballot	7/10/2013	7/19/2013	Quorum: 85.05% Approval: 72.43%	Support 7/19/13		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
403	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	Non-binding Poll	7/10/2013	7/19/2013	Quorum: 82.51% Approval: 64.59%			
404	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves: BAL-001-2	Final Ballot	7/16/2013	7/25/2013	Quorum: 92.31% Approval: 74.54%	No Consensus 7/22/13		The RSC has not reached a full consensus however the majority are in support. Issues outstanding for those not in support are concern over "hitting limits" more frequently and potential issues with BA's potentially "dragging" on the interconnection. NPCC will be voting affirmative on the standard.
405	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-023-3	Initial Ballot	7/26/2013	8/5/2013	Quorum: 80.05% Approval: 93.00%	Support 8/5/13		
408	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025-1	Final Ballot	8/2/2013	8/12/2013	Quorum: 89.13% Approval: 76.52%	Support 8/12/13		
406	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Initial Ballot	8/2/2013	8/12/2013	Quorum: 76.32% Approval: 62.74%	Support 8/9/13		
407	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Non-binding Poll	8/2/2013	8/12/2013	Quorum: 75.89% Approval: 55.45%			
409	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005-3	Initial Ballot	8/14/2013	8/23/2013	Quorum: 78.33% Approval: 79.42%	Support 8/23/13		
410	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005-3	Non-binding Poll	8/14/2013	8/23/2013	Quorum: 77.45% Approval: 81.37%			
411	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Ballot	8/16/2013	8/26/2013	Quorum: 76.14% Approval: 51.10%	No Consensus 8/26/13		NPCC to support with comments
412	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Non-binding Poll	8/16/2013	8/26/2013	Quorum: 75.98% Approval: 53.29%			
413	Project 2010-01	Project 2010-01 - Training - PER-005-2	Ballot	8/23/2013	9/3/2013	Quorum: 75.25% Approval: 34.46%	No Consensus 8/31/13		NPCC to support with comments The most contentious issues raised by RSC members was surrounding the Control Center definition and the potential to vastly expand those needing training subject to the standard and compliance and that there was no need for a standard, rather, the FERC Directives should be addressed through other means.
414	Project 2010-01	Project 2010-01 - Training - PER-005-2	Non-binding Poll	8/23/2013	9/3/2013	Quorum: 80.45% Approval: 34.24%			

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
415	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	Ballot	8/23/2013	9/3/2013	Quorum: 81.89% Approval: 43.79%	Oppose 8/31/13		The standard, in the view of the group, has extensive issues including but not limited to, applicability issues, lacks clarity, missing measures, quality, and other substantive issues. NPCC will be submitting detailed comments to address these issues. The RSC does not believe it would be beneficial to support the standard at this point as the next step, if it fails the initial ballot, would still require an additional ballot prior to moving to recirculation due to the substantive changes that are needed for the next revision. NPCC will be submitting helpful comments to NERC and supporting the drafting team effort.
416	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	Non-binding Poll	8/23/2013	9/3/2013	Quorum: 79.95% Approval: 44.23%			
417	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1, MOD-033-1	Ballot	8/26/2013	9/4/2013	Quorum: 82.29% Approval: 41.24%	Support 8/31/13		
418	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1, MOD-033-1	Non-binding Poll	8/26/2013	9/4/2013	Quorum: 79.66% Approval: 40.00%			
419	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Ballot	8/26/2013	9/4/2013	Quorum: 81.96% Approval: 55.76%	Support 8/31/13		
420	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Non-binding Poll	8/26/2013	9/4/2013	Quorum: 80.35% Approval: 58.97%			
421	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Additional Ballot	8/26/2013	9/4/2013	Quorum: 78.68% Approval: 66.11%	Support 8/31/13		
426	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-023-3	Final Ballot	9/4/2013	9/13/2013	Quorum: 85.93% Approval: 90.83%	Support 8/5/13		
422	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-002-2, BAL-013-1	Ballot	9/6/2013	9/16/2013	Quorum: 76.15% Approval: 58.23%	No Consensus 9/12/13		
423	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-002-2, BAL-013-1	Non-binding Poll	9/6/2013	9/16/2013	Quorum: 75.69% Approval: 59.66%			
424	Project 2012-INT-04	Project 2012-INT-04 - Interpretation of CIP-007-3 for ITC	Final Ballot	9/11/2013	9/20/2013	Quorum: 91.64% Approval: 98.61%	Support 3/14/13		

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
425	Project 2012-INT-06	Project 2012-INT-06 - Interpretation of CIP-003-3 for Consumers Energy	Final Ballot	9/11/2013	9/20/2013	Quorum: 90.98% Approval: 98.92%	Support 3/14/13		
427	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Additional Ballot	10/9/2013	10/21/2013	Quorum: 77.58% Approval: 88.75%	Support 10/16/13		
428	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Non-binding Poll	10/9/2013	10/21/2013	Quorum: 75.89% Approval: 90.04%			
429	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005-3	Final Ballot	10/16/2013	10/25/2013	Quorum: 85.71% Approval: 85.38%			
430	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Additional Ballot	10/18/2013	10/29/2013	Quorum: 75.83% Approval: 72.55%	Support 10/21/13		
431	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation - EOP-010-1	Final Ballot	10/25/2013	11/4/2013	Quorum: 86.90% Approval: 91.95%			
432	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-002-4	Additional Ballot	10/25/2013	11/7/2013	Quorum: 76.67% Approval: 58.24%	No Consensus 11/1/13		
433	Project 2010-01	Project 2010-01 - Training - PER-005-2	Additional Ballot	11/1/2013	11/12/2013	Quorum: 76.23% Approval: 56.48%	Support 11/11/13		
434	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-004-3	Initial Ballot	11/4/2013	11/13/2013	Quorum: 76.12% Approval: 67.35%	Support 11/5/13		
435	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-006-4	Initial Ballot	11/4/2013	11/13/2013	Quorum: 75.82% Approval: 75.58%	Support 11/5/13		
436	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-009-2	Initial Ballot	11/4/2013	11/13/2013	Quorum: 75.82% Approval: 68.40%	Support 11/5/13		
437	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-010-2	Initial Ballot	11/4/2013	11/13/2013	Quorum: 75.82% Approval: 58.03%	Support 11/5/13		
438	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-011-1	Initial Ballot	11/4/2013	11/13/2013	Quorum: 75.52% Approval: 71.35%	Support 11/5/13		
439	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - Definition	Initial Ballot	11/4/2013	11/15/2013	Quorum: 76.42% Approval: 77.82%	Support 11/5/13		
440	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	Final Ballot	11/8/2013	11/18/2013	Quorum: 81.68% Approval: 74.34%	Support 10/21/13		
441	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Additional Ballot	11/8/2013	11/20/2013	Quorum: 81.69% Approval: 82.97%	No Consensus 8/26/13		
442	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1	Additional Ballot	11/8/2013	11/20/2013	Quorum: 79.05% Approval: 73.46%	Support 8/31/13		
443	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-033-1	Additional Ballot	11/8/2013	11/20/2013	Quorum: 79.84% Approval: 69.42%	Support 8/31/13		
444	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Additional Ballot	11/13/2013	11/22/2013	Quorum: 80.54% Approval: 57.59%	Support 8/31/13		
445	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4	Additional Ballot	11/15/2013	11/25/2013	Quorum: 80.81% Approval: 69.43%			
446	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-002-3	Additional Ballot	11/15/2013	11/25/2013	Quorum: 81.06% Approval: 66.09%			
447	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-002-2	Additional Ballot	12/2/2013	12/12/2013	Quorum: 75.29% Approval: 64.24%	No Consensus 12/9/13	Affirmative	

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
448	Project 2007-11	Project 2007-11 Disturbance Monitoring - PRC-002-2	Initial Ballot	12/6/2013	12/16/2013	Quorum: 82.25% Approval: 43.29%	No Consensus 12/15/13	Affirmative	Highlights of comments received expressed: • Agreement with the methodology to determine BES locations for which data had to be captured • Use of the term "locations" • DDR for Flowgates, IROLs • Clarification needed for some data that is to be captured • Editorial suggestions
449	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1	Final Ballot	12/6/2013	12/16/2013	Quorum: 87.53% Approval: 77.49%	Support 8/31/13	Affirmative	
450	Project 2008-12	Project 2008-12 Coordinate Interchange Standards - INT-006-4	Final Ballot	12/10/2013	12/20/2013	Quorum: 85.07% Approval: 80.77%	Support 11/5/13	Affirmative	
451	Project 2008-12	Project 2008-12 Coordinate Interchange Standards - INT-009-2	Final Ballot	12/10/2013	12/20/2013	Quorum: 85.07% Approval: 72.86%	Support 11/5/13	Affirmative	
452	Project 2008-12	Project 2008-12 Coordinate Interchange Standards - INT-011-1	Final Ballot	12/10/2013	12/20/2013	Quorum: 84.78% Approval: 72.91%	Support 11/5/13	Affirmative	
453	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	Final Ballot	12/11/2013	12/20/2013	Quorum: 87.16% Approval: 86.40%	No Consensus 8/26/13	Affirmative	
454	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4	Final Ballot	12/13/2013	12/23/2013	Quorum: 84.34% Approval: 75.35%		Affirmative	
455	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-027-1	Additional Ballot	12/9/2013	12/31/2013	Quorum: 76.60% Approval: 65.71%	No Consensus 12/27/13	Affirmative	
456	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-033-1	Additional Ballot	1/10/2014	1/21/2014	Quorum: 76.92% Approval: 81.41%	Support 8/31/13	Affirmative	
457	Project 2010-01	Project 2010-01 - Training - PER-005-2	Additional Ballot	1/8/2014	1/22/2014	Quorum: 7912% Approval: 74.63%	Support 11/11/13	Affirmative	
458	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-004-3	Additional Ballot	1/10/2014	1/22/2014	Quorum: 75.22% Approval: 81.19%	Support 11/5/13	Affirmative	
459	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-010-2	Additional Ballot	1/10/2014	1/22/2014	Quorum: 75.22% Approval: 90.23%	Support 11/5/13	Affirmative	
460	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - Definition	Additional Ballot	1/16/2014	1/29/2014	Quorum: 76.12% Approval: 92.17%	Support 11/5/13	Affirmative	
461	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-002-4	Additional Ballot	1/22/2014	1/31/2014	Quorum: 76.03% Approval: 71.86%	No Consensus 11/1/13	Affirmative	Ballot Period Extended to 2/4/14
462	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-004-3	Final Ballot	1/27/2014	2/5/2014	Quorum: 83.88% Approval: 83.44%	Support 11/5/13	Affirmative	
463	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - INT-010-2	Final Ballot	1/27/2014	2/5/2014	Quorum: 83.58% Approval: 91.51%	Support 11/5/13	Affirmative	
464	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-033-1	Final Ballot	1/27/2014	2/5/2014	Quorum: 82.49% Approval: 82.45%	Support 8/31/13	Affirmative	
465	Project 2010-01	Project 2010-01 - Training - PER-005-2	Final Ballot	1/27/2014	2/5/2014	Quorum: 84.02% Approval: 77.06%	Support 11/11/13	Affirmative	

Line	Project	Link to Ballot Results https://standards.nerc.net/Ballot.aspx (clicking in the column to the right of "Ballot Periods" column links to the Ballot Results)	Ballot Type	Start Date	End Date (Sorted Oldest to Newest)	Ballot Results	Recommendation / Date	How NPCC Voted	Comments
466	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards - Definition	Final Ballot	1/31/2014	2/10/2014	Quorum: 81.79% Approval: 90.12%	Support 11/5/13	Affirmative	
467	Project 2010-05.1	Project 2010-05.1 –Protection Systems: Phase 1 (Misoperations): PRC-004-3	Additional Ballot	2/21/2014	3/3/2014	Quorum: 75.06% Approval: 62.63%	Support 9/5/12	Affirmative	Ballot Period Extended to 3/11/14
468	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-002-4	Final Ballot	3/28/2014	4/7/2014	Quorum: 78.21% Approval: 77.62%	Support 3/28/14	Affirmative	
469	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Additional Ballot	4/1/2014	4/10/2014	Quorum: 76.92% Approval: 83.40%	Support 8/31/13	Affirmative	
470	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-002-3	Additional Ballot	4/4/2014	4/14/2014	Quorum: 78.03% Approval: 82.40%		--	
471	Project 2014-04	Project 2014-04 Physical Security - CIP-014-1	Initial Ballot	4/20/2014	4/24/2014	Quorum: 88.60% Approval: 82.07%	Support 4/23/14	Abstain	
472	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	Final Ballot	4/25/2014	5/5/2014	Quorum: 80.37% Approval: 90.00%	Support--4/25/14	Affirmative	
473	Project 2013-04	Project 2013-04 - Voltage and Reactive Control - VAR-001-4, VAR-002-3	Final Ballot	4/23/2014	5/5/2014	Quorum: 83.84% Approval: 88.26%	Support--4/10/14	Affirmative	
474	Project 2014-04	Project 2014-04 - Physical Security - CIP-014-1	Final Ballot	5/1/2014	5/5/2014	Quorum: 92.53% Approval: 85.61%	Support--4/23/14	Abstain	
475	Project 2010-02	Project 2010-02 - Connecting Facilities to the Grid - FAC-001-2 and FAC-002-2	Initial Ballot	5/6/2014	5/15/2014	Quorum: 85.79%/79.08% Approval: 86.28%/78.81%	No Consensus--5/15/14	Reject	
476	Project 2012-13	Project 2012-13 - NUC - Nuclear Plant Interface Coordination	Initial Ballot	5/13/2014	5/22/2014	Quorum: 80.60% Approval: 97.36%	Support--5/20/14	Affirmative	
477	Project 2007-17.3	Project 2007-17.3 - Protection System Maintenance and Testing - Phase 3 (Sudden Pressure Relays) - PRC-005-X	Initial Ballot	5/23/2014	6/2/2014	Quorum: 85.42% Approval: 47.89%			
478	Project 2010-13.3	Project 2010-13.3 - Phase 3 of Relay Loadability: Stable Power Swings	Initial Ballot	5/30/2014	6/9/2014	Quorum: 79.06% Approval: 17.02%	Does not Support--6/6/14	Negative	

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
1.	N/A	Standards Project Prioritization Reference Document and Tool	Project Prioritization Tool		1/21/11	2/10/11	Yes 2/10/11
2.	Project 2007-23	Project 2007-23 - Violation Severity Levels	VSLs		1/20/11	2/18/11	Yes 2/18/11
3.	N/A	CAN-0015--Draft CAN-0015 Unavailability of NERC Tools	CAN-0015 Unavailability of NERC Tools		2/4/11	2/18/11	Yes 2/18/11
4	N/A	CAN-0016--Draft CAN-0016 CIP-001-1 R1 - Applicability to Non-BES	CAN-0016 CIP-001-1, R1		2/4/11	2/18/11	Yes 2/18/11
5.	N/A	CAN-0018--Draft CAN-0018 FAC-008 R.1.2.1 - Terminal Equipment	CAN-0018 FAC-008, R.1.2.1		2/4/11	2/18/11	Yes 2/18/11
6.	Regional Standard	Regional Reliability Standards - PRC-006-NPCC-1 - Automatic Underfrequency Load Shedding	PRC-006-NPCC-1		1/10/11	2/24/11	
7.	Project 2007-07	Project 2007-07 - Vegetation Management - FAC-003	FAC-003-2		1/27/11	2/28/11	Yes 2/28/11
8.	N/A	CAN-0017--Draft CAN-0017 CIP-007 R5 System Access and Password Controls	CAN-0017 CIP-007, R5		2/11/11	3/4/11	Yes 3/4/11
9.	Project 2007-12	Project 2007-12 - Frequency Response	BAL-003-1		2/4/11	3/7/11	Yes 3/7/11
10.	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002, IRO-001, and IRO-014	COM-001 COM-002 IRO-001 IRO-014		1/18/11	3/7/11	Yes 3/7/11

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
11.	NERC RoP	Proposed Changes to Rules of Procedure to Add Section 1700 - Challenges to Determinations	RoP Section 1700		2/14/11	3/7/11	Yes 3/7/11
12.	Project 2009-02	Project 2009-02 - Real-time Reliability Monitoring and Analysis Capabilities	Concept White Paper		2/16/11	4/4/11	Yes 4/4/11
13.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface	Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR Standards		3/4/11	4/4/11	Yes 4/4/11
14.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2		3/9/11	4/8/11	Yes 4/8/11
15.	RFC RoP	Notice of Proposed Changes to RFC Rules of Procedure and Request for Comments			3/1/11	4/15/11	
16.	NERC RoP	Proposed Amendments to NERC Rules of Procedure Appendices 3B and 3D	Appendices 3B and 3D		3/1/11	4/15/11	Yes 4/15/11
17.	Project 2010-15	Project 2010-15 - Urgent Action Revisions to CIP-005-3 - CIP-005	CIP-005		3/29/11	4/28/11	Yes 4/27/11
18.	Project 2009-06	Project 2009-06 - Facility Ratings - FAC-008 and FAC-009	FAC-008-3		3/17/11	5/2/11	Yes 5/2/11
19.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		4/13/11	5/12/11	Yes 5/9/11
20.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition		4/28/11	5/27/11	Yes 5/27/11
21.	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs	TPL-001-2		4/18/11	5/31/11	Yes 5/31/11

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
22.	Project 2007-03	Project 2007-03 - Real-time Operations - TOP-001 through TOP-008 and PER-001	TOP-001 through TOP-008 and PER-001		4/26/11	6/9/11	Yes 6/9/11
23.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition		5/11/11	6/10/11	Yes 6/10/11
24.	NERC RoP	Rules of Procedure Development Team: BES Definition Exception Process	BES Definition Exception Process		5/11/11	6/10/11	Yes 6/10/11
25.	N/A	CAN-0024--Draft CAN-0024 CIP-002 through CIP-009 Routable Protocols and Data Diodes	CAN-0024 CIP-002 through CIP-009		5/20/11	6/10/11	
26.	N/A	CAN-0029--Draft CAN-0029 PRC-004-1 R1, R2 and R3 Misoperations	CAN-0029 PRC-004-1 R1, R2 and R3		5/20/11	6/10/11	
27.	N/A	CAN-0030--Draft CAN-0030 Attestations	CAN-0030 Attestations		5/20/11	6/10/11	
28.	N/A	CAN-0039--Draft CAN-0039 DOE Form 407	CAN-0039 DOE Form 407		5/20/11	6/10/11	
29.	Project 2010-05.1	Project 2010-05.1 – Protection Systems: Phase 1 (Misoperations)			6/10/11	7/11/11	
30.	Project 2007-09	Project 2007-09 – Generator Verification – MOD-025-2, MOD-027-1, PRC-019-1	MOD-025-2 MOD-027-1 PRC-019-1		6/15/11	7/15/11	Yes 7/15/11
31.	Project 2010-07	Project 2010-07 – Generator Requirements at the Transmission Interface – Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR standards	Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR standards		6/17/11	7/17/11	Yes 7/15/11
32.	Project 2007-09	Project 2007-09 – Generator Verification – MOD-026-1 and PRC-024-1	MOD-026-1 and PRC-024-1		6/15/11	8/1/11	Yes 8/1/11

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
33.	NERC RoP	Proposed Changes to NERC Rules of Procedure and associated Appendices (Appendix 4B – Sanction Guidelines; and Appendix 4C – Compliance Monitoring and Enforcement Program)	Appendices 4B and 4C		6/30/11	8/15/11	
34.	N/A	Compliance Application Notice (CAN) Process	CAN Process		8/15/11	9/6/11	Yes 9/6/11
35..	N/A	CAN-0016 CIP-001 R1 - Sabotage Reporting Procedure	CAN-0016 CIP-001, R1		8/15/11	9/6/11	Yes 9/6/11
36.	N/A	DRAFT CANs Posted for Comment and Retirement of CAN-0001 through 0004	CAN-0001 through 0004 Retirement		8/31/11	9/21/11	
37.	NERC RSDP	NERC 2012-2014 Reliability Standards Development Plan	2012-2014 RSDP		9/12/11	9/26/11	Yes 9/26/11
38.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		8/15/11	9/28/11	Yes 9/28/11
39.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System - Initial Ballot of Definition of BES	BES Definition		8/26/11	10/10/11	Yes 10/10/11
40.	Project 2010-17	Project 2010-17 - Bulk Electric System (BES) Definition - Technical Principles for Demonstrating BES Exceptions	Technical Principles for Demonstrating BES Exceptions		8/26/11	10/10/11	Yes 10/10/11

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
41.	N/A	New CAN Template, five DRAFT CANs for Industry review and CANs Status posted to NERC Compliance's Web site.	CANs		9/23/11	10/14/11	Yes 10/14/11
42.	RoP	Proposed Changes to NERC Rules of Procedure and All Appendices			9/2/11	10/17/11	
43.	Project 2010-17	Project 2010-17 - Bulk Electric System (BES) Definition - Rules of procedure Modifications to Support BES Exception Requests	RoP Section 509, Section 1703 and Appendix 5C		9/13/11	10/27/11	Yes 10/27/11
44.	N/A	CAN-0010--Definition of "Annual" and Implementation of Annual Requirements	CAN-0010 Definition of Annual		10/10/11	10/31/11	Yes 10/31/11
45.	N/A	CAN-0011--PRC-005-1 R2: New Equipment	CAN-0011 PRC-005-1 R2		10/10/11	10/31/11	Yes 10/31/11
46.	N/A	CAN-0012--Completion of Periodic Activity Requirements During Implementation Plan	CAN-0012 Completion of Periodic Activity Requirements		10/10/11	10/31/11	Yes 10/31/11
47	N/A	CAN-0013--PRC-023 R1 and R2 Effective Dates for Switch-on-to-Fault Schemes	CAN-0013 PRC-023 R1 and R2		10/10/11	10/31/11	
48.	N/A	CAN-0015--Unavailability of NERC Software Tools	CAN-0015 NERC Tools		10/10/11	10/31/11	Yes 10/31/11
49.	N/A	CAN-0022--VAR-002-1.1b R1 and R3 Generator Operation in Manual Mode	CAN-0022 VAR-002-1.1b R1 and R3		10/10/11	10/31/11	

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
50.	N/A	CAN-0024--CIP-002 R3 Routable Protocols and Data Diode Devices	CAN-0024 CIP-002, R3		10/10/11	10/31/11	Yes 10/31/11
51.	N/A	CAN-0026--TOP-006 R3 Protection Relays	CAN-0026 TOP-006, R3		10/10/11	10/31/11	Yes 10/31/11
52.	N/A	CAN-0028--TOP-006-1 R1.2 Reporting Responsibilities	CAN-0028 TOP-006-1, R1.2		10/10/11	10/31/11	
53.	N/A	CAN-0020--TPL-002, TPL-003, TPL-004 and TOP-002 Equipment Maintenance Outages	CAN-0020 TPL-002, TPL-003, TPL-004 and TOP-002		10/19/11	11/9/11	
54.	N/A	CAN-0030--Attestations	CAN-0030		10/19/11	11/9/11	
55.	Project 2011-INT-01	Project 2011-INT-01 - Interpretation of MOD-028 for Florida Power & Light Company	MOD-028, R3.1		10/3/11	11/16/11	Yes 11/16/11
56.	Project 2009-22	Project 2009-22 - Interpretation of COM-002-2 R2 by the IRC	Interpretation of COM-002-2, R2		10/4/11	11/18/11	Yes 11/18/11
57.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface	Various BAL, CIP, EOP, FAC, IRO, MOD, PER, PRC, TOP, and VAR Standards		10/5/11	11/18/11	Yes 11/18/11
58.	N/A	Draft Directive Regarding Generator Transmission Leads	Draft Directive #2011 CAG-001		10/17/11	11/18/11	Yes 11/18/11
59.	Project 2008-10	Project 2008-10 - Interpretation of CIP-006-1 R1.1 by Progress Energy	Interpretation of CIP-006-1, R1.1		10/12/11	11/21/11	Yes 11/21/11
60.	N/A	CAN-0040 - BAL-003 Frequency Bias Calculation			11/2/11	11/23/11	
61.	N/A	CAN-0043 - PRC-005 Protection System Maintenance and Testing Evidence	PRC-005 Evidence		11/2/11	11/23/11	Yes 11/22/11

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
62.	Project 2007-12	Project 2007-12 - Frequency Response	BAL-003-1			12/8/11	Yes 12/8/11
63.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2			12/12/11	Yes 12/12/11
64.	N/A	Draft CAN-0027: TOP-003 R2 Coordination of Scheduled Outages	CAN-0027 TOP-003, R2		11/22/11	12/14/11	
65.	NERC RoP	Proposed Changes to the NERC Rules of Procedure and Associated Appendices			11/7/11	12/22/11	
66.	NERC RoP	Notice of Revisions to Proposed New Sections 1.1.24 and 5.11 of Appendix 4C of the NERC Rules of Procedure, as Originally Posted for Comment on November 7, 2011			11/22/11	12/22/11	
67.	Regional Standard	Regional Reliability Standard PRC-006-NPCC-1 — Automatic Underfrequency Load Shedding	PRC-006-NPCC-1		11/22/11	12/22/11	
68.	Project 2008-06	Project 2008-06 - Cyber Security - Order 706 - CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1 (Version 5 CIP Standards)	Version 5 CIP Standards		11/7/11	1/6/12	Yes 1/6/12
69.	Project 2007-03	Project 2007-03 - Real-time Transmission Operations - TOP-001-2, TOP-002-3 and TOP-003-2	TOP-001-2 TOP-002-3 TOP-003-2		12/14/11	1/12/12	Yes 1/12/12
70.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	BES Definition, Phase 2		1/4/12	2/3/12	Yes 2/3/12

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
71.	N/A	Order 754 - Request for Data or Information	Data Request		12/22/11	2/6/12	Yes 2/6/12
72.	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002 and IRO-001-3	COM-001 COM-002 IRO-001-3		1/9/12	2/9/12	Yes 2/8/12
73.	WECC Regional Standard	Regional Reliability Standard BAL-004-WECC-02 - Automatic Time Error Correction	BAL-004-WECC-02		1/23/12	3/9/12	
74.	WECC Regional Standard	Regional Reliability Standard BAL-001-0.1a - Real Power Balancing Control Performance - WECC Variance	BAL-001-0.1a		1/23/12	3/9/12	
75.	N/A	NERC Functional Model Demand Response Functions and Entities	NERC Functional Model		2/13/12	3/14/12	
76.	Project 2009-26	Project 2009-26 - Interpretation of CIP-004-1 for WECC	Interpretation of CIP-004-1		2/8/12	3/23/12	Yes 3/23/12
77.	Project 2010-INT-05	Interpretation 2010-INT-05 - Interpretation of CIP-002-1 R3 for Duke Energy	Interpretation of CIP-002-1, R3		2/8/12	3/23/12	Yes 3/23/12
78.	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR -002 for Constellation	Interpretation of VAR -002		2/8/12	3/23/12	Yes 3/23/12
79.	Project 2007-17	Project 2007-17 Protection System Maintenance and Testing - PRC-005	PRC-005-2		2/28/12	3/28/12	Yes 3/28/12
80.	Project 2007-09	Project 2007-09 Generator Verification - MOD-026-1 and PRC-024-1	MOD-026-1 and PRC-024-1		2/29/12	3/29/12	Yes 3/29/12

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
81.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface - FAC-003-X, FAC-003-3	FAC-003-X FAC-003-3		3/9/12	4/9/12	Yes 4/9/12
82.	Project 2007-09	Project 2007-09 Generator Verification - MOD-025-2, MOD-027-1, and PRC-019-1	MOD-025-2 MOD-027-1 PRC-019-1		2/29/12	4/16/12	Yes 4/16/12
83.	Project 2010-07	Project 2010-07 - Generator Requirements at the Transmission Interface - PRC-005-1.1a	PRC-005-1.1a		3/2/12	4/16/12	Yes 4/16/12
84.	Project 2007-03	Project 2007-03 - Real-time Transmission Operations	TOP-001 through TOP-008 and PER-001		3/22/12	4/20/12	Yes 4/20/12
85.	Project 2012-INT-02	Request for Interpretation - Project 2012-INT-02 TPL-003-0a and TPL-004-0 for SPCS	Interpretation of TPL-003-0a and TPL-004-0		4/24/12	5/4/12	
86.	Project 2008-06	Project 2008-06 - Cyber Security Order 706 Version 5 CIP	CIP-002 and CIP-003 - Comment Form A		4/12/12	5/21/12	Yes 5/20/12
			CIP-004 thru CIP-007 - Comment Form B		4/12/12	5/21/12	Yes 5/20/12
			CIP-008 thru CIP-011 - Comment Form C		4/12/12	5/21/12	Yes 5/20/12
			Definitions and Implementation Plan - Comment Form D		4/12/12	5/21/12	Yes 5/20/12
87.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2		4/25/12	5/24/12	Yes 5/24/12
88.	Project 2007-12	Project 2007-12 Frequency Response Technical Conferences			5/30/12	6/15/12	

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
89.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	COM-003		5/7/12	6/20/12	Yes 6/20/12
90.	N/A	Adequate Level of Reliability Revised Definition and Associated Documents	Adequate Level of Reliability (ALR)		4/25/12	6/25/12	Yes 6/25/12
91.	N/A	Order 754 - Request for Data or Information	Data Request		5/11/12	6/25/12	Yes 6/25/12
92.	Project 2011-INT-02	Project 2011-INT-02 - Interpretation of VAR -002 for Constellation	Interpretation of VAR -002		5/22/12	6/27/12	Yes 6/27/12
93.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		5/29/12	6/27/12	Yes 6/27/12
94.	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserve	BAL-001-1		6/4/12	7/3/12	Yes 7/3/12
			BAL-002-2		6/4/12	7/3/12	Yes 7/3/12
			BAL-012-1		6/4/12	7/3/12	Yes 7/3/12
			BAL-013-1		6/4/12	7/3/12	Yes 7/3/12
95.	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-001 and PRC-027		5/21/12	7/5/12	Yes 7/5/12
96.	N/A	Cost Effective Analysis Process (CEAP) for NERC ERO Standards	CEAP		5/7/12	7/6/12	Yes 7/6/12
97.	Project 2006-06	Project 2006-06 - Reliability Coordination - COM-001, COM-002 and IRO-001-3	COM-001, COM-002 and IRO-001-3		6/7/12	7/6/12	Yes 7/6/12
98.	Project 2006-02	Project 2006-02 – Assess Transmission Future Needs and Develop Transmission Plans	TPL-002-1b, footnote ‘b’ and TPL-001-3, footnote 12		6/19/12	7/9/12	Yes 7/9/12
99.	N/A	Standard Processes Manual Revisions to Implement SPIG Recommendations	SPIG Reco		6/20/12	7/19/12	Yes 7/19/12

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
100.	Project 2012-INT-02	Project 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for System Protection and Control Subcommittee	- Interpretation of TPL-003-0a and TPL-004-0		6/20/12	7/20/12	Yes 7/19/12
101.	Project 2012-INT-05	Interpretation of 2012-INT-05 - Interpretation of CIP-002-3 for OGE	Interpretation of CIP-002-3		6/27/12	7/27/12	Yes 7/27/12
102.	Project 2011-INT-02	Project 2011-INT-02 - Rapid Revision to Address Interpretation of VAR-002 for Constellation	Rapid Revision to VAR-002		7/18/12	7/27/12	Yes 7/26/12
103.	Project 2010-INT-01	Project 2010-INT-01 - Rapid Revision of TOP-006 for FMPP	Rapid Revision of TOP-006		6/14/12	7/30/12	Yes 7/27/12
104.	Project 2012-08.1	Project 2012-08.1 - Phase 1 of Glossary Updates: Statutory Definitions	Glossary of Terms		6/19/12	8/2/12	Yes 8/2/12
105.	N/A	Reliability Guideline: System Operator Verbal Communications – Current Industry Practices	System Operator Verbal Communications		6/26/12	8/10/12	Yes 8/9/12
106.	Project 2007-17	Project 2007-17 - Protection System Maintenance and Testing - PRC-005	PRC-005-2		7/27/12	8/27/12	Yes 8/27/12
107.	Project 2010-11	Project 2010-11 - TPL Table 1 Order TPL-002-1b, footnote 'b' and TPL-001-3, footnote 12	TPL-002-1b, footnote 'b' and TPL-001-3, footnote 12		7/31/12	8/29/12	Yes 8/29/12
108.	Project 2006-02	Project 2006-02 - Assess Transmission and Future Needs			7/31/12	8/30/12	
109.	Project 2009-19	Project 2009-19 – Interpretation of BAL-002 by NWPP Reserve Sharing Group			7/25/12	9/4/12	

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
110.	Project 2013-02	Project 2013-02 - Paragraph 81	Paragraph 81		8/3/12	9/4/12	Yes 9/4/12
111.	Project 2010-05.1	Project 2010-05.1 - Protection Systems: Phase 1 (Misoperations)			7/25/12	9/7/12	Yes 9/7/12
112.	N/A	Definition of Adequate Level of Reliability	Adequate Level of Reliability (ALR)		8/15/12	9/13/12	Yes 9/13/12
113.	N/A	2013-2015 Reliability Standards Development Plan	2013-2015 RSDP		8/17/12	9/18/12	Yes 9/18/12
114.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols	COM-003-1		8/22/12	9/20/12	Yes 9/20/12
115.	Project 2009-01	Project 2009-01 - Disturbance and Sabotage Reporting	EOP-004-2		8/29/12	9/27/12	
116.	SPP Regional Standard	Regional Reliability Standard PRC-006-SPP-01 Automatic Underfrequency Load Shedding	PRC-006-SPP-01		8/15/12	9/28/12	
117.	Project 2008-06 Project 2008-06	Project 2008-06 - Cyber Security - Order 706 - CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1	Version 5 CIP Standards		9/11/12	10/10/12	Yes 10/10/12
			RSAW		9/11/12	10/10/12	Yes 10/10/12
118.	MRO SPM	Regional Reliability Standards - MRO Standards Process Manual			8/28/12	10/11/12	
119.	N/A	Standard Process Manual Revisions to Implement SPIG Recommendations	SPIG Reco		8/29/12	10/12/12	Yes 10/10/12
120.		Revisions to Outstanding VRFs and VSLs			9/5/12	10/19/12	
121.	Project 2013-01	Project 2013-01 - Cold Weather Preparedness			9/25/12	10/24/12	

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
122.	Project 2007-09	Project 2007-09 - Generator Verification			9/28/12	10/29/12	
123.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System			10/4/12	11/5/12	
124.	2007-12	Project 2007-12 - Frequency Response			10/5/12	11/7/12	
125.	Project 2008-06	Project 2008-06 - Cyber Security - Order 706 - CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1	Version 5 CIP Standards		10/26/12	11/7/12	
126.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	PRC-025		10/5/12	11/7/12	
127.	N/A	IRO-006-WECC-2			10/3/12	11/16/12	
128.	Project 2010-11	Project 2010-11 - TPL Table 1, Footnote B			10/5/12	11/19/12	
129.	Project 2012-INT-02	Interpretation 2012-INT-02 - Interpretation of TPL-003-0a and TPL-004-0 for SPCS	Interpretation of TPL-003-0a and TPL-004-0		10/22/12	12/5/12	Yes 12/5/12
130.	Project 2013-02	Project 2013-02 - Paragraph 81	Paragraph 81		10/25/12	12/10/12	Yes 12/10/12
131.	Project 2012-INT-06	Project 2012-INT-06 - Interpretation of CIP-003-3 for Consumers Energy	- Interpretation of CIP-003-3		11/9/12	12/10/12	Yes 12/10/12
132.	Project 2012-INT-04	Project 2012-INT-04 - Interpretation of CIP-007-3 for ITC	- Interpretation of CIP-007-3		11/9/12	12/10/12	Yes 12/10/12
133.	Project 2007-02	Project 2007-02 - Operating Personnel Communication Protocols - RSAW	COM-003-1		11/14/12	12/13/12	Yes 12/13/12
			COM-003-1 RSAW		11/14/12	12/13/12	Yes 12/13/12
134.	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-001 and PRC-027		11/16/12	12/17/12	Yes 12/17/12
135.	Project 2012-INT-05	Project 2012-INT-05 - Interpretation of CIP-002-3 for OGE	Interpretation of CIP-002-3		11/6/12	12/20/12	Yes 12/20/12

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
136.	N/A	Standard Processes Manual to Implement SPIG Revisions	SPIG Reco		11/21/12	12/20/12	Yes 12/20/12
137.	Project 2010-11	Project 2010-11 - TPL Table 1, Footnote B	TPL-002-1b, footnote 'b' and TPL-001-3, footnote 12		12/10/12	1/11/13	Yes 1/11/13
138.	Project 2007-09	Project 2007-09 - Generator Verification - PRC-024-1	PRC-024-1		12/12/12	1/11/13	Yes 1/11/13
139.	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-012-1	BAL-012-1		11/30/12	1/14/13	Yes 1/14/13
140.	N/A	Reliability Guideline--Draft Generating Unit Winter Weather Readiness - Current Industry Practices			12/20/12	2/4/13	Yes 2/4/13
141.	Project 2010-05-1	Project 2010-05-1 Protection System Misoperations					Yes 2/20/13
142.	Project 2007-09	Project 2007-09 Generator Verification - PRC-024-1	PRC-024-1	Formal	1/25/13	2/25/13	Yes 2/25/13
143.	N/A	Rapid Revision Procedure		Informal	2/25/13	3/6/13	Yes 3/6/13
144.	Project 2010-13-2	Project 2010-13-2 - Phase 2 of Relay Loadability - Generation - PRC-025-1	PRC-025-1	Formal	1/25/13	3/11/13	Yes 3/11/13
			Supplemental SAR	Informal	1/25/13	3/11/13	Yes 3/11/13
			Cost Effectiveness	CEAP Pilot	1/25/13	3/11/13	Yes 3/11/13
			RSAW	Feedback	1/25/13	3/11/13	Yes 3/11/13
145.	Project 2012-INT-04	Interpretation 2012-INT-04 - Interpretation of CIP-007 for ITC	Interpretation of CIP-007	Formal	2/6/13	3/22/13	Yes 3/22/13
146.	Project 2012-INT-06	Interpretation 2012-INT-06 - Interpretation of CIP-003 for Consumers Energy	Interpretation of CIP-003	Formal	2/6/13	3/22/13	Yes 3/22/13

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
147.	Project 2012-08-1	Project 2012-08-1 - Phase 1 of Glossary Updates--Statutory Definitions	Glossary of Terms	Formal	2/21/13	3/22/13	Yes 3/22/13
148.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003-1	COM-003-1	Formal	3/7/13	4/5/13	Yes 4/5/13
			RSAW	Feedback	3/7/13	4/5/13	Yes 4/5/13
149.	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves	BAL-001-2	Formal	3/12/13	4/25/13	Yes 4/25/13
			BAL-002-2	Formal	3/12/13	4/25/13	Yes 4/25/13
			BAL-013-1	Formal	3/12/13	4/25/13	Yes 4/25/13
150.	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays)	Draft SAR	Informal	4/5/13	5/6/13	Yes 5/6/13
			PRC-005-3	Formal	4/5/13	5/6/13	Yes 5/613
151.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation	PRC-023-3 PRC-025-1	Formal	4/25/13	5/24/13	Yes 5/24/13
152.	Project 2007-11	Project 2007-11 - Disturbance Monitoring — PRC-002 and PRC-018	SAR	Informal	5/03/13	6/03/13	Yes 6/3/13
153.	Project 2007-11	Project 2007-11 - Disturbance Monitoring PRC-002 and PRC-018	Request for Information	Informal	6/05/13	7/05/13	
154.	Project 2007-06	Project 2007-06 - System Protection Coordination - PRC-001 and PRC-027	PRC-001 and PRC-027		6/04/13	7/03/13	Yes 7/03/13
155.	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System (Phase 2)	BES Definition		5/29/13	7/12/13	Yes 7/12/13
156.	TRE Regional Standard	Regional Reliability Standard - BAL-001-TRE-01	BAL-001-TRE-01		5/31/13	7/15/13	
157.	N/A	NPCC Regional Standards Process Manual	NPCC RSPM		6/06/13	7/22/13	

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
158.	Project 2007-02	Project 2007-02 - Operating Personnel Communications Protocols - COM-003	COM-003-1		6/20/13	7/19/13	Yes 7/19/13
159.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-025	PRC-025-1		6/20/13	7/19/13	Yes 7/19/13
160.	Project 2010-13.2	Project 2010-13.2 - Phase 2 of Relay Loadability: Generation - PRC-023	PRC-023-3	Formal	6/20/13	8/05/13	Yes 8/5/13
161.	N/A	SPP RE Regional Standards Process Manual	SPP RSPM		6/26/13	8/09/13	
162.	Project 2013-03	Project 2013-03 - Geomagnetic Disturbance Mitigation	EOP-010-1	Formal	6/27/13	8/12/13	Yes 8/12/13
163.	Project 2007-17.2	Project 2007-17.2 - Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005	PRC-005-3	Formal	7/10/13	8/23/13	Yes 8/23/13
164.	Project 2008-12	Project 2008-12 - Coordinate Interchange Standards - Various INT standards	INT-004-3 INT-006-4 INT-009-2 INT-010-2 INT-011-1	Informal	7/25/13	8/23/13	Yes 8/23/13
165.	Project 2012-05	Project 2012-05 ATC Revisions (MOD A) - MOD-001-2	MOD-001-2	Formal	7/11/13	8/26/13	Yes 8/26/13
166.	Project 2010-01	Project 2010-01 - Training - PER-005-2	PER-005-2	Formal	7/19/13	9/03/13	Yes 9/3/13
167.	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	VAR-001-4 VAR-002-3	Formal	7/19/13	9/03/13	Yes 9/3/13
168	Project 2010-03	Project 2010-03 - Modeling Data (MOD B) - MOD-032-1, MOD-033-1	MOD-032-1 MOD-033-1	Formal	7/22/13	9/04/13	Yes 9/4/13

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
169.	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	MOD-031-1	Formal	7/22/13	9/04/13	Yes 9/4/13
170	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System – Phase 2	BES Definition Phase 2	Formal	8/6/13	9/4/13	Yes 9/4/13
171	Project 2012-13	Project 2012-13 - NUC Five-Year Review	NUC-001-2	5-year review	7/26/13	9/9/13	Yes 9/9/13
172	2014-2016 RSDP	2014-2016 Reliability Standards Development Plan	Reliability Standards Development Plan	Annual Review	8/30/13	9/13/13	Yes 9/13/13
173	Project 2010-02	Project 2010-02 Five-Year Review of FAC Standards	FAC-001-1 FAC-002-1	5-year review	8/1/13	9/16/13	Yes 9/16/13
174	Project 2010-02	Project 2010-02 Five-Year Review of FAC Standards	FAC-003-3 FAC-008-3 FAC-010-2.1 FAC-011-2 FAC-013-2 FAC-014-2	5-year review	8/1/13	9/16/13	Yes 9/16/13
175	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves - BAL-002-2, BAL-013-1	BAL-002-2	Formal	8/2/13	9/16/13	Yes 9/16/13
176	Project 2009-03	Project 2009-03 — Five-Year Review of Emergency Operations EOP-001, EOP-002, EOP-003, and IRO-001	EOP-001-2.1b EOP-002-3.1 EOP-003-2	5-year review	8/6/13	9/19/13	Yes 9/19/13
177	Project 2012-09	Project 2012-09 IRO Five-Year Review	IRO-003-2 IRO-004-2 IRO-005-4 IRO-006-5 IRO-006-East IRO-008-1 IRO-009-1 IRO-010-1a	5-year review	8/7/13	9/20/13	Yes 9/20/13
178	Project 2008-02	Project 2008-02 Undervoltage Load Shedding	Revised SAR	Informal	9/10/13	10/9/13	Yes 10/9/13

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
179	Project 2013-03	Project 2013-03 Geomagnetic Disturbance Mitigation	EOP-010-1	Formal	9/4/13	10/18/13	Yes 10/18/13
180	Project 2010-17	Project 2010-17 - Definition of Bulk Electric System	BES Definition	Formal	9/27/13	10/28/13	Yes 10/28/13
181	Project 2007-02	Project 2007-02 Operating Personnel Communications Protocols	COM-002-4	Formal	10/21/13	11/7/13	Yes 11/4/13
182	Project 2010-01	Project 2010-01 Training	PER-005-2	Formal	9/27/13	11/12/13	Yes 11/12/13
183	Project 2008-12	Project 2008-12 Coordinate Interchange Standards	Various INT Standards	Formal	9/30/13	11/13/13	Yes 11/13/13
184	Project 2012-05	Project 2012-05 ATC Revisions (MOD A)	MOD-001-2	Formal	10/4/13	11/20/13	Yes 11/18/13
185	Project 2010-03	Project 2010-03 Modeling Data (MOD B)	MOD-032-1, MOD-033-1	Formal	10/07/13	11/20/13	
186	Project 2010-04	Project 2010-04 Demand Data (MOD C)	MOD-031-1	Formal	10/09/13	11/22/13	Yes 11/22/13
187	Project 2013-04	Project 2013-04 Voltage and Reactive Control	VAR-001-4, VAR-002-3	Formal	10/11/13	11/25/13	Yes 11/25/13
188	Project 2009-03	Project 2009-03 Emergency Operations	SAR	Informal	11/06/13	12/05/13	Yes 12/5/13
189	Project 2010-14.1	Project 2010-14.1 - Phase 1 of Balancing Authority Reliability-based Controls: Reserves	BAL-002-2	Formal	10/28/13	12/11/13	Yes 12/11/13
190	Project 2007-11	Project 2007-11 - Disturbance Monitoring	PRC-002-2	Formal	11/01/13	12/16/13	Yes 12/16/13
191	Project 2007-06	Project 2007-06 - System Protection Coordination	PRC-027	Formal	11/04/13	12/18/13	Yes 12/18/13
192	Project 2014-01	Project 2014-01 - Standards Applicability for Dispersed Generation Resources	SAR	Formal	11/20/13	12/19/13	Yes 12/19/13

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
193	Project 2010-01	Project 2010-01 Training - PER-005-2	PER-005-2	Formal	12/4/13	1/22/14	Yes 1/17/14
194	Project 2010-03	Project 2010-03 Modeling Date - MOD B	MOD-033-1	Formal	12/6/13	1/22/14	Yes 1/21/14
195	Project 2008-12	Project 2008-12 Coordinate Interchange Standards	INT-004-3 INT-010-2	Formal	1/10/14	1/24/14	Yes 1/22/14
196	Project 2007-02	Project 2007-02 Operating Personnel	COM-002-4	Formal	1/22/14	1/31/14	Yes 1/31/14
197	Project 2014-02	Project 2014-02 Standard Authorization Request – Cyber Security Standards	CIP SAR	Informal	1/17/14	2/18/14	Yes 2/18/14
198	2014 Work Plan	2014 Work Plan for NERC Reliability Standards Development	2014 Work plan			2/21/13	Yes 2/21/14
199	Project 2010-17	Project 2010-17 Definition of Bulk Electric System - Phase 2	BES	Informal	1/29/14	2/27/14	Yes 2/27/14
200	Project 2010-05.1	Project 2010-05.1 Protection System: Phase 1 (Misoperations) - PRC-004-3	PRC-004-3	Formal	1/17/14	3/11/14	Yes 3/2/14
201	Project 2012-13	Project 2012-13 NUC-Nuclear Plant Interface Coordination Standard Authorization Request	NUC-001-2.1 SAR	Informal	2/12/14	3/13/14	Yes 3/13/14
202	Project 2010-05.2	Project 2010-05.2 Special Protection Systems (Phase 2 of Protection Systems) - SAR	SAR	Informal	2/18/14	3/19/14	Yes 3/19/14
203	Project 2014-03	Project 2014-03 - Revisions to TOP/IRO Reliability Standards	SAR	Formal	02/21/14	03/24/14	Yes 3/24/14

RSC Meeting #14-2, Agenda Item 6.3: Comment History

(Since last RSC Meeting)

Line	Project#	Description	Document	Comment Type	Start Date	End Date	NPCC Submitted
204	Project 2014-03	Technical Conferences on Revisions to TOP/IRO Reliability Standards	Technical Conference Topics	Informal	03/11/14	03/24/14	
205	Project 2014-04	Project 2014-04 - Physical Security	SAR	Informal	03/21/14	03/28/14	Yes 3/28/14
206	Project 2010-14.2	Project 2010-14.2 - Periodic Review of BAL Standards	Reco to Revise BAL-005 and BAL-006	Formal	02/21/14	04/07/14	
207	2010-05.2	Project 2010-05.2 - Phase 2 of Protection Systems - Revised Definition of Special Protection System	SPS Definition	Informal	03/11/14	04/09/14	Yes 4/9/14
208	Project 2010-04	Project 2010-04 - Demand Data (MOD C) - MOD-031-1	MOD-031-1	Formal	02/25/14	04/10/14	Yes 4/10/14
209	Project 2013-04	Project 2013-04 Voltage and Reactive Control - VAR-001-4, VAR-002-3	VAR-002-3	Formal	02/27/14	04/14/14	Yes 4/14/14
210	Project 2008-02	Project 2008-02 - Undervoltage Load Shedding - PRC-010, PRC-020, PRC-021 and PRC-022	PRC-010-1	Informal	03/17/14	04/16/14	Yes 4/16/14
211	Project 2014-04	Project 2014-04 Physical Security - CIP-014-1	CIP-014-1	Formal	04/10/14	04/24/14	Yes 4/24/14
212	Project 2009-03	Project 2009-03 Emergency Operations – EOP-011-1	EOP-011-1	Informal	03/28/14	04/28/14	Yes 4/28/14
213							
214							

Note: RSC past comment forms are being posted on the NPCC Website under "Standards - Regional Standards Comments."

Information in a Regional Standard Authorization Request (RSAR)

The tables below identify information to be submitted in a Regional Standard Authorization Request to the NPCC Regional Standards Process Manager, NPCCstandard@npcc.org . The NPCC Regional Standards Process Manager shall be responsible for implementing and maintaining this form as needed to support the information requirements of the standards process.

Regional Standard Authorization Request Form

Title of Proposed Standard:
Request Date:

RSAR Requester Information

Name:	**RSAR Type (Check box for one of these selections.)**	
Company:	☐	New Standard
Telephone:	☐	Revision to Existing Standard
Fax:	☐	Withdrawal of Existing Standard
Email:	☐	Urgent Action

Purpose (Describe the purpose of the proposed standard – what the standard will achieve in support of reliability.**)**
Industry Need (Provide a detailed statement justifying the need for the proposed standard, along with any supporting documentation**.)**
Brief Description (Describe the proposed standard in sufficient detail to clearly define the scope in a manner that can be easily understood by others.**)**

Reliability Functions

The Standard will Apply to the Following Functions (Check all applicable boxes.)		
☐	Reliability Coordinator	The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.
☐	Balancing Authority	The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
☐	Interchange Authority	Authorizes valid and balanced Interchange Schedules.
☐	Planning Authority	The responsible entity that coordinates and integrates transmission facility and service plans, resource plans, and protection systems.
☐	Transmission Service Provider	The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.
☐	Transmission Owner	The entity that owns and maintains transmission facilities.
☐	Transmission	The entity responsible for the reliability of its "local" transmission system,

	Operator	and that operates or directs the operations of the transmission facilities.
☐	Transmission Planner	The entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority Area.
☐	Resource Planner	The entity that develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority Area.
☐	Generator Operator	The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.
☐	Generator Owner	Entity that owns and maintains generating units.
☐	Purchasing-Selling Entity	The entity that purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. Purchasing-Selling Entities may be affiliated or unaffiliated merchants and may or may not own generating facilities.
☐	Distribution Provider	Provides and operates the "wires" between the transmission system and the customer.
☐	Load-Serving Entity	Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check all boxes that apply.)*	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.
☐	5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

☐	7. The security of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.

Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*
Recognizing that reliability is an Common Attribute of a robust North American economy:
1. A reliability standard shall not give any market participant an unfair competitive advantage.Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes

Detailed Description (Provide enough detail so that an independent entity familiar with the industry could draft a standard based on this description.)

Related Standards

Standard No.	**Explanation**

Related SARs or RSARs

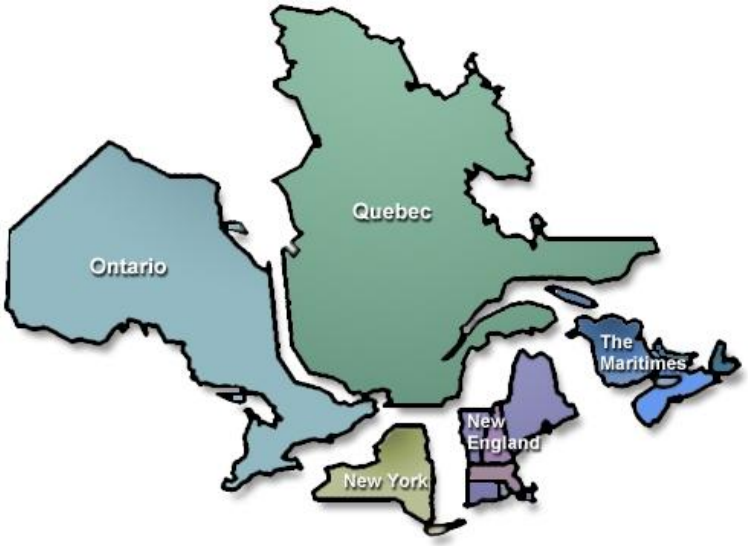
SAR ID	**Explanation**

NPCC, Inc.

NORTHEAST POWER COORDINATING COUNCIL, INC.
1515 BROADWAY, NEW YORK, NY 10036-8901 TELEPHONE: (212) 840-1070 FAX: (212) 302-2782

Northeast Power Coordinating Council, Inc.

Regional Reliability Standards Development Procedure



Approved by NPCC Board of Directors
September 19, 2007
Approved by NERC BOT October 23, 2007
Adopted by FERC March 21, 2008

NPCC

REGIONAL RELIABILITY STANDARDS DEVELOPMENT PROCEDURE

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 2

II. REGIONAL RELIABILITY STANDARD DEVELOPMENT PROCEDURE

1. CHARACTERISTIC ATTRIBUTES 2
2. ELEMENTS OF A REGIONAL STANDARD 5
3. TERMS AND FUNCTIONS 8
4. PROCEDURE DESCRIPTION 10
5. FLOWCHART 15
6. ERO AND REGULATORY APPROVALS 16
7. APPEALS 16

III. APPENDIX

A) RSAR FORM 19

I. EXECUTIVE SUMMARY

The purpose of the Northeast Power Coordinating Council, Inc. ("NPCC"), is to enhance the reliability of the international, interconnected bulk power system in Northeastern North America through the development of more stringent and specific regional reliability standards and compliance assessment and enforcement of continent-wide and regional reliability standards pursuant to the execution and implementation of a Regional Delegation Agreement with the Electric Reliability Organization ("ERO") and applicable Canadian Memoranda of Understanding that are backstopped by the Federal Energy Regulatory Commission ("FERC") and Canadian Provincial authorities. In the development and enforcement of Regional Reliability Standards, NPCC, to the extent possible, facilitates attainment of fair, effective, efficient, and competitive electric markets.

General Membership in NPCC is voluntary and is open to any person or entity, including any entity participating in the Registered Ballot Body of the ERO that has an interest in the reliable operation of the Northeastern North American bulk power system.

The NPCC Regional Reliability Standards Development Procedure describes the procedures, policies and practices implemented to ensure an "open, fair, and inclusive" process for the transparent initiation, development, implementation and revision of NPCC Regional Reliability Standards necessary for the reliable operation of the international and interconnected bulk power system in Northeast North America. These Standards will, in all cases, not be inconsistent with or less stringent than any requirements of the North American Electric Reliability Council/Electric Reliability Organization (NERC/ERO) Reliability Standards. The procedure will not unnecessarily delay the development of the proposed reliability standards. Each regional reliability standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of the reliability of the regional bulk power system. Each standard shall also be consistent with all of pertinent reliability principles and criteria, thereby ensuring that no standard undermines reliability through an unintended consequence.

II. REGIONAL RELIABILITY STANDARD DEVELOPMENT PROCEDURE

1. CHARACTERISTIC ATTRIBUTES

The NPCC Regional Reliability Standards Development Procedure is:

- **Open** — The NPCC Regional Reliability Standards Development Procedure provides any person the ability to participate in the development of a standard. Any entity that is directly and materially affected by the reliability of the NPCC's bulk power system has the ability to participate in the development and approval of reliability standards. There are no undue financial barriers to participation. Participation in the open comment process is not conditional upon membership in the ERO, NPCC or any organization, and participation is not unreasonably restricted on the basis of technical qualifications or other such requirements. NPCC utilizes a website to accomplish this. Online posting and review of standards and the real time sharing of comments uploaded to the website allow complete transparency.

- **Inclusive** — The NPCC Regional Reliability Standards Development Procedure provides any person with a direct and material interest the right to participate by expressing an opinion and its basis, have that position considered, and appealed through an established appeals process if adversely affected.

- **Balanced** — The NPCC Regional Reliability Standards Development Procedure has a balance of interests and all those entities that are directly and materially affected by the reliability of the NPCC's bulk power system are welcome to participate and shall not be dominated by any two interest categories and no single interest category shall be able to defeat a matter. This will be accomplished through the NPCC Bylaws defining eight sectors (categories) for voting.

- **Fair Due Process** — The NPCC Regional Reliability Standards Development Procedure provides for reasonable notice and opportunity for public comment. The procedure includes public notice of the intent to develop a standard, a 45 calendar day public comment period on the proposed standard request, or standard with due consideration of those public comments, and responses to those comments will be posted on the NPCC website. A final draft will be posted for a 30 calendar day pre-balloting period, and then a ballot of NPCC Members will be conducted. Upon approval by the NPCC Members, the NPCC Board then votes to approve submittal of the Regional Standard to NERC.

- **Transparent** — All actions material to the development of Regional Reliability Standards are transparent and information regarding the progress is posted on the NPCC website as well as through extensive email lists.

In as much as NPCC is one of several regional entities within the Eastern Interconnection of North America, there will be **no** *presumption of validity* by the ERO for any NPCC Regional Reliability Standard. In order to receive the approval of the ERO, the NPCC Reliability Standards Development Process must also achieve the following objectives:

- **No Adverse Impact on Reliability of the Interconnection** —An NPCC Regional Reliability Standard provides a level of bulk power system reliability that is necessary and adequate to protect public health, safety, welfare, and North American security and will not have an adverse impact on the reliability of the Interconnection or other Regions within the Interconnection.

- **Justifiable Difference** — An NPCC Regional Reliability Standard is based on justifiable differences between Regions, such as different electrical systems or facilities, sensitivity of load to disruptions, sensitivity of generation to disruptions, frequency and voltage sensitivity, system operating limit development and facilities ratings process, electrical system interactions, etc.

- **Uniformity**- NPCC Regional Reliability Standards shall provide for as much uniformity as possible with reliability standards across the interconnected bulk

power system of the North American continent. A NPCC Reliability Standard shall be more stringent than a continent-wide reliability standard, may include a regional variation that addresses matters that the continent-wide reliability standard does not, or shall be a regional difference necessitated by a physical difference in the northeast's bulk power system, where the interpretation of the phrase "physical difference" will be consistent with FERC's Order, issued September 22, 2004, Granting Request For Clarification regarding Docket No. PL04-5-000, Policy Statement on Matters Related to Bulk Power System Reliability.

- **No Undue Adverse Impact on Commerce** — An NPCC Regional Reliability Standard will not cause any undue adverse impact on business activities that are not necessary for reliability of the Region and its interconnected Regions. All regional reliability standards shall be consistent with NERC's market principles.

Other Attributes of the NPCC Regional Reliability Standards Development Procedure include;

- **Maintenance of Regional Reliability Standards-**NPCC Regional Standards will be reviewed for possible revision at least every three years and follow the same process as a new standard. The old standard will remain in place until such time as the revised version has passed through the entire process, at which point the old standard will be retired in accordance with any applicable new implementation plan associated with the approved revised standard. The review process shall be conducted by soliciting comments from the stakeholders and through open posting on the NPCC website. If no changes are warranted, Regional Standards Committee (RSC) shall recommend to the NPCC Board that the standard be reaffirmed. If the review indicates a need to revise or withdraw a standard, a regional standard authorization request shall be prepared by the RSC and submitted in accordance with the standards development process contained in this procedure.

- **Maintenance of Regional Reliability Standards Development Procedure-** This NPCC Regional Reliability Standards Development Procedure will be reviewed for possible revision at least once every five years or more frequently if needed and subject to the same procedure as that of the development of a standard. All such revisions shall be subject to approval by the NPCC Board, NERC, FERC, and could be subject to approval, if required, by applicable authorities in Canada. The NPCC RSC has the authority to make non-substantive changes to this procedure and subsequently notify the NPCC Board for their concurrence at their next scheduled meeting.

- **Interpretation of Standards-** All persons who are directly and materially affected by the NPCC's bulk power system reliability shall be permitted to request an interpretation of a standard. The person requesting an interpretation will send an email request to the Regional Standards Process Manager (RSPM), as noted on the NPCC website, explaining the specific circumstances surrounding the request and what clarifications are required as applied to those circumstances. The request should indicate the material

impact to the requesting party or others caused by the lack of clarity or a possibly incorrect interpretation of the standard. The RSPM along with guidance from the RSC will forward the request to the originating Task Force which acted as the drafting team for that regional reliability standard. The Task Force will address, through a written response, the request for clarification as soon as practical, but not more than 45 business days from its receipt by the Task Force. This written interpretation will be posted along with the final approved and adopted standard and will stand until such time as the standard is revised through the normal RSAR process, at which time the standard will be modified to incorporate the clarifications provided by the interpretation.

2. ELEMENTS OF A RELIABILITY STANDARD

- **Elements of a Regional Reliability Standard**
  To ensure uniformity of regional reliability standards, a regional reliability standard shall consist of the elements identified in this section of the procedure. These elements are intended to apply a systematic discipline in the development and revision of standards. This discipline is necessary to achieving standards that are measurable, enforceable, and consistent.

  All mandatory requirements of a regional reliability standard shall be within the standard document. Supporting documents to aid in the implementation of a standard may be referenced by the standard but are not part of the standard itself.

  The most current version of the approved NERC Reliability Standard template and its associated elements as or if applicable, will be used at the time of the development of the NPCC Regional Reliability Standard to ensure all essential elements are contained therein to achieve consistency and uniformity and meet all statutory requirements. A sample of the elements contained in the standard appears in Table 1 below, however the latest ERO Board approved Standard template, that may be found on the NERC website, will supersede the list below at the time the regional standard is developed.

Table 1- Elements of a Regional Reliability Standard

Identification Number	A unique identification number assigned in accordance with an administrative classification system to facilitate tracking and reference. (i.e. "NPCC- BAL-002-0-Date" which refers to NPCC Regional Standard, referencing NERC BAL-002 Version 0, with NPCC Effective Date-final adoption by all Regional Authorities)
Title	A brief, descriptive phrase identifying the topic of the standard.
Applicability	Clear identification of the functional classes of entities responsible for complying with the standard, noting any specific additions or exceptions. The standard will be applicable to the Bulk Power System unless otherwise noted.
Effective Date	The effective date of the standard or, prior to approval of the

and Status	standard, the proposed effective date.
Purpose	The purpose of the standard. The purpose shall explicitly state what outcome will be achieved or is expected by this standard.
Requirement(s)	Explicitly stated technical, performance, and preparedness requirements. Each requirement identifies what entity is responsible and what action is to be performed or what outcome is to be achieved. Each statement in the requirements section shall be a statement for which compliance is mandatory.
Risk Factor(s)	The potential reliability significance of each requirement, designated as a High, Medium, or Lower Risk Factor in accordance with the criteria listed below: A High Risk Factor requirement (a) is one that, if violated, could directly cause or contribute to bulk power system instability, separation, or a cascading sequence of failures, or could place the bulk power system at an unacceptable risk of instability, separation, or cascading failures; or (b) is a requirement in a planning timeframe that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk power system instability, separation, or a cascading sequence of failures, or could place the bulk power system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition. A Medium Risk Factor requirement (a) is a requirement that, if violated, could directly affect the electrical state or the capability of the bulk power system, or the ability to effectively monitor and control the bulk power system, but is unlikely to lead to bulk power system instability, separation, or cascading failures; or (b) is a requirement in a planning timeframe that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly affect the electrical state or capability of the bulk power system, or the ability to effectively monitor, control, or restore the bulk power system, but is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk power system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. A Lower Risk Factor requirement is administrative in nature and (a) is a requirement that, if violated, would not be expected to affect the electrical state or capability of the bulk power system, or the ability to effectively monitor and control the bulk power system; or (b) is a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to affect the electrical state or capability of the bulk power system, or the ability to effectively monitor, control, or restore the bulk power system.

Measure(s)	Each requirement shall be addressed by one or more measures. Measures are used to assess performance and outcomes for the purpose of determining compliance with the requirements stated above. Each measure will identify to whom the measure applies and the expected level of performance or outcomes required demonstrating compliance. Each measure shall be tangible, practical, and as objective as is practical. It is important to realize that measures are proxies to assess required performance or outcomes. Achieving the measure should be a necessary and sufficient indicator that the requirement was met. Each measure shall clearly refer to the requirement(s) to which it applies.

Table 2 — Compliance Elements of a Regional Reliability Standard

Compliance Monitoring Process	Defines for each measure: • The specific data or information that is required to measure performance or outcomes. • The entity that is responsible for providing the data or information for measuring performance or outcomes. • The process that will be used to evaluate data or information for the purpose of assessing performance or outcomes. • The entity that is responsible for evaluating data or information to assess performance or outcomes. • The time period in which performance or outcomes is measured, evaluated, and then reset. • Measurement data retention requirements and assignment of responsibility for data archiving. • Violation severity levels.

Supporting Information Elements

Interpretation	Any interpretation of regional reliability standard that is developed and approved in accordance with the "Interpretation of Standards" section of Appendix A of this procedure, to expound on the application of the standard for unusual or unique situations or to provide clarifications.
Implementation Plan	Each regional reliability standard shall have an associated implementation plan describing the effective date of the standard or effective dates if there is a phased implementation. The implementation plan may also describe the implementation of the standard in the compliance program and other considerations in the initial use of the standard, such as necessary tools, training, etc. The implementation plan must be posted for at least one public comment period and is approved as part of the ballot of the standard.

Supporting References	This section references related documents that support reasons for, or otherwise provide additional information related to the regional reliability standard. Examples include, but are not limited to: • Glossary of terms • Developmental history of the standard and prior versions • Notes pertaining to implementation or compliance • Standard references • Standard supplements • Procedures • Practices • Training references • Technical references • White papers • Internet links to related information

3. TERMS AND FUNCTIONS

- **Regional Standards Committee (RSC)**—An NPCC committee charged with management of the NPCC Standards Procedure under a sector based voting structure as described in the NPCC Bylaws. The NPCC RSC will consider requests for new or revised standards and be available for advisement to the NPCC Board on the standards.

  The RSC may not itself modify the standard without issuing a new notice to stakeholders regarding a vote of the modified standard. Any RSC action will only be activated in the event of a minor correction of a standard such as errata.

  The RSC is an open and balanced stakeholder committee inclusive of all stakeholder interests that provide for or are materially impacted by the reliability of the bulk power system.

  The RSC disposition regarding the regional standard authorization request, which will in all cases be within 60 calendar days of receipt of a completed standard request, shall include:

  - Accept the standard request as a candidate for development of a new standard, revision of an existing standard, or deletion of an existing standard. The RSC may, at its discretion, expand or narrow the scope of the standard request under consideration. The RSC shall prioritize the development of standards in relation to other proposed standards, as may be required based on the volume of requests and resources.

- Reject the standard request. If the RSC rejects a standard request, a written explanation for rejection will be delivered to the requester within 30 calendar days of the decision.
- Remand the standard request back to the requester for additional work. The standards process manager will make reasonable efforts to assist the requester in addressing the deficiencies identified by the RSC. The requester may then resubmit the modified standard request using the process above. The requester may choose to withdraw the standard request from further consideration prior to acceptance by the RSC.

The NPCC Standard Process responsibilities of the RSC will include:

- Review of NPCC Draft Standards for such factors as completeness, sufficient detail, rational result, and compatibility with existing standards; clarifying standard development issues not specified in this procedure. Under no circumstance will the RSC change the substance of a draft standard.
- Due consideration to the work of the drafting team as well as the comments of stakeholders and minority objections, in approving a proposed regional reliability standard to go to ballot.
- Approve standards for pre-ballot posting under a sector based voting structure as described later in the NPCC ~~Inc.~~ Bylaws or
- Remand the standard back to the Task Force acting as the drafting team for further work or recommend a change in those participating in the drafting team (i.e. a new drafting team).

- **Regional Standards Process Manager (RSPM) -** The Regional Reliability Standards Procedure shall be administered by a NPCC staff Regional Standards Process Manager. The RSPM is responsible for ensuring that the development and revision of standards is in accordance with this manual. The RSPM works to ensure the integrity of the process, format, consistency of quality, and completeness of the reliability standards. The RSPM facilitates all steps in the process.

- **Reliability Coordinating Committee (RCC)** —The RCC, will support the standards development process through the assignment of NPCC Task Forces. They will also provide a technical advisory role in the Regional Reliability Standards development procedure through recommendations.

- **Requester**— A Requester is any individual or an entity (organization, company, government authority, etc.) that submits a complete request for development, revision, or withdrawal of a standard. Any person or an entity that is directly and materially affected by an existing standard or the need for a new standard may submit a request for a new standard or revision to a standard. The Requester is assisted by the RSAR drafting team (if one is appointed by the RSC) to respond to comments and to decide if and when the RSAR is forwarded to the RSC with a request to draft a standard. The Requester is responsible for the RSAR, assisted by the RSAR drafting team and Regional Standards Process Manager, until such time the RSC authorizes

development of the standard. The Requester has the option at any time to allow the RSAR drafting team to assume full responsibility for the RSAR. The Requester may chose to participate in subsequent standard drafting efforts related to the RSAR.

- **Task Forces and Working Groups,**—The committees, task forces and working groups within NPCC , serve an active role in the standards process:
  - Identify the need for new or modified regional standards.
  - Initiate NPCC Standards actions by developing Regional Standard Authorization Requests (RSARs).
  - Develop comments (views and objections) to standards actions.
  - Participate in NPCC Standard drafting.
  - Provide technical oversight in response to changing industry conditions and ERO Requirements.
  - Conduct Field Tests as required

4. PROCEDURE DESCRIPTION

STEPS 1 AND 2: REQUEST TO DEVELOP A NEW REGIONAL STANDARD

Requests to develop a new Regional Reliability Standard shall be submitted to the RSPM by completing a **Regional Standard Authorization Request** (RSAR) ***(see Appendix A)***. The RSAR is a description of the new or revised standard in sufficient detail to clearly define the scope, purpose, and importance of the Regional Standard, impacted parties or other relevant information. A "needs" statement will provide the justification for the development of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard. The RSPM shall maintain the RSAR form and make it available electronically on the NPCC website.

Any person or entity ("Requester") directly or materially affected by an existing standard or the need for a new or revised standard may initiate a RSAR.

The Requester will submit the RSAR to the RSPM electronically and the RSPM will acknowledge receipt of the RSAR immediately, through electronic receipt. The RSAR, as a minimum, needs to contain the following information in order to be qualified for consideration. The NPCC RSPM will assist the Requester to ensure all the following information is submitted (on the RSAR) in a form appearing in Appendix A:

1. Proposed Title and Date of New RSAR
2. Requester's Name and Contact Information
3. Purpose of the Regional Standard
4. Description of Industry Need
5. Provide a Brief Description of the Standard
6. Identification of the Entities in the Functional Model as being responsible to adhere to the standard.
7. Necessary information to assist the drafting the team, to the extent feasible, to allow them to draft the standard.
8. A cross references to existing NPCC or NERC documents

The RSPM shall forward all properly completed RSARs to the RSC. The RSC shall meet at established intervals to review all pending RSARs. The frequency of this review process will depend on workload, but in no case shall a properly completed RSAR wait for RSC action more than 60 calendar days from the date of receipt. The RSC may take one of the following actions:

- Remand the RSAR back to the RSPM for additional work. In this case, the RSPM may request additional information or clarification for the RSAR from the Requester.
- Accept the RSAR as a candidate for a new or revised standard. In this case, the RSC will forward the RSAR to the RCC to assign a NPCC Task Force to provide technical support and analysis of comments for that RSAR, and assist the Requester and the RSPM in the remaining steps of the process. The RSPM shall post notification of intent to develop a standard on both NPCC and ERO websites within 30 calendar days of acceptance.
- Reject the RSAR. In this case, the RSC will provide a written explanation for rejection to the Requester within 30 calendar days of the rejection decision.

STEPS 3, 4, AND 5: RSC ACCEPTS RSAR AND RCC ASSIGNS TF TO DRAFT NEW OR REVISED STANDARD

A RSAR that is accepted by the RSC will be submitted to the RCC. Within 60 calendar days the RCC shall assign the development of the standard to a Task Force Drafting Team. The RSPM shall solicit and recommend a list of additional candidates for appointment to the team and shall submit the list to the RSC. This list shall include the Requester. The RSC may select other individuals to serve, with the Task Force to draft the Standard. This team shall consist of a small group of people who collectively have the necessary technical expertise and work process skills.

The RSPM shall assign NPCC staff personnel to assist in the drafting of the standard including compliance measure, process and elements. The drafting of measures and compliance administration aspects of the standard will be coordinated with the Compliance Program.

STEP 6: SOLICIT PUBLIC COMMENTS ON DRAFT STANDARD

Once a draft standard has been verified by the RSC to be within the scope and purpose of the RSAR, the RSPM will post the draft standard for the purpose of soliciting public comments. The posting of the draft standard will be linked to the RSAR for reference. In addition to the standard, an implementation plan shall be posted to provide additional details to the public and aid in their commenting and decision process. Comments on the draft standard will be accepted for a 45 calendar day period from the public notice of posting. Comments will be accepted on-line using the NPCC Open Process web-based application.

Final draft standards will be concurrently posted on the ERO website for comments.

STEPS 7, 8, AND 9: OPEN PROCESS POSTING AND ANALYSIS OF THE COMMENTS

The RSPM will assemble the comments on the new draft standard and distribute those comments to the Task Force acting as the standard drafting team. The Task Force shall give prompt consideration to the written views and comments of all participants. An effort to address all expressed comments shall be made, and each commenter shall be advised of the disposition of the comment and the reasons therefore, in addition to public posting of the responses.

The Task Force acting as the Standard Drafting Team shall take one of the following actions:

- Submit the draft standard for RCC endorsement as it stands, along with the comments received and responses to the comments. Based on the comments received, the Task Force acting as the standard drafting team may include revisions that are not substantive. A substantive change is one that directly and materially affects the application of the standard, including, for example: changing "shall" to "should," changing "should" to "shall"; adding, deleting, or revising requirements; or adding, deleting, or revising measures for which compliance is mandatory.
- Make substantive revisions to the draft standard and reposts it for further open review and comment.
- Task Force recommends Field Test if necessary to RSC.

Requester also may withdraw the request for a standard.

RCC submits proposed RRS to the RSC along with its recommendation based on comments, Task Force statements and any field test results.

STEPS 10 AND 11: RSC APPROVES OF THE NEW OR REVISED STANDARD FOR POSTING

If the RSC, acting with consideration of any recommendations by the RCC and utilizing the composite sector voting structure, as outlined in the NPCC, votes to post the draft standard for approval, the draft standard, all comments received, and the responses to those comments shall be posted electronically for the NPCC Members, by the RSPM and made public through the NPCC Website (www.npcc.org) for a 30 calendar day "pre-ballot review" and request for balloting. If the RSC decides more work is needed, the draft standard will be remanded back to the drafting Task Force. All actions of the RCC, Task Forces acting as drafting teams and the Regional Standards Committee will be recorded in regular minutes of the group(s) and posted on the NPCC website. Once the notice for a ballot has been issued, no substantive modifications may be made to the proposed standard unless the revisions are posted and a new notice of the vote is issued

STEPS 12, 13 AND 14: BALLOT OF STANDARD

Upon notification of a ballot, the Members of NPCC's registered ballot body will cast their vote consistent with the NPCC Bylaws. This ballot shall commence no sooner than 15 calendar days and no later than 30 calendar days following the notification of ballot. All members of the NPCC are eligible to participate in the voting on proposed, standard revisions or deletions of regional standards. The ballot period will typically begin immediately following the 30 calendar day pre-ballot posting and will last at least 10 business days.

The NPCC registered ballot body comprises all entities or individuals that qualify for one of the eight NPCC stakeholder sectors and are registered with NPCC as potential

ballot participants in the voting on standards. Each member of the NPCC registered ballot body is eligible to vote on standards.

In order for a NPCC Regional Standard to be approved;

- A quorum must be established by at least 50% of the NPCC Members of at least 60% of the Voting Sectors on the roster of Members maintained by NPCC.
- A two-thirds majority of the total weighted sector votes cast must be affirmative. The number of votes cast is the sum of affirmative and negative votes, excluding abstentions, and non-responses. Weighted sector vote will be calculated as follows;
  - Affirmative votes cast in each sector will be divided by the sum of affirmative and negative votes cast, in that same sector, to determine the fractional affirmative vote for each sector. Abstentions and non-responses will not be counted for the purposes of determining the fractional affirmative vote for a sector.
  - The sum of the fractional affirmative votes from all sectors divided by the number of sectors voting will be used to determine if a two-thirds majority has been achieved. (A sector will be considered as "voting" if any member of the sector in the ballot pool casts either an affirmative or a negative vote.)
  - A standard will be approved if the sum of fractional affirmative votes from all sectors divided by the number of voting sectors is at least 2/3.

Ballots will be cast electronically and alternatives are as follows;

- Affirmative
- Affirmative with Comments
- Negative
- Negative with Comments
- Abstain

The RSPM shall post the final outcome of the ballot process. If the standard is rejected, it may be withdrawn by either the RCC or the original Requester, or the standard may be remanded by the RSC back to the Task Force acting as the drafting team to address the issues. All comments submitted during the process will be posted and archived for consideration when redrafting the standard upon review.

The standard, once approved by ballot, and a recommendation will be forwarded to the NPCC Board for final Regional approval. The Board may not make substantive modifications to the standard. If the Board does not approve the standard for transmittal to NERC it will be remanded back to the RSC.

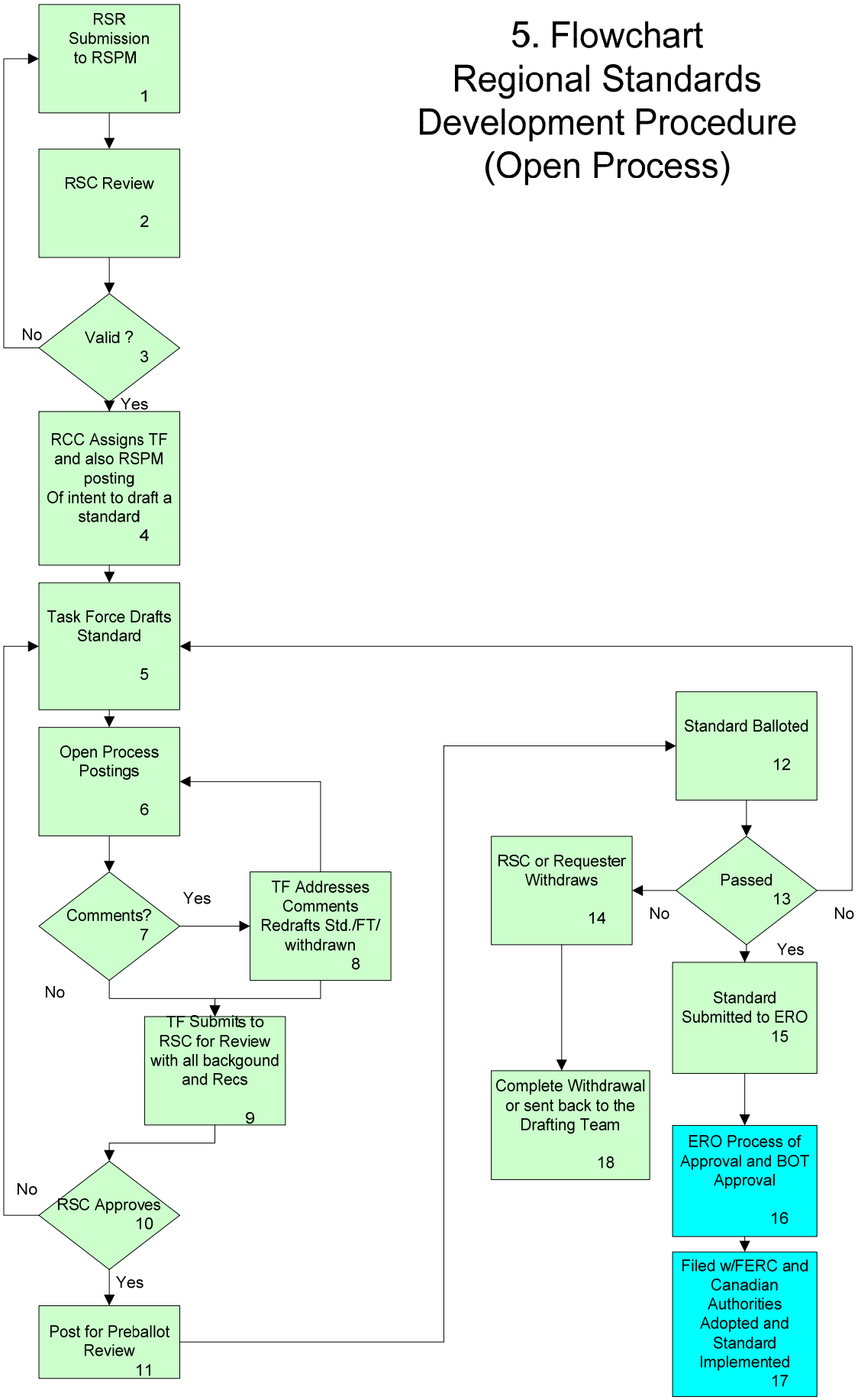
If the standard is approved, the standard will be submitted to the NERC/ERO Board of Trustees for approval.

STEPS 15, 16 AND 17: IMPLEMENTATION OF THE NPCC REGIONAL STANDARD
Upon approval within the NPCC , the standard will be submitted to the NERC/ERO for approval(s) and filing with FERC and applicable Canadian Governmental and/or Regulatory Authorities for adoption.

Once a reliability standard is adopted and made effective, all users, owners, planners, and operators of the Bulk Power System in the NPCC geographic area of the Northeast are required to comply with the standard. The NERC/ERO Board of Trustees has established a separate compliance program, also administered in the Northeast by NPCC , to measure compliance with the standards and administer sanctions as appropriate. After adoption of a NPCC Regional Standard, the standard will be forwarded to the compliance program for compliance monitoring and enforcement.

STEP 18: WITHDRAWAL OF STANDARD
Upon rejection of a proposed standard, the RCC or the requester may withdraw the standard completely or remand it back to the Task Force acting as the standard drafting team for further work.

5. Flowchart Regional Standards Development Procedure (Open Process)



6. ERO and Regulatory Process and Approvals

- **NERC/ERO Comment Period** —NERC/ERO shall publicly notice and request comment on the NPCC Regional Reliability Standard, allowing a minimum of 45 calendar days for comment on NERC's website and actively notify all adjoining Regions. Concurrent with this regional posting, final drafts will be forwarded to NERC for posting on the NERC website to ensure full industry awareness of the standard and expedite and coordinate all commenting. All comments will be responded to electronically through a posted response on the NPCC website or a link on the NERC website. NPCC shall have an opportunity to resolve any objections identified in the comments and may choose to withdraw the request, revise the NPCC Regional Reliability Standard and request another posting for comment, or submit the NPCC Regional Reliability Standard along with a response to any objections received, for approval by NERC.

- **NERC/ERO Approval of NPCC Regional Reliability Standards** — Proposed regional reliability standards shall be subject to approval by the NERC/ERO who shall have a process to evaluate and recommend whether a proposed non-Interconnection-wide NPCC Regional Reliability Standard has been developed in accordance with all applicable procedural requirements and whether NPCC has considered and addressed stakeholder objections. NPCC Board, having been notified of the results of the regional ballot concerning a NPCC Regional Reliability Standard, shall vote to submit the Standard to the NERC/ERO Board for approval as a NERC Reliability Standard. The NERC/ERO Board shall consider NPCC's request, the scope and implications of the Standard, the recommendation for action on the Standard, any unresolved stakeholder comments, and NPCC's consideration of comments and unresolved issues if any, in determining whether to approve the NPCC Regional Reliability Standard as a NERC Reliability Standard.

- **Regulatory Authority Approval** — An NPCC Regional Reliability Standard that has been approved by the NERC/ERO board shall be filed with FERC and applicable Canadian Governmental and/or Regulatory Authorities for approval and shall become effective and enforceable within the U.S., per Section 215 of the Federal Power Act, only when adopted by FERC, and within Canada, only when adopted by applicable Canadian Governmental and/or Regulatory Authorities. The regional reliability standard, once adopted will be made part of the body of NERC reliability standards and shall be mandatory and enforceable on all applicable bulk power system owners, operators, and users within the NPCC Region, regardless of membership status.

7. Appeals

- Persons who have directly and materially affected interests and who have been or will be adversely affected by any substantive or procedural action or inaction related to the development, approval, revision, reaffirmation, or withdrawal of a regional reliability standard shall have the right to appeal.

This appeals process applies only to the standards process as defined in this procedure.

The burden of proof to show adverse effect shall be on the appellant. Appeals shall be made within 30 calendar days of the date of the action purported to cause the adverse effect, except appeals for inaction, which may be made at any time. In all cases, the request for appeal must be made prior to the next step in the process.

The final decisions of any appeal shall be documented in writing and made public.

The appeals process provides two levels, with the goal of expeditiously resolving the issue to the satisfaction of the participants:

- Level 1 Appeal

Level 1 is the required first step in the appeals process. The appellant submits a complaint in writing to the RSPM that describes the substantive or procedural action or inaction associated with a reliability standard or the standards process. The appellant describes in the complaint the actual or potential adverse impact to the appellant. Assisted by any necessary staff and committee resources, the RSPM shall prepare a written response addressed to the appellant as soon as practical, but not more than 45 calendar days after receipt of the complaint. If the appellant accepts the response as a satisfactory resolution of the issue, both the complaint and response will be made a part of the public record associated with the standard and posted with the standard.

- Level 2 Appeal

If after the Level 1 Appeal the appellant remains unsatisfied with the resolution, as indicated by the appellant in writing to the regional standards process manager, the RSPM shall convene a Level 2 Appeals Panel. This panel shall consist of five members total appointed by the NPCC's board.

In all cases, Level 2 Appeals Panel members shall have no direct affiliation with the participants in the appeal.

The RSPM shall post the complaint and other relevant materials and provide at least 30 calendar days notice of the meeting of the Level 2 Appeals Panel. In addition to the appellant, any person that is directly and materially affected by the substantive or procedural action or inaction referenced in the complaint shall be heard by the panel. The panel shall not consider any expansion of the scope of the appeal that was not presented in the Level 1 Appeal. The panel may in its decision find for the appellant and remand the issue to the RSC with a statement of the issues and facts in regard to which fair and equitable action was not taken. The panel may find against the appellant with a specific statement of the facts that demonstrate fair and equitable treatment of the appellant and the appellant's objections. The panel may not, however, revise,

approve, disapprove, or adopt a reliability standard. The actions of the Level 2 Appeals Panel shall be publicly posted.

In addition to the foregoing, a procedural objection that has not been resolved may be submitted to the NPCC Board for consideration at the time the board decides whether to adopt a particular reliability standard. The objection must be in writing, signed by an officer of the objecting entity, and contain a concise statement of the relief requested and a clear demonstration of the facts that justify that relief. The objection must be filed no later than 30 calendar days after the announcement of the vote on the standard in question.

APPENDIX A

Information in a Regional Standard Authorization Request (RSAR)

The tables below identify information to be submitted in a Regional Standard Authorization Request to the NPCC Regional Standards Process Manager, NPCCstandard@npcc.org . The NPCC Regional Standards Process Manager shall be responsible for implementing and maintaining this form as needed to support the information requirements of the standards process.

Regional Standard Authorization Request Form

Title of Proposed Standard:
Request Date:

RSAR Requester Information

Name:	**RSAR Type (Check box for one of these selections.)**
Company:	☐ New Standard
Telephone:	☐ Revision to Existing Standard
Fax:	☐ Withdrawal of Existing Standard
Email:	☐ Urgent Action
Purpose (Describe the purpose of the proposed standard – what the standard will achieve in support of reliability**.)**	
Industry Need (Provide a detailed statement justifying the need for the proposed standard, along with any supporting documentation**.)**	
Brief Description (Describe the proposed standard in sufficient detail to clearly define the scope in a manner that can be easily understood by others**.)**	

Reliability Functions

The Standard will Apply to the Following Functions (Check all applicable boxes.)

☐	Reliability Coordinator	The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.
☐	Balancing Authority	The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.
☐	Interchange Authority	Authorizes valid and balanced Interchange Schedules.
☐	Planning Authority	The responsible entity that coordinates and integrates transmission facility and service plans, resource plans, and protection systems.
☐	Transmission Service Provider	The entity that administers the transmission tariff and provides Transmission Service to Transmission Customers under applicable transmission service agreements.
☐	Transmission Owner	The entity that owns and maintains transmission facilities.
☐	Transmission Operator	The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission facilities.
☐	Transmission Planner	The entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority Area.
☐	Resource Planner	The entity that develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority Area.
☐	Generator Operator	The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.
☐	Generator Owner	Entity that owns and maintains generating units.
☐	Purchasing-Selling Entity	The entity that purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. Purchasing-Selling Entities may be affiliated or unaffiliated merchants and may or may not own generating facilities.
☐	Distribution Provider	Provides and operates the "wires" between the transmission system and the customer.
☐	Load-Serving Entity	Secures energy and transmission service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check all boxes that apply.)*	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.
☐	5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.
Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*	
Recognizing that reliability is an Common Attribute of a robust North American economy:	
1. A reliability standard shall not give any market participant an unfair competitive advantage.Yes	
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes	
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes	
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes	

Detailed Description (Provide enough detail so that an independent entity familiar with the industry could draft a standard based on this description.)

Related Standards

Standard No.	**Explanation**

-t

Related SARs or RSARs

SAR ID	**Explanation**

Directory#1 Design and Operation of the BPS

TFCO and TFCP
Response to Open Process Comments
(as drafted by the CO7/CP11Working Group)

May 20th, 2014

IESO Comments	**pages 1-17.**
NYISO Comments	**pages 18-21.**
IS0-NE Comments	**pages 22-38.**
National Grid Comments	**pages 39-45.**
Dominion Comments	**page 46.**
NYSRC Comments	**page 47-55.**
TFCO Comments	**page 54-59.**
HQT Comments	**page 60-65.**

CO7/CP11 Response to Comments Received in NPCC Open Process Posting of Directory #1 Design and Operation of the Bulk Power System.

CO7/CP11 would like to thank those who provided comments on the draft of Directory #1 posted from December 11th, 2011 through January 25th, 2014.

Responses to individual comments are provided below.

Comments from - IESO:

The IESO offers the following general and specific comments for the TFCO's consideration:

General Comments:

~~*Comment: 1*~~

We support the revision to move this Directory into a Phase II structure to present criteria requirements that are clear, measurable and consistent with the NERC ERO Rules of Procedure.

However, the proposed draft document does not provide any references to indicating the mapping of specific Sections in the existing Directory 1 into the Requirements in the Phase II version.

Also, the rationale for removing and adding certain requirements/content has not been provided. It will be very helpful to present a mapping table, and insert text boxes where material changes are made to provide the rationale.

CO7/CP11 Response:
3/26/2014

Thank you for the comment.

CO7/CP11 agrees with the comment to provide mapping to the existing version of Directory#1.

The intent of the CO7/CP11 effort was to clarify the criteria and not to modify the criteria. The criteria requirements as written represent a consensus position of the CO7/CP11 Working Group.

Accordingly CO7/CP11 believes that text boxes and rationale statements are outside the scope of the CO7/CP11 assignment and specific questions on elements of the requirements should be addressed through the NPCC Open Process.

Specific Comments:

~~*Comment: 2*~~

Requirement R1:

R1 requires that each equipment owner verify the information it submits, but there is no explicit requirement on these entities so to do.

Further, the draft does not state who the recipient is. Existing Directory 1 states: “Each Registered Entity within an NPCC Reliability Coordinator Area shall provide needed information to its Reliability Coordinator as required.” It

is not obvious why this has not been captured in the draft since it could create some uncertainty.
Is the intent to rely on other Standards/Criteria to make clear these obligations (e.g. FAC-008-3 R7 and R8)? Please clarify.

If that is not the intent we suggest inserting "to its Reliability Coordinator" after "submits" and explicitly introducing a requirement for equipment owners to submit information.

CO7/CP11 Response:
2/12/2014

Thank you for the comment.

Comment accepted.

CO7/CP11 considered your comment and made revisions to Requirement R1 to improve its clarity.

CO7/CP11 also notes that the recipient of the information is described in Requirement R2.

~~*Comment:* **3**~~

Section 1.3 – Objective

The third paragraph in this Section proposes that:

"Simulation of contingency events shall be applied on bulk power system elements and the resulting performance requirements shall be monitored on the bulk power system."

We find this proposed change to the contingency criteria represents a major erosion of the NPCC basic design and operation criteria.

Previous version of this Directory and its predecessor A1 Document, did not restrict contingencies to just the bulk power system elements. Contingencies

on non-bulk power system elements that could result in material adverse effects must also be considered.

Although it is not common for contingencies on the non-bulk power system to be restrictive, it can and does happen particularly under outage conditions. The proposed revision to Directory #1 does not provide any rationale for this change. We therefore urge the responsible Task Force or Work Group to consider the following proposed changes:

Existing: *"Simulation of contingency events shall be applied on bulk power system elements and the resulting performance requirements shall be monitored on the bulk power system"*

Proposed changes:

"Performance requirements following simulated contingencies shall be satisfied on bulk power system elements."

CO7/CP11 Response:
4/29/2014

Thank you for the comment.

Comment not accepted.

The text that restricts contingencies to bulk power system elements in the CO7/CP11 draft of Directory#1 reflects the consensus view of the working group.

Fault location was discussed at length by the working group without achieving a unanimous position. After consideration the consensus view of the CO7/CP11 working group was to not accept the proposed changes.

~~*Comment:* **4**~~

Section 1.6.1

Resource Planner is included in the Applicability Section but there are no requirements that apply to the Resource Planner. Please remove it from the Applicability Section, or insert it to the appropriate requirements (e.g., R4 and/or R5).

Same comment on the Balancing Authority.

Now that Section 5.3 has been revised to become Requirement R6 with the RC being held responsible for coordinating outages and de-ratings or resources, BAs no longer have the responsibility to meet any criteria in Directory 1.

Please review and revise the Applicability Section or Requirement R6 accordingly.

CO7/CP11 Response:
2/26/2014.

Thank you for the comment.

Comment accepted.

The Functional Entity 'Resource Planner' has been added to Requirement R4.

Regarding the similar concern stated for Balancing Authority:

The term 'Each Functional Entity' in some cases is intended to apply to the Balancing Authority and therefore the BA should remain on the list of Functional entities in Section 1.6.1 of the document.

~~*Comment: 5*~~

Section 1.3

Suggest to add "Transmission Operator" after "…each Reliability Coordinator" since TOP is also held responsible for a number of requirements that address operating reliability of the BPS.

CO7/CP11 Response:
4/04/2014.

Thank you for the comment.

CO7/CP11 reviewed this comment and it led the group to review the language in the Objective section more comprehensively. The group deleted language pertaining to Functional Entities since functional responsibility is already covered in other parts of the document. Additionally, the group agreed to delete language it considered redundant and introduce language proposed in a comment by HQT.

~~*Comment: **6***~~

Requirement R2:

Similar to our comment for R1, it is not obvious who are the intended recipients of the submitted information. Please clarify.

CO7/CP11 Response:
2/26/2014.

Thank you for the comment.

Comment accepted.

CO7/CP11 agrees and has modified Requirement R2 to provide additional clarity.

~~*Comment: **7***~~

CO7/CP11 Response:
2/12/2014.

Thank you for the comment.

Comment accepted.

CO7/CO7 agrees with the comment and has inserted the word ‘is’ within the Requirement replacing ‘shall be’.

Requirement R4:

The IESO proposes to replace “… *deficiencies shall be*…” with “…*deficiencies are*…”

CO7/CP11 Response:
2/19/2014.

Thank you for the comment.

Comment accepted.

CO7/CO7 agrees with the comment and will be replace ‘shall be’ with ‘is’ in Requirement R4.

~~*Comment:* **8**~~

Requirement R5:

We propose the following editorial change to R5:

R5. Each Planning Coordinator shall evaluate and report the resource adequacy of its Planning Coordinator Area portion of the bulk power system, and obtain Reliability Coordinating Committee (RCC) approval for its Review

of Resource Adequacy. Appendix D provides guidance for the Area Review of Resource Adequacy.

Alternatively, since Requirement R4 already establishes a requirement for the Planning Coordinator to evaluate the resource adequacy of …, R5 should not duplicate that requirement. As such, the text "evaluate and" could be removed from the above proposed change.

CO7/CP11 Response:
2/26/2014.

Thank you for the comment.

Comment accepted.

The word 'evaluate' will be struck from R5 since the obligation to evaluate is already addressed in R4.

~~*Comment:* **9**~~

Requirement R6:

Please see our comment under Applicability Section 1.6.1 regarding BA's responsibility.

CO7/CP11 Response:
2/26/2014.

Thank you for the comment.

Comment not accepted.

The term 'Each Functional Entity' in some cases is intended to include the BA and therefore the BA will remain on the list of Functional Entities in Section 1.6.1 of the document.

~~*Comment: **10***~~

Requirement R11:

This requirement holds both the TP and the PC for having procedures and implementing a system design that ensures equipment capabilities are adequate for fault current levels. It also holds the PC for coordinating the procedures with procedures with adjacent Planning Coordinator Areas but it does not require such coordination for the TP.

Suggest to review what's really require of the TP, and revise the requirement accordingly since the sentence as drafted implies the TP also needs to coordinate but with adjacent Planning Coordinator Areas not the adjacent TPs.

CO7/CP11 Response:
3/05/2014.

Thank you for the comment.

Comment accepted.

The Functional Entity 'Transmission Planner" added to Requirement R11.

~~*Comment: **11***~~

Requirement R14 and Table 3:

The original Directory 1 required us to operate the power system in a manner that ensured the contingencies in Table 3 can be withstood without causing a

significant adverse effect on other reliability co-ordinator areas or the loss of a major portion of the system.

The new Directory 1 require us to meet a set of performance requirements on the entire BPS for all of the contingencies in Table 3, which we believe is far more restrictive than originally intended by Directory 1. We suggest the following changes to the Directory to return to the original intent of the directory:

a) Requirement R14 should be changed to:

"*R14. Each Reliability Coordinator and Transmission Operator shall establish limits and operate so that the contingencies specified in Table 3 shall not have a significant adverse impact on other Reliability Coordinator Areas."*

b) The following performance requirement (or the equivalent) should be added to Table 3:

"*At the transfer levels permitted by contingencies 1 to 3, if contingencies 4 to 8 can be withstood without causing significant adverse effect on other reliability co-ordinator areas, then these performance requirements apply only to contingencies 1 to 3."*

CO7/CP11 Response:
4/09/2014.

Thank you for the comment.

Comment accepted.

The CO7/CP11 has re-structured Table 3 to capture the spirit of this comment. The working group believes the structure of Table 3 (i.e. linking specific contingencies to specific performance requirements) is more likely to result in a consistent application of requirements so it has chosen this manner to address your comment.

~~*Comment: **12***~~

Requirements R15 and R16:

These requirements hold the RCs responsible for operating to respect normal and emergency conditions, but not the TOP who is also responsible for establishing normal transfer capabilities and emergency transfer capabilities, and operating their portion of the bulk power system accordingly, as stipulated in R14.

There appears to be redundant requirements between R14 and R15/R16, and if the latter two requirements are to be retained, they need to be revised to include the role of the TOP for operating under these conditions (as so reflected in R17).

CO7/CP11 Response:
3/12/2014.

Thank you for the comment.

Comment accepted.

Applicability to the Functional Entity 'TOP' has been added to requirement R14 and R15 in order to maintain consistency with the applicability of requirement R13.

Additionally, CO7/CP11 considered potential redundancy between Requirements R13, r14 and R15 and agreed to remove the word 'operate' from R13 pending further revisions to R13.

~~*Comment:* ***13***~~

Requirement R17:

R17 states that immediately after the occurrence of a contingency (within Table 3), we must prepare the system for the next contingency.

However, it is not clear whether we must prepare the system for all of the contingencies in Table 3 or just a subset of those contingencies. The original directory required us to prepare the system to withstand contingencies 1 to 3 in Table 3, within 30 minutes, following a contingency and, therefore, we suggest R17 to be changed as follows:

"R17. Each Reliability Coordinator and Transmission Operator shall assess the status of the bulk power system immediately after the occurrence of any contingency and prepare for the next contingency within the requirements for emergency transfers in Table 3."

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment not accepted.

CO7/CP11 reviewed this comment and is satisfied that the requirement as written together with the content of Table #3 is satisfactory.

~~*Comment: **14***~~

Requirement R17.1:

The IESO proposes to replace …"*shedding of firm load shall be required*…" with "*shedding of firm load shall be deployed…"*

CO7/CP11 Response:
3/19/2014

Thank you for the comment.

Comment accepted.

'Required' will be replaced with 'deployed' in R16.1.

~~*Comment: **15***~~

Requirement R18:

This requirement holds the RC responsible for notifying the applicable Reliability Coordinators of forced outages of any facility as per the NPCC Transmission Facilities Notification List and of any other condition which may impact inter-Area reliability.

We suggest to add the TOP to this requirement since forced outages of a TOP area's facility and of the system condition in a TOP area may also impact inter-Area reliability.

Holding the RC alone responsible to the notification task delays the process, and can expose to reliability gap if a TOP is not held accountable for the notification task involving the facilities/conditions in its area.

CO7/CP11 Response:
3/19/2014

Thank you for the comment.

Comment not accepted.

CO7/CP11 considered this comment and noted that including the TOP as a functional entity applicable to the requirement would result in a preponderance of notifications to the RC and that the language of the requirement as written was sufficient.

~~*Comment:* **16**~~

Requirement R19:

This requirement holds the RC responsible for coordinating scheduled outages of facilities that are on the NPCC Transmission Facilities Notification List sufficiently in advance of the outage.

This responsible was assigned to the responsible entities which included the TOPs in the existing Directory #1. The switch of responsibility to the RC will relieve the TOPs from having to coordinate this task, which can leave a reliability gap.

We believe the RC has a high-level oversight role to ensure facility outage schedules are coordinated, but the act of coordination needs to be performed by the TOPs themselves. We suggest to add or replace RCs with TOPs for this requirement.

In addition, the IESO found "*sufficiently in advance*" is not specific enough. We suggest that the Task Force or Work Group specify what "sufficiently in advance" means.

CO7/CP11 Response:
3/19/2014

Thank you for the comment.

Comment not accepted.

CO7/CP11 has reviewed the comment and did not accept the comment to include the TOP as part of the functional applicability of R18 and to clarify 'sufficiently in advance' in the language of R18.

The group noted that Section 5.5 of the current Directory#1 holds the R.C. responsible for coordinating such outages and noted that the R.C. was the appropriate functional entity to provide such coordination.

The group also acknowledged that the comment to improve the term 'sufficiently in advance' was a valid concern.

However, CO7/CP11 noted that it had spent considerable time discussing this issue during its first review of the draft and could not improve on the term because of a variety of reasons which include different internal procedures and scheduling constraints.

The group considered removing the subject term completely from the requirement in order to address the comment, however CO7/CP11 agreed that term was useful in the context of the requirement as written.

~~*Comment:* **17**~~

Requirement R20:

This requirement holds the RC responsible for coordinating voltage control between TOP Areas. This responsible was assigned to the responsible entities which include the TOPs in the existing Directory #1. The switch of

responsibility to the RC will relieve the TOPs from having to coordinate this task, which can leave a reliability gap.

Further, the RC does not own or operate any TOP meters; this renders the RCs unable to meet Requirement R20.1.

Suggest to add or replace RCs with TOPs for this requirement.

Also, Appendix G stipulates that the TOPs are to following the voltage control and coordination procedures.

We suggest the drafting team (WG/TF) to review the role of TOP in coordination of voltage control and schedule.

CO7/CP11 Response:
3/19/2014

Thank you for the comment.

Comment not accepted.

CO7/CP11 has reviewed the comment and did not accept the comment to include the TOP as part of the functional applicability of R19.

The group noted that although the TOP has a role in voltage control in accordance with Appendix G, the RC is the appropriate functional entity to coordinate wide area voltage control and the language of the requirement as written was sufficient.

~~*Comment:* ***18***~~

Tables 1, 2 and 3:

The subtitle "*Compliance with Directory#1 shall be demonstrated for all requirements listed in the table below that are not required for compliance with the NERC Reliability Standards"* sends the message that NPCC does not require compliance with all requirements.

If the intention was to avoid duplication of sanctions from NERC and NPCC for the same violation, that should be clarified in a different place.

CO7/CP11 Response:
4/24/2014

Comment accepted.

CO7/CP11 agrees with the comment and has deleted the subject compliance statement from Tables #1 and #3 and further recommended that this statement be captured in the Compliance section of the document.

CO7/CP11 developed Tables#1 and#3 which organize requirements that are applicable to NPCC BPS elements and compliance with the performance requirements in the Tables shall be demonstrated for those elements.

Certain requirements presented in the Tables are duplicative with NERC requirements, however since the BES and BPS may comprise a different set of elements CO7/CP11 included all requirements that are applicable to the BPS.

Comments from – NYISO:

The New York Independent System Operator (NYISO) respectively submits comments on the subject draft Directory 1 revision which was posted on December 11, 2013 for review and comment.

The NYISO generally supports the posted version of Directory 1, and submits the following comments for consideration:

~~*Comment:* ***19***~~

The NYISO concurs with the following comment by the New York State Reliability Council (NYSRC):

"A new sentence has been added to the Resource Adequacy Criterion Requirement R4.1 in this Directory 1 draft as follows: "In the calculation of available resources, supply-side purchases from neighboring systems are limited to firm capacity backed purchases."

We understand that this sentence was taken from an earlier version of the Introduction of Appendix D – Guidelines for Area Review of Resource Adequacy.

The paragraph from which this sentence was taken describes types of supply and demand-side facilities that contribute to resource capacity. There is no indication as to why this particular type of supply-side measure was singled out for inclusion in R4.1 when many other important types of supply-side and demand-side components included in resource adequacy reviews were not also incorporated in the Resource Adequacy Criterion draft revision.

Notwithstanding this, the NYSRC maintains that the Guidelines for Area Review of Resource Adequacy – not the reliability criterion – continues to be the appropriate document for describing requirements for all load and capacity models and assumptions that are incorporated in Area resource adequacy assessments.

We recommend that Appendix D be restored to its 12/1/2009 version since it has not been demonstrated that the above referenced information is no longer required for preparing Area resource adequacy assessments.

CO7/CP11 Response:
2/19/2014

Thank you for the comment.

Comment accepted.

CO7/CP11 agrees with the comment and will transfer the language on supply side purchases that was moved to Requirement R4.1 back to Appendix D *Guidelines for Area Review of Resource Adequacy*.

~~*Comment:* **20**~~

The NYISO concurs with the following comment by the NYSRC:

Requirement R8 requires that credible combinations of certain specified system conditions that stress the system be modeled.

However, R8 does not specify the objective or use of this modeling requirement, e.g., whether it is intended by R8 that the system shall be designed to meet such combinations of system conditions.

CO7/CP11 Response:
3/5/2014.

Thank you for the comment.

Comment accepted.

CO7/CP11 agrees with the comment and has renamed R8 to R7.1 in order to link the objective of these studies to the planning obligations in Table 1.

~~*Comment: **21***~~

Requirement R6.1 states,

"*Perform a summer and winter reliability assessment every year*."

This does not provide enough clarity as to what NPCC Task Force or Working Group is responsible for the performance and review of this assessment.

Is each Reliability Coordinator individually responsible for this requirement? Is CO-12 responsible? Is CP-8 responsible?
This requirement should be revised to provide appropriate clarity both in terms of performance responsibility and review responsibility, and/or reference an appendix which would provide guidance.

CO7/CP11 Response:
3/12/2014.

Thank you for the comment.

Comment accepted.

Since Requirement R6.1 is a sub requirement of R6 the applicability of the parent requirement R6 also applies to R6.1.

In this case the functional entity responsible for R6.1 is the Reliability Coordinator.

Additionally CO7/CP11 has revised requirement R6.1 to improve its clarity.

~~*Comment:* **22**~~

In Appendix D, the title of 3.6 is misleading and inconsistent with the content. The title should be revised to "*Potential Reliability Impacts and Mitigation Mechanisms"*.

CO7/CP11 Response:
4/09/2014.

Thank you for the comment.

Comment accepted.

Appendix D *Guidelines for Area Review of Resource Adequacy* Section 3.6 and 3.7 language reordered.

Comments from – ISO-NE:

ISO New England has the following comments on the posted version of Directory 1, listed as DRAFT 14: December 11th, 2013:

~~*Comment: **23***~~

Page 3:

Delete the period after "Appendix A – Reserved for Future Use"

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

Period deleted after 'Appendix A-Reserved for Future Use".

~~*Comment: **24***~~

There appears to be inconsistent use of bolding when using the term "bulk power system". These comments attempted to catch each instance, but the entire document should be reviewed for consistency.

CO7/CP11 Response:
3/25/2014.
Thank you for the comment.

Comment accepted.

Entire document reviewed to insure the term “bulk power system’ is bolded consistently throughout.

~~*Comment :* ***25***~~

Page 5, Section 1.3:

4th paragraph, last line, “bulk” should be bold.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

“Bulk” bolded. (Page 5, Section 1.3, 4th paragraph, last line.)

~~*Comment :* ***26***~~

Page 5, Section 1.4:

The effective date will need to be updated once this document is finalized.

CO7/CP11 Response:
3/25/2014

Thank you for the comment.

Comment accepted.

The effective date of this document will remain as indicated in the Table of Contents as December 1, 2009 reflecting the date that Directory#1 initially became effective as balloted by the NPCC Full Members.

However, the 'Revision Review Record' on the title page along with the "Revision History" page will be updated to reflect the date that this version of the document becomes effective.

~~*Comment : 27*~~

Page 6, Section 1.6.2:

Delete "NPCC transmission" from the first line of the first paragraph. This should be redundant with "NPCC bulk power system elements" used in the next line and may cause users to ignore criteria on BPS facilities that they do not consider transmission.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

"NPCC transmission" has been deleted from the first line of the paragraph.

~~*Comment:* **28**~~

Page 7, title of Section 3:

Delete “More Stringent Criteria”. This is unnecessary.

CO7/CP11 Response:
2/12/2014.

Thank you for the comment.

Comment accepted.

Removed ‘More Stringent’ from title of 3.0

~~*Comment:* **29**~~

Page 8, last line of R7:

Delete “NPCC” from “NPCC bulk power system”. BPS is an NPCC defined term and adding NPCC adds unnecessary confusion.

CO7/CP11 Response:
3/5/2014.

Thank you for the comment.

Comment accepted.

Deleted “NPCC” from “NPCC bulk power system”

~~*Comment: **30***~~

Page 8, last two lines of R11:

….. state "*and coordinate these procedures with adjacent Planning Coordinator Areas"*. This language is overly burdensome. If there is a written procedure in the corner of a system that cannot possibly impact neighbors, this should be unnecessary. Suggest "*and coordinate these procedures with affected Planning Coordinator Areas"*.

CO7/CP11 Response:
3/5/2014.

Thank you for the comment.
Comment accepted.

Deleted "adjacent" and replaced it with "materially affected" in the last sentence of R11.

~~*Comment: **31***~~

Page 9, first line of R12.3:

Delete NPCC from before bulk power system, similar to our comment 5.

CO7/CP11 Response:
3/5/2014.

Thank you for the comment.
Comment accepted.

Deleted "NPCC" from "NPCC bulk power system"

~~*Comment : **32***~~

Page 9, R13.2:

Should be unnecessary as Directory 7 should require this.

CO7/CP11 Response:
3/12/2014.

Thank you for the comment.

CO7/CP11 agrees with the comment and has deleted the Requirement since it is redundant with NPCC Directory #7.

~~*Comment: **33***~~

Page 9, R14:

Last line states that system conditions are described in Table 3 and they are not present. Suggest deleting “and system conditions” from R14.

CO7/CP11 Response:
3/25/2014

Comment accepted.

Deleted the term ‘system conditions’.

~~*Comment :* **34**~~

Page 9, R16:

Last line, “emergency” should be bold.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

“Emergency” bolded in R16.

~~*Comment:* **35**~~

Page 9, R17:

Suggest adding “*specified in Table 3*” to the end of R17 so that it reads “…after the occurrence of any contingency and prepare for the next contingency specified in Table 3.” The current wording suggests that after the occurrence of the first contingency, the operator must posture the system to be ready for ANY next contingency, including ECs. Adding the suggested language limits the contingencies to those located in Table 3.

CO7/CP11 Response:
3/25/2014.

Comment accepted.

‘as specified in Table #3’ added to the language of R16.

~~*Comment: **36***~~

Table 1, Performance Requirement vi:

The evaluation of reclosing is limited to automatic. Should manual reclosing also be included here?

If so, the word "automatic" could be deleted or it could be modified to read "…with due regard to successful and unsuccessful automatic and manual reclosing, where automatic reclosing does not exist."

CO7/CP11 Response:
3/26/2014

Comment accepted.

CO7/CP11 agreed to delete the word 'automatic' when describing reclosing operations both in Table #1 Performance Requirement vi and Table#3 Performance Requirement vii.

~~*Comment: **37***~~

Table 2:

There is a note at the top that reads *"Compliance with Directory#1 shall be demonstrated for all requirements listed in the table below that are not required for compliance with the NERC Reliability Standards."*

This should be deleted. Unlike the design criteria specified in Table 1, there are no requirements listed in Table 2.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

Deleted the subject note in Table#2. (Table #2 provides assessment criteria and not performance requirements.)

~~*Comment: **38***~~

Table 2:

Fault description corresponding to item 4, the font appears to change size throughout the description.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

Font size adjusted.

~~*Comment:* **39**~~

Table 2, contingency 7:

Uses the term “Council”. Suggest replacing this with “NPCC” to avoid confusion.

CO7/CP11 Response:
3/25/2014.

Comment accepted.

The term ‘Council” has been replaced by ‘NPCC” in Table #2 contingency#7.

~~*Comment:* **40**~~

Table 3, in the column listed as “Normal Transfer Capability”:

Delete the periods from “i to xi.” They are inconsistent with the convention used throughout the tables.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

Periods after “i to xi” deleted in Table #3 in the column under ‘Normal Transfer Capability”.

~~*Comment:* ***41***~~

Table 3, performance requirement xi and the note underneath:

Bulk power system should be bold.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

"Bulk Power System" bolded in Table #3 performance requirement 'xi' and in the note at the bottom of Table#3.

~~*Comment:* ***42***~~

Table 3, performance requirement xi.

While members of CP-11 and CO-7 participated in the discussion of the wording of requirement, the subtlety of what is means is not understood by those who did not participate.

The language relies on the nuance introduced by the fact that the description is for an element that remains faulted and also provides no description on what is permissible if a fault has been removed.

Suggested wording: *"Normal transfer levels shall not require system adjustments before attempting manual reclosing of elements to maintain stability of the BPS unless specific instructions describing alternate actions are in effect."*

CO7/CP11 Response:
3/26/2014.

Comment accepted.

CO7/CP11 reviewed this comment and agreed to revise Table #3 Performance Requirement xi to further clarify the conditions under which manual reclosing is permissible.(removed the reference to faulted elements).

~~*Comment:* **43**~~

Table 3, performance requirement xii:

Suggest changes similar to those suggested in comment 21. Replace wording with:

> *"Emergency transfer levels may require system adjustments before attempting manual reclosing of elements to maintain stability of the bulk power system. "*

CO7/CP11 Response:
3/26/2014.

Comment accepted.

CO7/CP11 reviewed this comment and agreed to revise Table #3 Performance Requirement xii to further clarify the conditions under which manual reclosing is permissible.(removed the reference to faulted elements).

~~*Comment:* ***44***~~

While the Table of Contents lists Appendix A as “Reserved for Future Use”, there is no placeholder in the document itself. The document transitions right into Appendix B. It would be clearer if a page was inserted for Appendix A that that noted it was “Reserved for Future Use”.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.
Comment accepted.
A placeholder page will be added for Appendix A.

~~*Comment:* ***45***~~

Appendix B, Section 1.0, fifth line:

Uses the term “bulk power transmission system”. It is unclear if this is something different than the BPS. Suggest deleting the word “transmission” and making the remaining “bulk power system” bold.

CO7/CP11 Response:
4/04/2014.

Thank you for the comment.

Comment accepted. The word ‘transmission’ has been deleted and the remaining term ‘bulk power system’ has been bolded in Appendix b, Section 1.0, 5th line.

~~*Comment:* **46**~~

Appendix B, Section 1.0, sixth line:

Says that the periodic reviews encompass the BPS "*and the transmission interconnections to other Planning Coordinator Areas"*.

This indicates that this applies to interconnections to other Planning Coordinator Areas, even if they are none BPS. Suggest striking this language.

CO7/CP11 Response:
4/24/2014

Thank you for the comment.

Comment accepted.

Subject language deleted.

~~*Comment:* **47**~~

Appendix B, last paragraph of Section 4.0, first line:

Suggest capitalizing "coordinator".

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

'Coordinator" has been capitalized.

~~*Comment :* **48**~~

Appendix B, Section 5.0, part d:

States: "*Plots of angles versus time for significant machines, HVdc and SVC response, voltages at…*"

The use of the term SVC is too specific. It rules out other FACTS devices such as STATCOMs. Suggest using a more generic term so that all types of equipment of interest are included.

CO7/CP11 Response:
4/04/2014.

Thank you for the comment.

Comment accepted.

CO7/CP11 has revised the language in Appendix B, Section 5.0 part d to address the comment.

~~*Comment:* **49**~~
Appendix E, Section 3,

Should require that the exclusion is approved by the RCC.

As currently written Section 3 ends with finding the position of each Task Force with no step for final approval.

Additionally, Table 1, Performance Requirement vii states that the RCC must accept each request for exclusion. Adding a step for the RCC approval to Appendix E, Section 3 would address these concerns.

CO7/CP11 Response:
4/16/2014.

Thank you for the comment.

Comment accepted.

CO7/CP11 has revised Appendix E *Guidelines for Requesting Exclusions to Simultaneous Loss of Two Adjacent Transmission Circuits on a Multiple Circuit Tower* to include language that provides for RCC approval of such exclusions.

~~*Comment:* ***50***~~

Appendix G, Section 3.1.a:

Suggest deleting the period at the end after “between the reporting Reliability Coordinator and Adjacent Reliability Coordinators.”

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

Period deleted.

Comments from – National Grid):

Subject: Open Process Posting of NPCC Directory # 1 Design and Operation of the Bulk Power System.

~~*Comment:* ***51***~~

National Grid is very concerned with the change proposed in Directory 1 specific to footnote vii of Table 1.

The proposed change from the existing Directory 1 is to change the phrase *"...that involve a fault…*" to "*...that involve normal fault clearing...*"

While this seems a simple change, we are concerned that it could adversely impact protection system design as well as bulk power system stability.

The footnote is the new directory's method of addressing the issue of ensuring that stability is maintained whether fault clearing is maintained by system A protection group or system B protection group.

The present directory handles this in the introductory paragraphs of sections 5.4.1 and 5.5.1.

The footnote mechanism itself is not the issue of concern.

Rather, it is the action of the footnote to restrict application of the stability testing under either protection group clearing to only cases with normal fault clearing.

The result of the change is to eliminate the need to perform this step for the former fault "c." / now Event number 4 - a *"permanent phase to ground fault on any transmission circuit, transformer, or bus section with delayed fault clearing"*.

The concern that prompts a need and desire to ensure acceptable stability performance under fault clearing (either normal or delayed) by either

protection group is that the two NPCC required groups may not necessarily have the same speed of operation.

One might clear in "high speed" while the other may use a stepped distance design which would take longer.

The test of simulating fault clearing with either group and ensuring acceptable performance in each case confirms that the two protection groups provided are capable of performing the specified protective function and thus meet the NPCC Protection Criteria.

The proposal to limit such testing to only faults involving normal clearing may stem from a perception that delayed fault clearing implies a failure in one protection group already.

This is not correct.

Delayed fault clearing results from a mechanical failure which causes the breaker to not operate within its expected time. This situation is not a result of any system contingency. It is a condition which could occur quite some time prior to the system fault and persist undetected, only coming to light when the breaker is called upon to operate as a result of the fault.

And during that event one or the other protection group could suffer a failure.

NPCC criteria provide redundancy for the mechanical portion of the breaker (operating mechanism and contacts) through the breaker failure scheme, which is a separate protection group associated with the breaker. It is not part of the System A or System B protection group of an element.

But it is initiated by each of the protection groups which trip the breaker.

Thus, whether normal fault clearing or delayed fault clearing, there could be a difference in operating time due to differences between System A and System B protection groups.

Ensuring that protection groups will deliver their expected performance is important under all fault types - not just those involving normal clearing.

We believe that the footnote needs to retain the present text of "*for each of the contingencies that involve a fault, stability shall be maintained…*" in order to continue to protect NPCC bulk power system reliability.

CO7/CP11 Response:
5/20/2014

Thank you for the comment.

Comment accepted.

CO7/CP11 did not reach consensus on this issue.

Some CO7/CP11 Members agreed that the existing NPCC criteria requires the testing of certain faults with the slower of either protection system A or protection system B and that the proposed change would impact reliability by weakening the criteria.

Conversely other CO7/CP11Members contended that the change was necessary in order to properly clarify the criteria in order to avoid an overly conservative interpretation.

Ultimately, the TFCP directed that the criteria should remain as currently written and that notwithstanding the dissenting opinion the subject change to the criteria should be eliminated.

~~*Comment:* **52**~~

Table#1:

We believe appropriate limits should be specified in footnote iii. similar to footnote iv. E.g. Voltages and loadings shall be within applicable normal limits for pre-contingency conditions.

CO7/CP11 Response:
3/26/2014.

Comment accepted.

CO7/CP11 reviewed this comment and agreed to move the word ’applicable’ in front of the word ‘limits’ in Table 1 Performance Requirement iii and Table#3 Performance Requirement iv in order to improve clarity.

~~*Comment:* ***53***~~

Table#1:

Why is Event 3 (Loss of single pole of direct current facility) and Event 7 (Simultaneous permanent loss of both poles of a direct current bipolar facility) listed separately when both are functionally equivalent depending on the design of the dc facility?

This is an "or" not an "and". Wouldn't the requirements as stated require the owner of an HVdc bipolar facility to do unnecessary studies to demonstrate compliance?

CO7/CP11 Response:
3/25/2014

Thank you for the Comment.

Comment not accepted.

CP11/CO7 reviewed this comment and concluded that Contingency Event # 3 should remain in both Table#1 and Table #3 for the following reasons:

Regarding the Planning Table (Table#1) CP11/CO7 suggests maintaining the parallel structure with Table 3 including Contingency Event #3.

Additionally, it is understood that if a system has a bipolar dc facility and testing for Contingency Event #7 has been performed it is not necessary to perform the testing for Contingency Event #3(loss of a single pole).

Also, in Table#1 if a system has a mono-polar dc facility, Contingency Event #7 would not be applicable; however the loss of this mono-polar facility would be tested under Contingency Event #3 thereby justifying its presence in the table.

Finally, regarding the Operations Table (Table#3) all losses of a single element should be included to establish emergency transfer capability. Therefore, loss of a single pole DC current facility (bi-polar) was included with Contingency events #1 and #2 for emergency transfer capability.

~~*Comment:* **54**~~

Table#1:

The wording of Event 8.f. might negate itself (8… after the loss of the following…f. opening of any circuit breaker).

Taken together this says to simulate the loss of the opening of a circuit breaker, but that isn't what is meant.

Event 8.f. also contradicts itself when considering the fault type (opening of any breaker without a fault during a phase-to-ground fault).

Unless what is meant is a pullout of a remote breaker for a fault.

It is unlikely that an SPS would have been put in for that. It seems Event 8f would be better described in its own Event line - similar to Event 2.

CO7/CP11 Response:
3/26/2014

Comment accepted.

A new event line has been established in Table#1.

8f transferred to new contingency event #9….'the failure of a CB to operate when initiated by a SPS after opening of any C.B.'….

Fault Type: No Fault.

~~*Comment:* ***55***~~

Table#2:

Considering that most EHV and a good many HV circuit breakers have each pole in a separate tank (not to mention live-tank breakers), how is Event 5. (Loss of a circuit breaker due to a three-phase internal fault) relevant?

Does it not impose an undue burden for an unrealizable condition?

CO7/CP11 Response:
3/26/2014.

Thank you for the comment.

The word 'internal' has been deleted from Tables 1, 2 and 3 to eliminate ambiguity.

Furthermore CO7/CP11 notes that the intention is to address the zone of protection for the circuit breaker.

~~*Comment: **56***~~

The previous version of Directory 1 contained definition of terms in Appendix A. This proposed version has Appendix A reserved for future use. Where are the defined terms?

Have they all been incorporated into the NPCC Glossary?

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.
Comment accepted.

NPCC has established a Glossary of Terms to replace the A-7 document and the separate section within each Directory has been retired; all NPCC defined terms reside in the Glossary of Terms.

~~*Comment: **57***~~

Section 1.4:

States the Effective Date is December 1, 2009. This will need to change to reflect lead time for completion of open process and member acceptance voting.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

The effective date of this document will remain as indicated in the Table of Contents as December 1, 2009 reflecting the date that Directory#1 initially became effective as balloted by the NPCC Full Members.

However, the 'Revision Review Record' on the title page along with the "Revision History" page will be updated to reflect the date that this version of the document becomes effective.

Comments from – Dominion:

Comment#1:

~~*Comment:* ***58***~~

Section 1.6.2 (Applicability of NPCC Criteria):

Contains new "boiler plate" language in the second paragraph requested by the TFCO to addresses the applicability of the NPCC criteria. To be consistent with the NPCC Bylaws (Article IV, 4.2, (2)), Dominion suggest a modification to the last sentence as follows:

NPCC will not enforce compliance to the NPCC Directory requirements in this document on any entity that is not an NPCC Full Member.

CO7/CP11 Response:
4/04/2014.

Thank you for the comment.

Comment accepted. CO7/CP11 has incorporated the suggested language into the document.

Comments from – New York State Reliability Council (NYSRC):

The New York State Reliability Council (NYSRC) respectively submits comments on the subject draft Directory 1 revision which was posted on December 11, 2013 for review and comment.

The NYSRC generally supports the posted version of Directory 1, and submits the following comments for consideration:

General Comment:

~~*Comment:* **59**~~

Our review of the Directory 1 draft would have been made easier if a redline version had been made available along with a clean version. Changes were not only made in the reliability criteria section of the Directory, but also in its many appendices. Comparing this 50-page draft with the most recently posted December 1, 2009 version was very difficult without having a redline version

available. We strongly suggest that the next Directory 1 draft include a redline version.

CO7/CP11 Response:
3/26/2014.

Thank you for the comment.

Comment accepted.

CO7/CP11 notes that the draft of Directory#1 has undergone significant structural changes that would render a redlined to the current version unusable.

However, a red-line to the most recent posted draft of the document will be provided for subsequent postings.

Additionally, CO7/CP11 will also provide mapping to the existing version of Directory#1.

Specific Comments:

~~*Comment:* **60**~~

The NPCC Directory Development and Revision Manual indicates in its Introduction that each directory identifies NERC ERO Standards that are associated with the directory. This Directory 1 draft does not include such a list of associated NERC Standards.

We also note that other NPCC directories include a lead in sentence to the criteria, such as: “These criteria are in addition to, more stringent than, and more specific than NERC or any Regional reliability standard requirements.”

We suggest a similar sentence be included in Directory 1.

CO7/CP11 Response:
3/26/2014

Thank you for your comment.
Comment not accepted.

CO7/CP11 has reviewed this comment and determined that the list of ERO standards should no longer appear in the Directory for the following reasons:

- Regulatory approval and version control can lead to different versions of the ERO Standards in effect within US and Canadian provinces.
- BPS and BES represent different equipment.

CO7/CP11 recommends revising the subject section of the Directory Manual to eliminate the section on ERO standards and also recommends removing the subject list of ERO standards from all other Directories.

Additionally, CO7/CP11 recommends omitting the language surrounding the more stringent criteria and regional standards and also recommends removing this language from all other Directories since this language may no longer be accurate given that the NERC standards are evolving beyond the criteria.

~~*Comment:* ***61***~~

Directory 1 is clear in Section 1.6.2 that it applies to NPCC BPS elements that are defined by NPCC A-10 tests where the criterion is potential significant adverse impact outside of the Local Area.

NPCC's Glossary of Terms defines Local Area as, "An electrically confined or radial portion of the system. The geographic size and number of system elements contained will vary based on system characteristics. A local area may be relatively large geographically with relatively few buses in a sparse system, or be relatively small geographically with a relatively large number of buses in a densely networked system."

This definition is vague and ambiguous. It can lead to widely varied lists of

BPS elements with a range of economic impacts.

Also, A-10 is based upon Security performance and does not address Adequacy performance.

Please clarify with respect to Directory 1.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

CO7/CP11 has reviewed your comment and found that the definition of local area is beyond the scope of the CO7/CP11 assignment which was to reformat the Directory#1 criteria into auditable requirements.

CP7/CP11 recommends that the appropriate forum for the review of this definition is a review of the NPCC A10 methodology and the NPCC Glossary of Terms.

Directory#1 Requirements R4 – R6 address resource adequacy which utilize system transfer security criteria.

~~*Comment Type: P.*~~ ~~***62***~~

A new sentence has been added to the Resource Adequacy Criterion Requirement R4.1 in this Directory 1 draft as follows: *"In the calculation of available resources, supply-side purchases from neighboring systems are limited to firm capacity backed purchases."*

We understand that this sentence was taken from an earlier version of the Introduction of Appendix D – Guidelines for Area Review of Resource Adequacy.

The paragraph from which this sentence was taken describes types of supply and demand-side facilities that contribute to resource capacity. There is no indication as to why this particular type of supply-side measure was singled out for inclusion in R4.1 when many other important types of supply-side and demand-side components included in resource adequacy reviews were not also incorporated in the Resource Adequacy Criterion draft revision.

Notwithstanding this, the NYSRC maintains that the Guidelines for Area Review of Resource Adequacy – not the reliability criterion – continues to be the appropriate document for describing requirements for all load and capacity models and assumptions that are incorporated in Area resource adequacy assessments.

We recommend that Appendix D be restored to its 12/1/2009 version since it has not been demonstrated that the above referenced information is no longer required for preparing Area resource adequacy assessments.

CO7/CP11 Response:
2/19/2014.

Thank you for the comment.

CO7/CP11 agrees with the comment and will transfer the language on supply side purchases that was moved to Requirement R4.1 back to Appendix D *Guidelines for Area Review of Resource Adequacy.*

~~*Comment: **63***~~

Requirement R8 requires that credible combinations of certain specified system conditions that stress the system be modeled. However, R8 does not specify the objective or use of this modeling requirement, e.g., whether it is intended by R8 that the system shall be designed to meet such combinations of system conditions.

CO7/CP11 Response:
3/5/2014.

Thank you for the comment.

Comment accepted.

CO7/CP11 agrees with the comment and has renamed R8 to R7.1 in order to link the objective of these studies to the planning obligations in Table 1.

~~*Comment: **64***~~

The following note appears in Tables 1-3: "*Compliance with Directory #1 shall be demonstrated for all requirements listed in the table below that are not required for compliance with the NERC Reliability Standards.*"

This note suggests that some requirements in these tables are NERC Standard requirements.

Without specifying which requirements in these tables are associated with NERC Standards, how can compliance with Directory 1 be demonstrated?

CO7/CP11 Response:
4/24/2014

Thank you for the comment.

CO7/CP11 agrees with the comment and has deleted the subject compliance statement from Tables #1 and #3 and further recommended that this statement be captured in the Compliance section of the document.

CO7/CP11 developed Tables#1 and#3 which organize requirements that are applicable to NPCC BPS elements and compliance with the performance requirements in the Tables shall be demonstrated for those elements.

Certain requirements presented in the Tables are duplicative with NERC requirements, however since the BES and BPS may comprise of different elements CO7/CP11 included all requirements that are applicable to the BPS.

~~*Comment:* **65**~~

Documented in the Final Meeting Minutes of the 10/17-18/2013 NPCC TFCO meeting, a bullet item on page 5 of the minute's states:

- *Station service supply (non-NPCC BPS) is viewed as loss of a transformer (NPCC BPS) so that by extension Directory #1 covers some non-NPCC BPS facilities that impact the NPCC BPS. The intention is to cover loss of the station service transformer consistently throughout NPCC.*

The latest Directory 1 draft, however, makes no reference to station service transformers or any other station service supply equipment.

If station service transformers are expected to be treated as NPCC BPS elements and, therefore, required to comply with NPCC Directory Criteria, this requirement should be clearly delineated.

Without delineation, treatment of station service supply for NPCC BPS facilities will (1) not be addressed in a consistent fashion, (2) create a potential reliability gap and (3) result in a potential compliance issue for industry entities.

CO7/CP11 Response:
3/26/2014.

Thank you for the comment.

CO7/CP11 has reviewed your comment and found that the delineation between BPS and non BPS facilities is beyond the scope of the CO7/CP11 assignment which was to reformat the Directory#1 criteria into auditable requirements.

CP7/CP11 recommends that the appropriate forum for BPS and non BPS facilities is a review of the NPCC A10 methodology and the NPCC Glossary of Terms.

Comments from – TFCO (via NPCC Staff):

Appendix F-Procedure for Operational Planning Coordination

~~*Comment :* ***66***~~

Appendix F section 2.1:

Insert ‘during the’ …….delete ‘in advance of’.

Insert ‘and documented in the summer and winter NPCC Reliability Assessment reports.

CO7/CP11 Response:
4/09/2014.

Thank you for the comment.

Comment accepted.

Appendix F Section 2.1 language revised.

~~*Comment:* ***67***~~

Appendix F section 5.1:

Insert ‘and as necessary adjacent RC Areas’

Insert: ‘addressed’……. delete ‘discussed’.

CO7/CP11 Response:
4/09/2014.

Thank you for the comment.

Comment accepted.

Appendix F Section 5.1 language revised.

~~*Comment:* ***68***~~

Appendix F Attachment A:

Insert ’Independent Power Producers Line Item 2’.

Insert: ‘Any entity that owns or operates an electricity generating facility that is not included in an electric utility's rate base. This term includes, but is not limited to, co generators and small power producers and all other nonutility electricity producers, such as exempt wholesale generators, who sell electricity.’

CO7/CP11 Response:
4/09/2014.

Thank you for the comment.

Comment accepted.

Additional Line item inserted and renamed as ‘Other Generation Capacity’.

~~*Comment:* ***69***~~

Reorder line Items #2 through #18.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

Items #2 through #18 reordered.

~~*Comment:* ***70***~~

Net Capacity:

Insert: ‘Line3’…reorder Line 3 to Line 4.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

Line#3 and Line #4 reordered.

~~*Comment:* ***71***~~

Peak Load Forecast:

Insert: ‘along with the day during which the peak is expected to occur’

CO7/CP11 Response:
4/09/2014.

Thank you for the comment.

Comment accepted.

Appendix F Attachment A Line item#6 language revised.

~~*Comment:* ***72***~~

Available Reserve:

Reorder Line 4 and Line 5 to Line 5 and Line 6.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

Lines#4 and #5 reordered to Lines #5 and Line #6.

~~*Comment: **73***~~

Net Reserve:

Reorder Line 6 Line 7 and Line 8 to Line 7 Line 8 and Line 9.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

Line#6, Line #7 and Line#8 reordered to Lines #7, Line#8 and Line#9.

~~*Comment: **74***~~

Gross Margin:

Reorder Line 11 and Line 12 to Line 12 and Line 13.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

Line#11 and Line #12 reordered to Line #12 and Line#13.

~~*Comment: **75***~~

Net Resource Capacity Margin:

Reorder line 11 and Line 12 to Line 12 and Line 13.

CO7/CP11 Response:
3/25/2014.

Thank you for the comment.

Comment accepted.

Line#11 and Line #12 reordered to Line #12 and Line#13.

~~*Comment: **76***~~

Minimum Load Forecast:

Insert: ‘and indicate the day on which they are expected to occur.’

CO7/CP11 Response:
4/09/2014.

Thank you for the comment.

Comment accepted.

Appendix F Attachment A Line item#17 language revised

Comments from – HQT:

HQT respectfully submits comments on the Directory 1 revision that was posted on December 11, 2013.

HQT generally supports this version.

Many requirements are clearer and the table format contributes to even more clarity.

HQT is especially satisfied with the modification about flows adjustments after a first loss in Table 3 and with a clear statement in section 1.3 that contingencies are applied only to BPS elements.

However, HQT makes the following comments or suggestions:

~~*Comment: 77*~~

1.3 Objective:

We propose to add the following sentence at the end of 1st paragraph of the Objective: *"This aims to avoid instability, voltage collapse and widespread cascading outages".*

CO7/CP11 Response:
4/04/2014.

Thank you for the comment.

Comment accepted. CO7/CP11 has incorporated the suggested language into the Objective section.

~~*Comment: **78***~~

R1:

Information verification:

It may be very hard to demonstrate compliance with the requirement that information shall be verified annually. It is not clear what is meant by verification. We propose that NPCC establish a general methodology about how this verification should be done, distinguishing between existing and new data.

CO7/CP11 Response:
2/12/2014.

Thank you for the comment.

CO7/CP11 considered your comment and the issue of how to determine compliance to verification will be described in the Measures.

CO7/CP11 will seek guidance from its respective Task Forces on the development of the Measures.

~~*Comment:* ***79***~~

R4:

Responsibility:

In some places, the Resource Planner is involved for requirement R4 about the probability of loss of load expectation (LOLE). We propose to say "*Each Planning Coordinator, or each Resource Planner, shall…"*

CO7/CP11 Response:
2/12/2014.

Comment accepted.

Thank you for the comment.

CO7/CO7 agrees with the comment and has inserted Resource Planner in the applicability of Requirement R4.

~~*Comment:* ***80***~~

Table 1, event 2:

It may be helpful to specify what is really expected, maybe such as opening of one point for a line circuit connected to three points.

CO7/CP11 Response:
3/26/2014.

Thank you for the comment.

CO7/CP11 reviewed the circumstances associated with Table #1 Contingency Event #2 and feels the language as presented is satisfactory.

CO7/CP11 also noted that in certain cases judgement must be utilized when choosing how to apply this contingency.

~~*Comment:* **81**~~

Table 1 and 3:

Events 1 and 4 are slightly different than former D1. We propose to modify as following: *"Fault on any of the following*:"
For event 5, "loss of a circuit breaker" may cause confusion and we recommend the following: "*Internal breaker fault*", and "*phase to ground with normal fault clearing*". This is consistent with TPL-001-4 and let planners identify the elements that will be lost according to its single line diagram and protection scheme.

CO7/CP11 Response:
3/25/2014

Comment accepted.

CO7/CP11 agrees with the comment and has revised Table #1 and Table #3 accordingly.

~~*Comment Type:* **82**~~

Table 2, Extreme System Conditions:

Performance i. on pre-contingency conditions (specifying conditions not exceeded more than 25% of the time) should not apply to this part. Instead, conditions of either normal peak load or extreme peak load should apply, because the test wants to identify Extreme Conditions.

CO7/CP11 Response:
3/25/2014.

Comment accepted.

CO7/CP11 reviewed this comment and agreed to revise the Performance Assessments in Table#2, by deleting assessment i (a) from extreme weather assessment and deleting i (a) and i (b) from the fuel shortage assessment.

CO7/CP11 also spent considerable time discussing the wording of assessment i(a) and ultimately decided not to revise the language as currently written.

~~*Comment:* ***83***~~

General comments:

R13 – SPS:

There has been no consensus on CP11/CO7 to write criteria to identify type 1 SPS usage for the BPS. As a solution, R13 proposes a process to obtain approvals.

We agree that this is an improvement, but we will have to wait and see if experience proves in practice the efficiency of this solution.

With the change of BES definition at NERC, compliance of BPS to D1 through Interim or Comprehensive Transmission Review will no longer be sufficient for compliance with TPL at NERC.

In fact, TPL-001-4 includes some requirements that are more stringent than D1: 1) necessity to make sensitivity studies, 2) considering protection system outage in contingencies, 3) presenting both short and long term assessments, 4) making analyses for extreme contingencies at peak load or with two consecutive 3-phases fault contingencies without system adjustment in between.

Also, TPL applies to many more facilities, such as BES facilities not included in BPS. Members will need to be conscious of those differences.

CO7/CP11 Response:
3/12/2014.

Thank you for the comment.

CO7/CP11 has reviewed your comment and appreciates the additional information provided.

NPCC, Inc.

NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

May 22nd, 2014

Subject: Posting for Open Process Review of NPCC Directory#1 *Design and Operation of the BPS.*

NPCC Full Member Representatives and Alternates:

Please find attached clean and redlined versions of NPCC Directory#1 *Design and Operation of the Bulk Power System* which is now posted to receive your comments through the NPCC Process for Open Review.

On January 31st, 2013 the Task Force on Coordination of Planning (TFCP) and the Task Force on Coordination of Operation (TFCO) requested a collaborative review of the Phase 2 draft of Directory#1 by their respective working groups the CO7 and the CP11.

The combined CP11/CO7 Working Group completed an initial review of Directory#1 during which it reformatted the Directory#1 criteria into measurable requirements and posted a draft to the NPCC Open Process for 45 days concluding on January 25th, 2014.

NPCC received comments from eight of its Members and the Working Group reconvened to address comments, draft responses and revise the document as necessary.

Significant revisions to the draft based on the review of comments received include:

- Further revisions to the Objective section to clearly delineate where applicable performance requirements should be monitored.
- Revisions to the requirement language and performance attributes to improve clarity.
- Changes to the Directory format based on Working Group review and comment.
- Mapping of the reformatted criteria to the current in force version of Directory#1.
- Minor revisions to the Appendices.

However the CO7/CP11 Working Group was unable to reach consensus regarding a Member comment directed at a potential change to the criteria.

Specifically, the comment asserted that the existing NPCC criteria requires the testing of certain faults with the slower of either protection system A or protection system B and that the proposed change would impact reliability by weakening the criteria.

Conversely other Working Group Members contended that the change was necessary in order to properly clarify the criteria in order to avoid an overly conservative interpretation.

Ultimately, the TFCP directed that the criteria should remain as currently written and that notwithstanding the dissenting opinion the subject change to the criteria should be eliminated.

Subsequent to the CO7/CP11 review of comments the TFCO and the TFCP have reviewed the draft and have approved posting the document to the NPCC Open Process.

The NPCC Open Process may be accessed through the following link:

https://www.npcc.org/Standards/SitePages/NonStandardsList.aspx

Comments on Directory#1 will be received for forty five days through July 07, 2014.

Please contact me with any questions regarding the NPCC Open Process or the content of this document.

Gerry Dunbar
Northeast Power Coordinating Council, Inc.
212.840.1070 (p)
212.302.2782 (f)
gdunbar@npcc.org

NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

DRAFT 14:
Redlined to CO7/CP11 Review of Open Process Comments
Regional Reliability Reference Directory # 1
Design and Operation of the Bulk Power System

Task Force on Coordination of Planning Revision Review Record:

May 22nd, 2014

Note: Requirement R8 reordered as Requirement R7.1 on 3/5/2014, which reordered all subsequent requirements and sub requirements in the draft after R7.1.

Therefore, comments in the margin referencing requirements after R7.1 will no longer be aligned. (Reference is now (Requirement Rx -1).

Adopted by the Members of the Northeast Power Coordinating Council, Inc., on December 01, 2009 based on recommendation by the Reliability Coordinating Committee, in accordance with Section VIII of the NPCC Amended and Restated Bylaws dated July 24, 2007 as amended to date.

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

Revision History

Version	Date	Action	Change Tracking (New, Errata or Revisions)
0	December 1, 2009		New
1	4/20/2012	Errata Changes in Appendices B and E.	Errata

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

Table of Contents

1.0 Introduction 4
1.1 Title: Design and Operation of the Bulk Power System 4
1.2 Directory Number: 1 4
1.3 Objective: 4
1.4 Effective Date: December 1, 2009 4
1.5 Background 4
1.6 Applicability 5
1.6.1 Functional Entities 5
1.6.2 Applicability of NPCC Criteria: 5
2.0 Defined Terms: 5
3.0 NPCC Full Member, More Stringent Criteria: 6
4.0 Compliance: 11

Field Code Changed

Table 1 - Planning Design Criteria, Contingency events, Fault type, Performance requirements

Table 2 - Planning Criteria: Extreme Contingency and System Conditions, Fault type, Performance assessments

Table 3 - Operating Criteria**,** Contingency events, Fault type, Performance requirements

Appendix A - Reserved for Future Use~~.~~

Appendix B - Guidelines and Procedures for NPCC Area Transmission Review

Appendix C - Procedure for Testing and Analysis of Extreme Contingencies

Appendix D - Guidelines for Area Review of Resource Adequacy

Appendix E - Guidelines for Requesting Exclusions to Simultaneous Loss of Two Adjacent Transmission Circuits on a Multiple Circuit Tower

Appendix F - Procedure for Operational Planning Coordination

Appendix G - Procedures for Inter Reliability Coordinator Area Voltage Control

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

1.0 Introduction

1.1 Title: Design and Operation of the Bulk Power System

1.2 Directory Number: 1

1.3 Objective:

The objective of this Directory is to provide a "design-based approach" to design and operate the **bulk power system** to a level of reliability that will not result in the loss or unintentional separation of a major portion of the system from any of the contingencies referenced in **R7** and **R14.** The intent of this approach is to avoid instability, voltage collapse and widespread cascading outages. Loss of small portions of a system (such as radial portions) may be tolerated provided these do not jeopardize the reliability of the remaining **bulk power system**.

Mapped to Section# 1.3 Objective.

CO7/CP11 revised language to improve clarity.

In NPCC the technique for achieving this level of reliability is to require that the **bulk power system** be designed and operated to meet the performance requirements for the representative **contingencies** as specified in this Directory. Simulations shall be used to assess and analyze these **contingencies. Contingency** events shall be applied on **bulk power system** elements and the resulting performance requirements shall be monitored on the **bulk power system.**

~~Simulation of contingency events shall be applied on **bulk power system** elements and the resulting performance requirements shall be monitored on the **bulk power system.**~~

~~It is the responsibility of each Reliability Coordinator to ascertain that their portion of the **bulk power system** is operated in conformance with these criteria. It is the responsibility of each Transmission Planner and Planning Coordinator to ascertain that their portion of the **bulk power system** is designed in conformance with these criteria. Loss of small portions of a system (such as radial portions) may be tolerated provided these do not jeopardize the reliability of the remaining **bulk power system.**~~

The characteristics of a reliable **bulk power system** include adequate **resources** and transmission to reliably meet projected customer electricity demand and energy requirements as prescribed in this document.

1.4 Effective Date: December 1, 2009

Mapped to Section#1.5 Background.

Background

This Directory was developed from the NPCC A-2 criteria document - *Basic Criteria for the Design and Operation of Interconnected Power Systems* (May 6, 2004

version). Guidelines and Procedures for consideration in the implementation of this Directory are provided in the Appendices.

1.6 Applicability

1.6.1 Functional Entities

Reliability Coordinators
Transmission Operators
Balancing Authorities
Planning Coordinators
Transmission Planners
Resource Planners
Generator Owners
Transmission Owners

Mapped to Section #1.6.1 Functional Entities.

CO7/CP11 updated to include GO's and TO's as responsible Functional Entities.

1.6.2 Applicability of NPCC Criteria:

New Section.

Added at the request of TFCO to clearly specify applicability of NPCC criteria.

Will be inserted in all NPCC Directories.

The requirements of an NPCC Directory apply only to those ~~NPCC transmission~~ facilities defined as NPCC **bulk power system** elements and identified through the performance based methodology of NPCC Document A-10, "*Classification of Bulk Power System Elements*," the list of which is maintained by the NPCC Task Force on System Studies and approved by the NPCC Reliability Coordinating Committee."

Requirements to abide by an NPCC Directory may also reside in external tariff requirements, bilateral contracts and other agreements between facility owners and/or operators and their assigned Reliability Coordinator, Planning Coordinator, Transmission Operator, Balancing Authority and/or Transmission Owner as applicable and may be enforceable through those external tariff requirements, bilateral contracts and other agreements. NPCC will not enforce compliance to the NPCC Directory requirements in this document on any entity that is not an NPCC Full Member.

Mapped to Section #2.

NPCC defined terms no longer contained in each Directory. All NPCC defined terms reside in the NPCC Glossary A-7.

2.0 Defined Terms:

Unless specifically noted in this document terms in bold typeface are defined in the NPCC Glossary of Terms.

3.0 NPCC Full Member~~, More Stringent~~ Criteria:

Information for Planning and Operational Assessments

R1 mapped to Section #5.1.3 CO7/CP11 revised to improve clarity. No change in intent of requirement

R1 Each Functional Entity that owns equipment shall ~~annually~~ submit verified ~~verify the~~ information representing the physical or control characteristics of its equipment for system modelling and reliability analysis of the ~~it submits for use in for~~ **bulk power system** ~~analysis. representing the physical or control characteristics of the equipment~~.

R2 mapped to Section #5.1.3 CO7/CP11 revised to improve clarity. No change in intent of requirement

R2 Each Planning Coordinator and Reliability Coordinator shall collect and ~~,~~ maintain information needed for system modelling and reliability analysis of the **bulk power system** as submitted in accordance with Requirement R1. ~~and submit information needed for system modelling and reliability analysis of the **bulk power system**.~~

R2.1 mapped to Section #5.1.3.

CO7/CP11 added R2.1 to clarify existing process.

R2.1 This information shall be submitted to NPCC upon request.

R3 Each Reliability Coordinator shall share and coordinate forecast system information and real-time information to enable and enhance the analysis and modeling of the interconnected **bulk power system** by security application software on energy management systems.

R3 mapped to Section #5.1.3 No change in intent of requirement.

Resource Adequacy

R4 Each Planning Coordinator or Resource Planner shall probabilistically evaluate resource adequacy of its Planning Coordinator **Area** portion of the **bulk power system** to demonstrate that the loss of **load** expectation (LOLE) of disconnecting **firm load** due to resource deficiencies ~~shall be~~are is, on average, no more than 0.1 days per year.

R4 and R4.1 mapped to Section # 5.2.

No change in intent of requirements.

R4.1 Make due allowances for demand uncertainty, scheduled outages and deratings, forced outages and deratings, assistance over interconnections with neighboring Planning Coordinator **Areas**, transmission transfer capabilities, and capacity and/or load relief from available operating procedures. ~~In the calculation of available **resources,** supply-side purchases from neighbouring systems are limited to firm capacity backed purchases~~

.

R5 Each Planning Coordinator shall ~~evaluate~~ report and obtain Reliability Coordinating Committee (RCC) approval for its Review of **Resource** Adequacy. Appendix D provides guidance for the Area Review of **Resource** Adequacy.

R5, R5.1, R5.2, and R5.3 moved from existing Appendix D Section#3--- proposed as new requirements.

R5.1 The Review of **Resource** Adequacy will be presented to the NPCC Task

Force on Coordination of Planning (TFCP). Comprehensive and Interim reviews shall be presented to the TFCP before the beginning of the first time period covered by the assessment.

R5.2 A Comprehensive Review of **Resource** Adequacy is required every three years and will cover a time period of five years. If changes in planned facilities or forecasted system conditions warrant, TFCP may require a Comprehensive Review of **Resource** Adequacy in less than 3 years.

R5.3 In subsequent years, each Planning Coordinator shall conduct an Annual Interim Review of **Resource** Adequacy that will cover, at a minimum, the remaining years studied in the Comprehensive Review of **Resource** Adequacy.

R6 Each Reliability Coordinator shall coordinate outages and deratings of **resources** to verify adequate **resources** will be available to meet the forecasted demand and **reserve** requirements. Appendix F provides guidance for Operational Planning Coordination.

R6 mapped to Section #5.3.

Proposed changes in requirement.

R6.1 A Summer and Winter Reliability Assessment will be presented to the NPCC Task Force on Coordination of Operation (TFCO) every year. ~~The Review of **Resource** Adequacy will be presented to the NPCC Task Force on Coordination of Planning (TFCP). Perform a summer and winter reliability assessment every year~~.

R6.1 moved from existing Appendix F Section#2.1--- proposed as new requirement.

Transmission Planning

R7 Each Transmission Planner and Planning Coordinator shall plan the system to meet the respective performance requirements for the **contingencies** as specified in ~~the system conditions, contingencies and performance requirements contained within~~ Table 1 in the design of its ~~NPCC~~ **bulk power system**.

R7 and R7.1 mapped to Section #5.4.

Table#1established to organize performance requirements, fault types and contingencies.

Performance requirements in Table#1 mapped to Sections# 5.4.1 and Section# 5.4.2.

R7.1 ~~Each Transmission Planner and Planning Coordinator shall model~~ Credible combinations of system conditions which stress the system shall be modelled including, load forecast, inter-Area and intra-Area transfers, transmission configuration, active and reactive resources, generation availability and other dispatch scenarios.

R8 Each Transmission Planner and Planning Coordinator shall assess the impact of the extreme **contingencies** listed in Table 2. Appendix C provides guidance for testing and analyzing extreme contingencies.

R8 mapped to Section#5.6.

Table#2 established to organize the performance assessments in Section#5.6.

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

R9 Each Transmission Planner and Planning Coordinator shall assess the impact of extreme system conditions, one condition at a time, subject to contingencies as listed in the "Extreme System Conditions" category of Table 2.

R9 mapped to Section#5.7.

No change in intent of requirement.

R10 Each Transmission Planner and Planning Coordinator shall have procedures and implement a system design that ensures equipment capabilities are adequate for fault current levels with all transmission and generation facilities in service for all operating conditions which are not prohibited by a procedure and coordinate these procedures with ~~adjacent~~ materially affected Transmission Planner and Planning Coordinator Areas.

R10 mapped to Section#5.4.3.

No change in intent of requirement.

R11 Each Planning Coordinator shall conduct and obtain Reliability Coordinating Committee (RCC) approval for its Transmission Review. Appendix B provides guidance for Transmission Reviews.

R11 moved from Appendix B Section#1.

Proposed as new requirement.

R11.1 A Comprehensive Transmission Review is required at least once every five years or if major or pervasive system changes have occurred. If changes in the planned facilities or forecasted system conditions warrant, the Task Force on System Studies (TFSS) may require a Comprehensive Transmission Review in less than five years.

R11.2 The proposal for the type of annual Transmission Review shall be presented to TFSS by March of the year during which the review is conducted. Approval for the type of Transmission Review shall be obtained from the TFSS. The annual Transmission Review shall be presented to the TFSS by April of the following year.

R11.3 If the results of the Transmission Review indicate that the planned ~~NPCC~~ **bulk power system** will not be in conformance with NPCC Directory #1, the Transmission Review shall incorporate a corrective action plan to achieve conformance.

R11.1, R11.2 and R11.3 moved from Appendix B Section#4.

Proposed as new requirements.

Special Protection Systems

R12 Each Functional Entity that proposes a new or modified SPS shall consider the complexity of the scheme and the consequences of correct or incorrect operation as well as its benefits.

R12 and R12.1 mapped to Section#5.1.1.

No change in intent of requirement.

R12.1 Provide a rationale and justification to the TFCP including factors such as project delays, temporary construction configurations, unusual combinations of system conditions, equipment outages and infrequent contingencies.

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

~~**R12.2** Obtain approvals in accordance with Directory#7.~~

Transmission Operation

R13 mapped to Section #5.1.2.

Table#3 established to organize performance requirements, fault types and contingencies.

Performance requirements in Table#3 mapped to Sections# 5.5, Section# 5.5.1. and 5.5.2.

R13 Each Reliability Coordinator and Transmission Operator shall establish **normal transfer capabilities** and **emergency transfer capabilities, for** ~~and operate~~ its portion of the **bulk power system** to meet the respective performance requirements ~~and system conditions~~ for the **contingencies** as specified in Table 3.

R14 mapped to Section #5.1.2.

No change in intent of requirement.

R14 Each Reliability Coordinator and **Transmission** Operator shall operate to **normal transfer capabilities** unless an **emergency,** in accordance with NPCC Directory# 2, is identified.

R15 mapped to Section #5.5.3.

No change in intent of requirement.

R15 Each Reliability Coordinator and Transmission Operator shall make system adjustments once an **emergency** has been identified, including the pre-**contingency** disconnection of **firm load,** to avoid exceeding **emergency transfer capabilities.**

R16 mapped to Section #5.5.3.

No change in intent of requirement.

R16 Each Reliability Coordinator and Transmission Operator shall assess the status of the **bulk power system** immediately after the occurrence of any **contingency** and prepare for the next **contingency as specified in Table 3**.

R16.1 mapped to Section #5.5.3.

No change in intent of requirement.

R16.1 Voltage reduction and shedding of firm load shall be ~~required~~ deployed to return the system to a secure state, if other system adjustments are not adequate. Voltage reduction need not be initiated and firm load need not be shed to observe a post contingency loading requirement until the **contingency** occurs, provided that adequate response time for this action is available.

R16.2 mapped to Section #5.5.3.

No change in intent of requirement.

R16.2 System adjustments shall be completed as quickly as possible following any **contingency,** ~~,~~ but ~~in all cases~~ within 30 minutes after the occurrence of any **contingency** specified in Table 3.

R17 mapped to Section #5.5.

No change in intent of requirement.

R17 Each Reliability Coordinator shall notify the applicable Reliability Coordinators of forced outages of any facility as per the NPCC Transmission Facilities Notification List and of any other condition which may impact inter-Area reliability.

R18 mapped to Section #5.5.

No change in intent of requirement.

R18 Each Reliability Coordinator shall coordinate scheduled outages of facilities that are on the NPCC Transmission Facilities Notification List sufficiently in advance of the outage to permit the affected Reliability Coordinators to maintain reliability. Appendix F provides guidance for Operational Planning Coordination.

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

R18.1 moved from Appendix F Section#4.2.

Proposed as new requirement.

R18.1 Review and update its Facilities Notification List and submit the list to the NPCC Task Force on Coordination of Operation (TFCO) annually.

R19 moved from Appendix G Section#1.

Proposed as new requirement.

R19 Each Reliability Coordinator shall coordinate voltage control between Transmission Operator Areas. Appendix G provides guidance for Inter- Reliability Coordinator Area Voltage Control.

R19.1 moved from Appendix G Section#2.1.

Proposed as new requirement.

R19.1 Metering for **reactive power** resources and voltage controller status shall be consistent between adjacent Transmission Operators.

R19.1 moved from Appendix G Section#4.3.

Proposed as new requirement.

R19.2 Upon request from the TFCO, perform an Inter-Area Voltage Control Assessment.

4.0 Compliance:

Compliance with the requirements set forth in this Directory will be in accordance with the NPCC Criteria Compliance and Enforcement Program (CCEP).

Compliance with Directory#1 shall be demonstrated for all requirements that are not required for compliance with the NERC Reliability Standards and NPCC will not enforce duplicate sanctions for the same violation.

Prepared by: Task Force on Coordination of Planning

Review and Approval: Revision to any portion of this Directory will be posted by the lead Task Force in the NPCC Open Process for a 45 day review and comment period. Upon addressing all the comments in this forum, the Directory document will be sent to the remaining Task Forces for their recommendation to seek RCC approval.

Upon approval of the RCC, this Directory will be sent to the Full Member Representatives for their final approval if sections pertaining to the Requirements and Criteria portion have been revised. All voting and approvals will be conducted according to the most current "NPCC. Bylaws" in effect at the time the ballots are cast.

Revisions pertaining to the Appendices or other portions of the document such as links, etc., only require RCC approval.
Errata may be corrected by the Lead Task Force at any time.

This Directory will be updated at least once every three years and as often as necessary to keep it current and consistent with NERC, Regional Reliability Standards and other NPCC documents.

References:
NPCC Glossary of Terms
Emergency Operations (NPCC Directory #2)
Maintenance Criteria for Bulk Power System Protection (NPCC Directory #3)
Bulk Power System Protection Criteria (NPCC Directory #4)
Reserve (NPCC Directory #5)
Special Protection Systems (NPCC Directory #7))
Classification of Bulk Power System Elements (A-10)

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

Table 1

Planning Design Criteria: Contingency events, Fault type and Performance requirements to be applied to bulk power system elements

~~*Compliance with Directory#1 shall be demonstrated for all requirements listed in the table below that are not required for compliance with the NERC Reliability Standards.*~~

Category	**Contingency** events Simulate the removal of all elements that protection systems, including Special Protection Systems, are expected to automatically disconnect for each event that involves an AC fault.	**Fault** type (permanent) **On the listed elements where applicable**	**Performance** requirements
I **Single Event**	1. Fault on ~~Loss of~~ any of the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section	Three-phase **fault** with **normal fault clearing**	i. to ix.
	2. Opening of any circuit breaker	No fault	
	3. Loss of single pole of a direct current facility	No fault	
	4. Fault on~~Loss of~~ any of the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section	Phase to ground fault with **delayed fault clearing**	
	5. Fault~~Loss~~ on~~of~~ a circuit breaker	Phase to ground ~~internal~~ **fault,** with **normal fault clearing**	
	6. Simultaneous fault~~loss~~ on ~~of~~ two adjacent transmission circuits on a multiple circuit tower.	Phase to ground **faults** on different phases of each circuit, with **normal fault clearing**	
	7. Simultaneous permanent loss of both poles of a direct current bipolar facility	Without an ac fault	
	8. The failure of a circuit breaker to operate when initiated by a **SPS** after a fault ~~the loss of~~on the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section f. opening of any circuit breaker (without a fault)	Phase to ground **fault**, with **normal fault clearing**	

Performance requirements in Table#1 mapped to Sections# 5.4.1 and Section# 5.4.2.

Category	**Contingency** events Simulate the removal of all elements that protection systems, including Special Protection Systems, are expected to automatically disconnect for each event that involves an AC fault.	**Fault** type (permanent) **On the listed elements where applicable**	**Performance** requirements
II Event(s) after a first loss and after System Adjustment	1. Following the loss of any critical : a. transmission circuit, b. transformer, c. series or shunt compensating device or d. generator e. Single pole of a direct current facility and after System Adjustment, Categor~~y~~ies I **Contingencies** shall also apply.	Any Category I event as described above.	Performance requirements i to ix apply **Area** generation and **power** flows are adjusted between outages by the use of resources available within ten minutes following notification and other system adjustments such as HVDC and phase angle regulator adjustments that can be made within 30 minutes.

Performance Requirements~~:~~ for the contingencies defined in Table 1 :

i. Loss of a major portion of the system or unintentional separation of a major portion of the system shall not occur.

ii. Loss of small or radial portions of the system pre-determined by studies is acceptable provided the performance requirements are not violated for the remaining **bulk power system**.

iii. Voltages and loadings shall be within applicable limits for the ~~applicable~~ pre-**contingency** conditions.

iv. Voltages and loadings shall be within **applicable emergency limits** for post-**contingency** conditions.

v. Adequate reactive power resources and appropriate controls shall be available to maintain voltages within applicable limits.

vi. The **stability** of the **bulk power system** shall be maintained during and following the most severe **contingencies,** with due regard to successful and unsuccessful ~~automatic~~ **reclosing**.

vii. For each of the **contingencies** that involve~~s a **normal**~~ **fault clearing**, **stability** shall be maintained when the simulation is based on **fault clearing** initiated by the **"system A" protection group**, and also shall be maintained when the simulation is based on **fault clearing** initiated by the **"system B" protection group**. When applying this requirement to **contingency** Event ***no 6***, the failure of a **protection group** shall apply only to one circuit at a time.

viii. Regarding **contingency** ***no 6***, if multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded. Other similar situations can be excluded on the basis of acceptable risk, provided that the Reliability Coordinating Committee specifically accepts each request for exclusion. (See Appendix E.)

ix. Transient voltage response shall be within acceptable limits established by the Planning Coordinator and the Transmission Planner.

Table 2

Planning Criteria: Extreme Contingency and System Conditions, Fault type and Performance Assessments to be applied to bulk power system elements

~~*Compliance with Directory#1 shall be demonstrated for all requirements listed in the table below that are not required for compliance with the NERC Reliability Standards.*~~

Category	**Contingency** events Simulate the removal of all elements that protection systems, including Special Protection Systems, are expected to automatically disconnect for each event that involves an AC fault.	**Fault** type (permanent) and/or **condition applied** **On the listed elements where applicable**	**Performance** to be assessed
Extreme Contingency	1. Loss of the entire capability of a generating station.	No Fault	i, ii, iii.
	2. Loss of all transmission circuits emanating from a generating station, switching station, substation or dc terminal.	No Fault	
	3. Loss of all transmission circuits on a common right-of-way.	No Fault	
	4. Fault~~Loss~~ on of any of the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section	Three-phase **fault** with **delayed fault clearing (**with due regard to successful and unsuccessful ~~automatic~~ **reclosing**.)	
	5. ~~Loss~~ Fault on ~~of~~ a circuit breaker	Three-phase ~~internal~~ **fault**, with **normal fault clearing**	
	6. Sudden loss of a large load or major load center.	No Fault	
	7. The effect of severe power swings arising from disturbances outside the ~~Council's~~ NPCC's interconnected systems.	Fault applied as necessary.	
	8. Failure of a **Special Protection System**, to operate when required following the normal contingencies listed in Table 1, Category I, Single Event.	As listed in Table 1, Category I, Single Event.	
	9. The operation or partial operation of a **Special Protection System** for an event or condition for which it was not intended to operate.	No Fault	
	10. Sudden loss of fuel delivery system to multiple plants, (e.g. gas pipeline contingencies).	No Fault.	
	Any additional extreme contingencies identified by each Planning Coordinator Area.	Fault applied as necessary.	
Extreme	Contingency events listed in Table 1, Category I, Single Event	Peak **load** conditions resulting from extreme weather.	i(b, c), ii, iii.

Performance assessments in Table#2 mapped to Section#5.6.

NPCC Directory #1
Table 2

Category	**Contingency** events Simulate the removal of all elements that protection systems, including Special Protection Systems, are expected to automatically disconnect for each event that involves an AC fault.	**Fault** type (permanent) and/or **condition applied** **On the listed elements where applicable**	**Performance** to be assessed
System Conditions **Extreme System Conditions**		Generating unit(s) fuel shortage (e.g. gas supply adequacy or low hydro) under normal weather peak conditions	i(c), ii, iii

Performance Assessment

i. Model the following pre-contingency conditions:

   a. transfers within or between Transmission Planner and Planning Coordinator Areas should be studied at values not expected to be exceeded more than 25% of the time.

   b. highly probable dispatch patterns of generation for the transfers being studied

   c. appropriate load representation (e.g. active and reactive power as a function of voltage) for transient tests and post transient load flows.

ii. Examine post contingency steady state conditions, as well as stability, overload, cascading outages and voltage collapse to obtain an indication of system robustness and determine the extent of any widespread system disturbance

iii. Where assessment concludes there are serious consequences, an evaluation of implementing a change to design or operating practices to address such contingencies shall be conducted.

Table 3

Operating Criteria: Contingency events, Fault type and Performance requirements to be applied to bulk power system elements to establish transfer capabilities.

~~*Compliance with Directory#1 shall be demonstrated for all requirements listed in the table below that are not required for compliance with the NERC Reliability Standards.*~~

~~Category~~	**Contingency** events Simulate the removal of all elements that protection systems, including Special Protection Systems, are expected to automatically disconnect for each event that involves an AC fault.	**Fault** type (permanent) **On the listed elements where applicable**	**Performance** requirements	
			Normal Transfer Capability	**Emergency** Transfer Capability (only after an **Emergency** is identified)
~~I~~ ~~Single Event~~	1. Fault on~~Loss of~~ any of the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section	Three-phases **fault**, with **normal fault clearing**	i.,ii, iii,iv,v, vi, vii ~~to~~ viii, ~~xi~~, x, xi.	i, ii, iii, iv, v, vi, vii,viii ~~ix,~~ x, xii,
	2. Opening of any circuit breaker	No fault		
	3. Loss of single pole of a direct current facility	No fault		
	4. Fault on~~Loss of~~ any of the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section	Phase to ground fault, with **delayed fault clearing**	i,ii,iii,iv,vii,viii,ix,x,xi,	Contingency Events 4 through 8 do not apply after an emergency is identified.
	5. Fault on ~~Loss of~~ a circuit breaker	Phase to ground ~~internal~~ **fault,** with **normal fault clearing**		
	6. Simultaneous fault on ~~loss of~~ two adjacent transmission circuits on a multiple circuit tower.	Phase to ground **faults** on different phases of each circuit, with **normal fault clearing**		
	7. Simultaneous permanent loss of both poles of a direct current bipolar facility	Without an ac fault		
	8. The failure of a circuit breaker to operate when initiated by a **SPS** after a fault on the ~~the loss of the~~ following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section	Phase to ground **fault**, with **normal fault clearing**		

Performance requirements in Table#3 mapped to Sections# 5.5, Section# 5.5.1., and 5.5.2.

	9. ~~opening of any circuit breaker (without a fault)~~			
	9. The failure of a circuit breaker to operate when initiated by a SPS after opening of any circuit breaker.	No fault.	i. i,ii,iii,iv,vii,viii,ix,x, xi,	

Performance Requirements for the contingencies defined in Table 3:

i. Loss of a major portion of the system or unintentional separation of a major portion of the system shall not occur.

ii. Loss of small or radial portions of the system pre-determined by studies is acceptable provided it does not violate the performance requirements for the remaining BPS.

iii. Individual Reliability Coordinator Areas shall be operated in a manner such that **Contingencies** and conditions applied can be withstood without causing **significant adverse impact** on other Reliability Coordinator Areas.

~~ii.~~iv. Voltages and loadings shall be within applicable limits for the ~~applicable~~ pre-**contingency** conditions.

~~iii.~~v. Voltages and loadings shall be within **applicable emergency limits** for post-**contingency** conditions.

~~iv.~~vi. Adequate reactive power resources and appropriate controls shall be available to maintain voltages within applicable limits.

~~v.~~vii. The **stability** of the **bulk power system** shall be maintained ~~during and following the most severe **contingencies**~~**,** with due regard to successful and unsuccessful ~~automatic~~ **reclosing**.

~~vi.~~viii. For each of the **contingencies** that involve ~~a **normal**~~ **fault clearing**, **stability** shall be maintained when the simulation is based on **fault clearing** initiated by the **"system A" protection group**, and also shall be maintained when the simulation is based on **fault clearing** initiated by the **"system B" protection group**. When applying this requirement to **contingency** Event ***no 6***, the failure of a **protection group** shall apply only to one circuit at a time.

~~vii.~~ix. Regarding **contingency *no 6***, if multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded. Other similar situations can be excluded on the basis of acceptable risk, provided that the Reliability Coordinating Committee specifically accepts each request for exclusion. (See Appendix E.)

~~viii. Individual Reliability Coordinator Areas shall be operated in a manner such that **Contingencies** and conditions applied can be withstood without causing **significant adverse impact** on other Reliability Coordinator Areas.~~

~~ix.~~x. Appropriate adjustments shall be made to Reliability Coordinator Area operation to accommodate the impact of **protection group outages**, including the **outage** of a **protection group** which is a part of a **Type I special protection system**. For typical periods of forced outage or maintenance of a **protection group**, it can be assumed, unless there are indications to the contrary, that the remaining **protection** will function as designed. If the **protection group** will be out of service for an extended period of time, additional adjustments to operations may be appropriate considering other system conditions and the consequences of possible failure of the remaining **protection group.**

~~x.~~xi. Normal transfer levels shall not require system adjustments before attempting manual~~ly~~ reclosing of ~~faulted~~ elements unless specific instructions describing alternate actions are in effect to maintain stability of the **BPS**.

~~xi.~~xii. Emergency transfer levels may require system adjustments before attempting ~~manually reclosing~~manual reclosing of ~~faulted~~ elements to maintain stability

of the **bulk power system**.

Operating to the contingencies listed above in Table 3 is considered to provide an acceptable level of **bulk power system** security. However, under high risk conditions, such as severe weather, the expectation of the occurrence of contingencies not listed in Table 3 and/or the associated consequences may be judged to be significantly greater. When these conditions exist, consideration should be given to operating in a more conservative manner.

Appendix A – Reserved for Future Use

Appendix B - Guidelines and Procedures for NPCC Transmission Reviews

1.0 Introduction

NPCC has established a Reliability Assessment Program to bring together work done by NPCC, Transmission Planners and Planning Coordinators relevant to the assessment of **BPS reliability**. As part of the Reliability Assessment Program, the Task Force on System Studies (TFSS) is charged on an ongoing basis with conducting periodic reviews of the **reliability** of the planned **bulk power ~~transmission~~ system** of each Planning Coordinator Area of NPCC ~~and the transmission interconnections to other Planning Coordinator Areas.~~ The purpose of these reviews is to determine whether each Planning Coordinator Area's planned bulk power transmission system is in conformance with the NPCC Directory #1 *Design and Operation of the Bulk Power System*. The annual Area Transmission Review required in R12 is presented for this purpose. It is expected that this Review will cover Directory #1 requirements as they apply to the **bulk power system**.

2.0 Purpose of Review Presentation

The purpose of the presentation associated with an Area Transmission Review is to demonstrate that the Planning Coordinator's planned **bulk power system** based on its projection of available **demand**, transmission, and **resources**, is in conformance with the Directory #1 criteria. By such a presentation, the Task Force will satisfy itself that the criteria have been met and, in general, that the **reliability** of the NPCC Interconnected Systems will be maintained.

3.0 Study Year To Be Considered

It is suggested that a study year of 4 to 6 years from the reporting date is a realistic one, both from the viewpoint of minimum lead times required for construction, and the ability to alter plans or facilities. The reviews may be conducted for a longer term beyond 6 years to address identified marginal conditions that may have longer lead-time solutions.

4.0 Types and Frequency of Reviews

As described in requirement **R12,** each Planning Coordinator is required to present an annual transmission review to TFSS. However, the review presented by the Planning Coordinator may be one of three types: a Comprehensive (or Full) Review, an Intermediate (or Partial) Review, or an Interim Review.

A Comprehensive Review is a thorough assessment of the Planning Coordinator's entire bulk power transmission system, and includes sufficient analyses to fully address all aspects of an Area Transmission Review as described in **R12.**

In the years between Comprehensive Reviews, Planning Coordinators may conduct either an Interim Review, or an Intermediate Review, depending on the extent of the Planning

Coordinator's system changes since its last Comprehensive Review. If the system changes are relatively minor, the Planning Coordinator may conduct an Interim Review. In an Interim Review, the Planning Coordinator provides a summary of the changes in planned facilities and forecasted system conditions since its last Comprehensive Review and a brief discussion and assessment of the impact of those changes on the bulk power transmission system. No new analyses are required for an Interim Review.

If the Planning Coordinator's system changes since its last Comprehensive Review are moderate or concentrated in a portion of the Planning Coordinator's system, the Planning Coordinator may conduct an Intermediate Review. An Intermediate Review covers all the elements of a Comprehensive Review, but the analyses may be limited to addressing only those issues considered to be of significance, considering the extent of the system changes.

In March of each year, after a Planning Ceoordinator presents a proposal for the type of review to be conducted during the current year, TFSS will consider each Planning Coordinator's proposal. TFSS will either indicate their concurrence, or require the Planning Coordinator to conduct a more extensive review if the Task Force feels that such is warranted based on the Planning Coordinator's system changes since its last Comprehensive Review.

5.0 Format of Presentation – Comprehensive and Intermediate Review

a) Introduction

- Reference the most recent Area Comprehensive Review and any subsequent Intermediate or Interim reviews as appropriate.
- Describe the type and scope of this review.
- For a Comprehensive Review, describe the existing and planned **bulk power system** facilities included in this review.
- Describe changes in system facilities, **bulk power system elements** and **loads** since the most recent Comprehensive Review.
- Include maps and one-line diagrams of the system showing proposed changes as necessary.
- Describe the demand levels to be studied, according to the range of forecast system demands.
- Identify projected firm transfers and interchange schedules.

b) Present the scope of the analyses. The analyses conducted for a Comprehensive Review should be thorough, but an Intermediate Review may focus on specific areas of the system, specific system conditions, or a more limited set of "critical" **contingencies**.

c) Steady State Assessment

- Present the **load** model, power factor, demand side management, and other modeling assumptions used in the analysis. Discuss the methodology used in voltage assessments. (An Intermediate Review may refer to the discussion from the last Comprehensive Review.)
- Provide supporting information on the **contingencies** selected for evaluation and an explanation of why **contingencies** not simulated would produce less severe results.
- Provide information on the generation dispatch conditions assumed in the analysis.
- Include plots of "base case" **load** flows with all lines in service for the various conditions studied, e.g., peak, off-peak, and heavy transfers.
- Present the effects of major planned changes on the system.
- Identify applicable transfer limits within and between Planning Coordinator Areas.
- Show the adequacy of voltage performance and voltage control capability for the planned bulk power transmission system.

d) Stability Assessment

Present and/or refer to significant studies showing the effect of **contingencies** on the system and report on the most severe **contingencies** in the following manner:

- Provide supporting information on the **contingencies** selected for evaluation and an explanation of why **contingencies** not simulated would produce less severe results.
- The nature of the **fault** applied, **elements** switched, and **fault clearing** times.
- Plots of angles versus time for significant machines, response of real and reactive power control devices ~~HVdc and SVC response~~, voltages at significant buses and significant interface flows.

For a Comprehensive or Intermediate Review, present the **load** model and other modeling assumptions used in the analysis. (An Intermediate Review may refer to the discussion from the last Comprehensive Review.)

e) **Fault** Current Assessment

- Present the methodology and assumptions used in the **fault** current assessment. (An Intermediate Review may refer to the discussion from the last Comprehensive Review.)

- Present instances where **fault** levels exceed equipment capabilities and measures to mitigate such occurrences.

- Present changes to **fault** levels at stations adjacent to other Planning Coordinator Areas.

f) Extreme **Contingency** Assessment

- Present the scope of the analyses including a description of the system conditions assessed. The analyses conducted for a Comprehensive Review should be thorough, but an Intermediate Review may focus on specific areas of the system, specific system conditions, or a more limited set of "critical" **contingencies**.

- Provide supporting information on the extreme **contingencies** selected for evaluation and an explanation of why the remaining **contingencies** not simulated would produce less severe results.

- Review the results for widespread cascading due to overloads, instability or voltage collapse caused by extreme **contingencies**

- In the case where **contingency** assessment reveals serious consequences, conduct an evaluation of implementing a change to address such **contingencies**.

g) Extreme System Condition Assessment

- Present the scope of the analyses including a description of the system conditions assessed. The analyses conducted for a Comprehensive Review should be thorough, but an Intermediate Review may focus on specific areas of the system, specific system conditions, or a more limited set of "critical" **contingencies**.

- Provide the rationale for the loss of fuel supply conditions selected for evaluation and an explanation of why other loss of fuel supply conditions not simulated would produce less severe results.

- Provide supporting information on the **contingencies** selected for evaluation and an explanation of why the remaining **contingencies** not simulated would produce less severe results.

- In the case where extreme condition assessment reveals serious consequences, conduct an evaluation of implementing measures to mitigate such consequences.

h) Review of **Special Protection Systems (SPSs)**

- Present the scope of review. A Comprehensive Review should review all the existing, new, and modified **SPSs** included in its transmission plan. An Intermediate Review may focus on the new and modified **SPSs**, and just those existing **SPSs** that may have been impacted by system changes since they were last reviewed.

- Present the need and utilization for Type I and Type II **SPSs.** For instances where a **SPS** utilization is anticipated to increase, the TFSS should inform the Task Force on Coordination of Planning (TFCP) of this finding.

- Review the validity of the classification of Type III **SPSs**. For instances where a **SPS** which was formerly considered to have only local consequences is identified as having the potential for inter- Planning Coordinator Area effects, for the time period being reviewed, the TFSS should notify the Task Force on Coordination of Planning, System Protection and Coordination of Operation. In such instances a complete review of the **SPS** should be made, as per the *Procedure for NPCC Review of New or Modified Bulk Power System Special Protection Systems (SPS)* in Directory #7.

i) Review of Dynamic Control Systems (DCSs)

Review of potential consequences of failure or misoperation of Dynamic Control Systems (DCS), as defined in NPCC Document C-33 *Procedure for Analysis and Classification of Dynamic Control Systems*. For Type I and Type II DCSs, present and/or refer to appropriate **stability** studies analyzing the consequences of failure or misoperation in accordance with the Joint Working Group (JWG)-1 report, "Technical Considerations and Suggested Methodology for the Performance

Evaluation of Dynamic Control Systems". A Comprehensive Review should address all potentially impactful existing and new DCSs, but an Intermediate Review may focus on new DCSs and only those existing DCSs that may have been impacted by system changes since they were last reviewed.

j) Review of Exclusions to the Directory#1 *Criteria*

Review any exclusions granted under NPCC *Guidelines for Requesting Exclusions to Simultaneous Loss of Two Adjacent Transmission Circuits on a Multiple Circuit Tower* (Appendix E). A Comprehensive Review should address all exclusions, but an Intermediate Review may focus on just those exclusions that may have been impacted by system changes since they were last reviewed.

k) Overview Summary of System Performance for Year Studied

6.0 Format of Presentation - Interim Review

a) Introduction of Interim Review

b) Reference the most recent Comprehensive Review and any subsequent Intermediate or Interim Reviews as appropriate.

c) Changes in Facilities (Existing and Planned) and Forecasted System Conditions Since the Last Comprehensive Review.

- **Load** Forecast
- Generation **Resources**
- **Bulk Power System elements**
- Transmission Facilities
- **Special Protection Systems**
- Dynamic Control Systems
- Exclusions

d) Brief Impact Assessment and Overview Summary

The Planning Coordinator will provide a brief assessment of the impact of these changes on the **reliability** of the interconnected **bulk power system**, based on engineering judgment and internal and joint system studies as appropriate.

7.0 Documentation

The documentation required for a Comprehensive or Intermediate Review should be in the form of a report addressing each of the items of the above presentation format. The report should be accompanied by the Planning Coordinator's **bulk power system** map and one-line diagram, summary tables, figures, and appendices, as appropriate. The report may include references to other studies performed by the Planning Coordinator or by utilities within the Planning Coordinator Area that are relevant to the Area Transmission Review, with appropriate excerpts from those studies.

The documentation required for an Interim Review should be in the form of a short summary report (normally not exceeding 5 pages), containing a description of system changes and a brief assessment on their impact on the **reliability** of the interconnected **bulk power system**

8.0 Task Force Follow-Up Procedures

8.1 Once a Planning Coordinator has presented its Transmission Review report to the TFSS, TFSS will review the Planning Coordinator's report and any supporting documentation and consider whether to accept the report as complete and in full conformance with these Guidelines :

a. If the report is found to be unacceptable, TFSS will indicate to the Planning Coordinator the specific areas of deficiency, and request the Planning Coordinator to address those deficiencies.

b. If there is no concurrence about the results and conclusion(s) of the Planning Coordinator's Review, TFSS will indicate to the Planning Coordinator the specific areas of disagreement, and work with the Planning Coordinator to try to achieve concurrence. If agreement has not been reached within a reasonable period of time, TFSS will prepare a summary of the results of its review, and present the summary to the TFCP.

c. If the report is considered as complete and in full conformance with these Guidelines, TFSS will accept the report.

8.2 If the Area Transmission Review indicates an overall **bulk power system** reliability concern (not specific to the Planning Coordinator's planned bulk power transmission system), TFSS will consider what additional studies may be necessary to address the concern, and prepare a summary discussion and recommendation to the Task Force on Coordination of Planning

8.3 Upon completion of an Area Review, TFSS will report the results of the review to the Task Force on Coordination of Planning. The TFCP will then review and vote on the completeness and acceptability of the Area Transmission Review and report its finding to the Reliability Coordinating Committee for a final review and approval.

Appendix C - Procedure for Testing and Analysis of Extreme Contingencies

1.0 Introduction

Extreme **Contingencies** (ECs) are tested "as a measure of system strength" in order to identify potential patterns of weakness in the bulk power transmission system. This procedure for the testing and analysis of ECs should be used when testing ECs for NPCC studies or studies submitted for NPCC review.

This procedure applies to transmission planning studies that consider the overall performance of the interconnected systems of the NPCC Planning Coordinator Areas. It principally applies to NPCC - wide studies of the **bulk power system** and generally does not apply to studies normally conducted by NPCC Transmission Planner and Planning Coordinators that concentrate on individual or a limited number of facilities. This procedure also applies to Area Transmission Reviews, and may be applicable to other studies conducted by the Transmission Planner and Planning Coordinators, and even to individual facility investigations, where such studies and investigations consider the overall performance of the interconnected systems of the NPCC Planning Coordinator Areas. Certain Transmission Planners or Planning Coordinators may elect to completely mitigate the effects of specific ECs.

Finally, this procedure should be followed in multi-regional studies in which NPCC is an active participant, to the extent that this is within the scope of such multi-regional efforts.

2.0 Choosing Contingencies for Testing

The ECs are defined as per **Requirement R9.** Testing should focus on those ECs expected to have the greatest potential effect on the interconnected system. Particular attention should be paid to **contingencies** which would result in major angular power shifts, e.g., interruption of shorter transmission paths carrying heavy power flows, leaving longer transmission paths as the only remaining paths. Additionally, **contingencies** which would result in reversal of major power transfers, e.g. loss of major ties in a neighboring region or Area when said region or Area was transferring power away from the area of interest, should be considered for their impact in subjecting the system to severe power swings. In considering specific **contingencies** to be investigated in an NPCC study, all relevant testing done at the Transmission Planner and Planning Coordinator level should first be reviewed.

In general, a **contingency** in a particular Planning Coordinator Area should be studied, if requested by any other Transmission Planner or Planning Coordinator, based on a reasonable surmise that the requesting Entity may be adversely affected.

3.0 Modeling Assumptions

As referenced in Table 2, performance assessment “i” for **R9**, the assumed generation dispatch, transfers levels, load levels and **load** representation are major considerations in EC tests. It is not the intent to test the worst imaginable extreme, but EC tests should be severe.

The specification of appropriate **load** representation applies to long term stability tests or post-transient power flows as well as **transient stability** tests.

4.0 Evaluating Individual Test Results

A question in evaluating the results of a particular test run is - “Does the system "pass" or "fail" for this **contingency**?” While in the final analysis this is a matter of informed engineering judgment, factors which should be considered include:

1. Lines or transformers loaded above **short time emergency ratings**,

2. Buses with voltage levels in violation of **applicable emergency limits**, (which vary depending on the location within the system),

3. Magnitude and geographic distribution of such overloads and voltage violations across the system,

4. Transient generator angles, frequencies, voltages and power,

5. Operation of Dynamic Control Systems and **Special Protection Systems** (**SPS**),

6. Oscillations that could cause generators to lose synchronism or lead to dynamic instability,

7. Net loss of source resulting from any combination of loss of synchronism of one or more units, generation rejection or runback initiated by SPS, or any other defined system separation,

8. Identification of the extent of the Planning Coordinator Area (s) involved for any indicated instability or islanding (the involvement of more than one Planning Coordinator Area, should be a major consideration),

9. **Relay** operations or the proximity of apparent impedance trajectories to **relay** trip characteristics,

10. The angle across opened breakers,

11. Adequacy of computer simulation models and data.

Finally, a judgment should be attempted as to whether a "failure" is symptomatic of a basic system weakness, or just sensitivity to a particular EC. For example, should failures turn up for several EC tests in a particular part of the system, it is likely that a basic system weakness has been identified.

The loss of portions of the system should not necessarily be considered a failed result, provided that these losses do not jeopardize the integrity of the overall BPS.

NPCC study groups should avoid characterizations like "successful" and "unsuccessful" when commenting on individual runs. Rather, the specific initial conditions directly causing or related to the failure, the complete description of the nature of the failure (e.g., voltage collapse, instability, system separation, as well as the facilities involved), and the extent of potential impact on other Planning Coordinator Areas should be reported.

5.0 Evaluating the Results of EC Tests

EC test reports should focus on those portions of the system in which basic system weaknesses may be developing, rather than on the results of one specific **contingency**.

Any patterns of weaknesses should be identified, which may include reference to earlier NPCC studies and/or Transmission Planner, Planning Coordinator or member system investigations. There is also a need to distinguish between a "failed" test which indicates sensitivity only to a particular **contingency** run and a "failed" test which indicates a more general system weakness (always keeping in mind the severity of possible consequences of the **contingency**). Actions taken by member systems, Transmission Planners or Planning Coordinators to reduce the probability of occurrence or mitigate the consequences of the **contingency** should also be cited.

NPCC follow-up, after publication of a final report, is appropriate only for instances of possible general system weakness. In these instances, the results should be specifically referred to the affected Transmission Planner(s) or Planning Coordinator(s) for further and more detailed investigation with subsequent reporting to NPCC.

Appendix D - Guidelines for Area Review of Resource Adequacy

1.0 Introduction

NPCC has established a Reliability Assessment Program to bring together work done by the NPCC and Planning Coordinators relevant to the assessment of **bulk power system reliability**. As part of the Reliability Assessment Program, each Planning Coordinator submits to the Task Force on Coordination of Planning its Area Review of Resource Adequacy, which is an annual assessment to demonstrate that the proposed resources of each NPCC Planning Coordinator will meet NPCC resource adequacy planning requirements, consistent with these guidelines. The Task Force is charged, on an ongoing basis, with reviewing and recommending NPCC Reliability Coordinating Committee approval of these reviews of **resource** adequacy of each Planning Coordinator Area of NPCC.

The NPCC role in monitoring conformance with the NPCC Directory #1 - *Design and Operation of Bulk Power System* is essential because under this criterion, each Planning Coordinator determines its resource requirements by considering interconnection assistance from other Planning Coordinators, on the basis that adequate **resources** will be available in those Planning Coordinator Areas. Because of this reliance on interconnection assistance, inadequate **resources** in one Planning Coordinator Area could result in adverse consequences in another Planning Coordinator Area.

It is recognized that all Planning Coordinators may not necessarily express their own **resource** adequacy criterion as stated in Requirements R4, R5, and R6 of the Directory #1 criteria. However, the Directory #1 criteria provide a reference point against which a Planning Coordinator's **resource** adequacy criterion can be compared.

2.0 Purpose of Presentation

The purpose of the presentation associated with a resource adequacy review is to show that each Planning Coordinator's proposed resources are in accordance with the NPCC Directory #1 - Design and Operation of the Bulk Power System. By such a presentation, the Task Force will satisfy itself that the proposed resources of each NPCC Planning Coordinator will meet the NPCC Resource Adequacy Requirements, as defined NPCC Directory #1, over the time period under consideration.

3.0 Format of Presentation and Report – Comprehensive Review

Each Planning Coordinator should include in its presentations and in the accompanying report documentation, as a minimum, the information listed below. At its own discretion,

the Planning Coordinator may discuss other related issues not covered specifically by these guidelines.

3.1 Executive Summary

3.1.1 Briefly illustrate the major findings of the review.

3.1.2 Provide a table format summary of major assumptions and results.

3.2 Table of Contents

3.2.1 Include listing of all tables and figures.

3.3 Introduction

3.3.1 Reference the previous NPCC Area Review.

3.3.2 Compare the proposed resources and load forecast covered in this NPCC review with that covered in the previous review

3.4 Resource Adequacy Criterion

3.4.1 State the Planning Coordinator's resource adequacy criterion.

3.4.2 State how the Planning Coordinator criterion is applied; e.g., load relief steps.

3.4.3 Summarize resource requirements to meet the criteria for the time period under consideration. If interconnections to other Planning Coordinators and regions are considered in determining this requirement, indicate the value of the interconnections in terms of megawatts. In the calculation of available **resources**, supply- side resources from neighboring systems are limited to firm capacity backed purchases.

3.4.4 Provide either an estimate of the resources required to meet the NPCC criteria or a statement as to the comparison of the two criteria, if the Planning Coordinator criterion is different from the NPCC criterion

3.5 Resource Adequacy Assessment

3.5.1 Evaluate proposed resources versus the requirement to reliably meet projected electricity demand assuming the Planning Coordinator's most likely load forecast.

3.5.2 Evaluate proposed resources versus the requirement to reliably meet projected electricity demand assuming the Planning Coordinator's high load growth scenario.

3.5.3 Describe load and resource uncertainties on projected Planning Coordinator Area reliability and describe mechanisms to mitigate anticipated material adverse effects on reliability.

3.5.4 Describe anticipated effects from proposed major changes to market rules on Planning Coordinator Area reliability.

3.5.5 Summarize resource adequacy studies conducted since the previous Area Review, as appropriate

3.6 ~~Proposed Resource Capacity Mix~~ Reliability Impacts Due to Environmental Regulations and Fuel Supply Issues.

3.6.1 Discuss anticipated material adverse effects on reliability resulting from the proposed resources fuel supply and transportation. ~~or environmental considerations~~.

3.6.2 Discuss anticipated reliability impacts related to an Area's compliance with State, Federal or Provincial requirements (such as environmental, renewable energy, or greenhouse gas reductions).

3.7 Mitigation Measures for Environmental Regulations and Fuel Supply Issues

~~3.6.2~~3.7.1 Describe available mechanisms to mitigate anticipated reliability impacts of resource fuel supply, demand resource response, fuel transportation issues and/or environmental considerations.

~~Discuss anticipated reliability impacts related to an Area's compliance with State, Federal or Provincial requirements (such as environmental, renewable energy, or greenhouse gas reductions).~~

4.0 Format of Presentation and Report – Annual Interim Review

The Annual Interim Review should include a reference to the most recent Comprehensive Review; a listing of major changes in: facilities and system conditions, load forecast, generation resources availability; related fuel supply and transportation information, environmental considerations, demand response programs, transfer capability and emergency operating procedures. In addition, the assessment should also include a comparison of major changes in market rules, implementation of new rules, locational requirements, and installed capacity requirements. Finally, the report should include a

brief impact assessment and an overall summary.

The Planning Coordinator will provide a brief assessment of the impact of these changes on the reliability of the interconnected bulk power system. This assessment should be based on engineering judgment, internal system studies and appropriate joint interconnected studies. To the extent that engineering judgment or existing studies can be used to clearly demonstrate that a Planning Coordinator Area is expected to meet the NPCC resource adequacy criterion, detailed system LOLE studies are not required.

The documentation for the Annual Interim Review should be in the form of a summary report (normally not exceeding three to five pages.)

Sections A and B should describe the reliability model and program used for the resource adequacy studies discussed in Section 3.5. Section C should describe the Task Force follow-up procedures.

A. Description of Resource Reliability Model

1.1 Load Model

1.1.1 Description of the **load** model and basis of period **load** shapes.

1.1.2 How **load** forecast uncertainty is handled in model.

1.1.3 How the electricity demand and energy projections of interconnected entities within the Planning Coordinator Area that are not members of the Planning Coordinator Area are addressed.

1.1.4 How the effects (demand and energy) of demand-side management programs (e.g., conversion, interruptible demand, direct control **load** management, demand (**load**) response programs) are addressed.

1.2 Supply Side Resource Representation

1.2.1 Resource Ratings

1.2.1.1 Definitions.

1.2.1.2 Criteria for verifying **ratings**. Reference NPCC Directory#9 Verification of Gross and Net Real Power Capability and Directory#10 Verification of Gross and Net Reactive Power Capability.

1.2.2 Unavailability Factors Represented

1.2.2.1 Type of unavailability factors represented; e.g., forced outages, planned outages, partial derating, etc.

1.2.2.2 Source of each type of factor represented and whether generic or individual unit history provides basis for existing and new units

1.2.2.3 Maturity considerations, including any possible allowance for in-service date uncertainty.

1.2.2.4 Tabulation of typical unavailability factors.

1.2.3 Purchase and Sale Representation

1.2.3.1 Describe characteristics and level of dependability of transactions.

1.2.4 Retirements.

1.2.4.1 Summarize proposed retirements.

1.3 Representation of Interconnected System in Multi-Area Reliability Analysis, including which Planning Coordinator Areas and regions are considered, interconnection capacities assumed, and how expansion plans of other Planning Coordinators and regions are considered.

1.4 Modeling of Variable and Limited Energy Sources.

1.5 Modeling of Demand Side Resources and Demand (Load) Response Programs.

1.5.1 Description should include how such factors as in-service date uncertainty, **rating**, availability, performance and duration are addressed.

1.6 Modeling of all Resources.

1.6.1 Description should include how such factors as in-service date uncertainty; capacity value, availability, **emergency** assistance, scheduling and deliverability are addressed.

1.7 Other assumptions i.e., internal transmission limitations, maintenance over-runs, fuel supply and transportation and environmental constraints.

1.8 Incorporate the reliability impacts of market rules.

B. Other Factors, If Any, Considered in Establishing Reserve Requirement Documentation

The documentation required to meet the requirements of the above format should be in the form of summaries of studies performed within a Planning Coordinator Area, including references to applicable reports, summaries of reports or submissions made to regulatory agencies.

C. Task Force Follow-Up Procedures

Once a specific Planning Coordinator has made a presentation or a series of presentations to the Task Force on Coordination of Planning, the latter shall:

1.1 Prepare a brief summary of key issues discussed during the presentation.

1.2 Note where further information was requested and the results of such further interrogations.

1.3 Note the specific items that require additional study and indicate the responsibilities for undertaking these studies.

1.4 Recommend to the Reliability Coordinating Committee whether the Resource Adequacy Review is suitable for approval.

Appendix E - Guidelines for Requesting Exclusions to Simultaneous Loss of Two Adjacent Transmission Circuits on a Multiple Circuit Tower.

1.0 Introduction

Directory #1 allows for requests for exclusion from the simultaneous loss of two adjacent transmission circuits on multiple circuit towers on the basis of acceptable risk. All exclusions must be reviewed by the applicable Task Forces and approved by the Reliability Coordinating Committee (RCC). An acceptance of a request for exclusion is dependent on the successful demonstration that such exclusion is an acceptable risk. These guidelines describe the procedure to be followed and the supporting documentation required when requesting exclusion, and establishes a procedure for periodic review of exclusions of record.

2.0 Documentation

The documentation supporting a request for exclusion to the Criteria includes the following:

2.1 A description of the facilities involved, including geographic location, length and type of construction, and electrical connections to the rest of the interconnected power system;

2.2 Relevant design information pertinent to the assessment of acceptable risk, which might include: details of the construction of the facilities, geographic or atmospheric conditions, or any other factors that influence the risk of sustaining the loss of adjacent transmission circuits on a multiple circuit tower;

2.3 An assessment of the consequences of the loss of adjacent transmission circuits on a multiple circuit tower, including, but not limited to, a discussion of levels of exposure and probability of occurrence of **significant adverse impact** on the **bulk power system** ;

2.4 For existing facilities, the historical outage performance, including cause, for such **contingencies** on the specific facility (facilities) involved as compared to that of other multiple circuit tower facilities;

2.5 For planned facilities, the estimated frequency of adjacent transmission circuit multiple circuit tower **contingencies** based on the historical performance of facilities of similar construction located in an area with similar geographic climate and topography.

3.0 Procedure for obtaining an Exclusion

The following procedure is used to obtain an exclusion:

3.1 The entity requesting the exclusion (the Requestor) submits the request and supporting documentation to the Task Force on System Studies (TFSS) after acceptance has been granted by the Requestor's own Planning Coordinator, if such process is applicable.

3.2 TFSS reviews the request, verifies that the documentation requirements have been met, and determines the acceptability of the request.

3.3 If TFSS deems the request acceptable, TFSS requests the Task Force on Coordination of Planning (TFCP), the Task Force on Coordination of Operation (TFCO), and the Task Force on System Protection (TFSP) to review the request. The Requestor provides copies of the request and supporting documentation to the other Task Forces as directed by TFSS. If additional information is requested by the other Task Forces as part of their assessment, the Requestor provides this information directly to the interested Task Force, with a copy to the TFSS. The other Task Forces review the request and indicate their acceptance or non-acceptance to TFSS.

3.4 If all Task Forces deem the request for exclusion acceptable, the TFSS will forward a recommendation for approval to the RCC.

3.5 Exclusion requests will be effective upon approval by the RCC.

NPCC Directory #1
Appendix F

Appendix F – Procedure for Operational Planning Coordination

1.0 Introduction

The Reliability Coordinators (RC) of the Northeast Power Coordinating Council, Inc. (NPCC) require access to the security data specified in this procedure in order to adequately assess the reliability of the NPCC **bulk power system**. All users of the electric systems, including market participants, should supply such data to the NPCC Reliability Coordinators. Coordination among and within the Reliability Coordinator Areas (RC Area) of NPCC is essential to the reliability of interconnected operations. Timely information concerning system conditions should be transmitted by the NPCC RC Areas to other RC Areas as needed to assure reliable operation of the **bulk power system**. One aspect of this coordination is to ensure that adjacent RC Areas and neighboring systems are advised on a regular basis of expected operating conditions, including generator, transmission and system **protection**, including Type I **special protection system,** outages that may materially reduce the ability of an RC Area to contribute to the reliable operation of the interconnected system, or to receive and/or render assistance to another RC Area. To the extent practical, the coordination of outage schedules is desirable in order to limit the severity of such impacts.

To ensure that there is effective coordination for system **reliability** concerns, this document establishes procedures for the exchange of information regarding load/capacity forecasts, including firm sales and firm purchases, generator outage schedules, and transmission outage schedules for those **elements** that may have an adverse impact on other RC Area(s). It also details general action that may be taken to improve the communication of problems as well as specific topics that may be discussed in regularly scheduled conference calls or ad -hoc conference calls arranged in anticipation of problems such as capacity deficiency or inadequate light load margin in one or more RC Areas.

NPCC participants and other recipients of the information provided by processes in this guideline should adhere to the NPCC Critical Energy Infrastructure Information Non – Disclosure agreement.

2.0 Load/Capacity Forecasts

2.1 Twice yearly by May 15th and November 15th respectively, the Operations Planning Working Group (CO 12) will perform a summer and winter assessment for the next season.

The results will be reviewed by the NPCC TFCO and the NPCC Reliability Coordinating Committee (RCC) ~~in advance~~during the ~~of the~~ spring and autumn meetings of both groups and documented in the summer and winter NPCC Reliability Assessment reports.

2.2 Each week, each RC Area will review its weekly net resource capacity margin, as defined in Attachment A, for the twelve weeks to follow and forward the information to the NPCC Staff for distribution to all NPCC RC Areas. If an NPCC RC Area identifies a deficiency or light load condition, the RC Area should identify the cause(s) and mitigation measures that have been implemented, or will be implemented, to manage the issue.

3.0 Generator Outage Coordination

3.1 Each RC Area should exchange current and expected generator outages that may have a significant impact on an adjacent RC Area or neighboring systems or a significant impact on the transfer capability between RC Areas.

4.0 Transmission Outage Coordination

4.1 Advance Planning of Transmission Facility Outages

Each RC should exchange critical transmission **element** outages as identified in the coordination agreements with their interconnected neighbors, **elements** identified on the Facilities Notification List and multiple transmission **element** outages that may have an adverse impact on external energy transfers. Each Reliability Coordinator shall minimize the duration of outages to facilities that impact inter-Reliability Coordinator Areas.

4.2 Facilities Notification List

The NPCC Facilities Notification List, Attachment D, has two components:

1) the NPCC Transmission Facilities Notification List; and
2) the list of NPCC Type I **special protection systems**.

The Facilities Notification List is developed by each RC Area and specifies all facilities that, if removed from service, may have a significant, direct or indirect impact on another RC Area's transfer capability. The cause of such impact might include stability, voltage, and/or thermal considerations.

Prior to October 1st of each year, each RC Area will review and update its Facilities Notification List and coordinate necessary changes with other appropriate NPCC RC Areas. Prior to January 1st, and after review by the TFCO, the jointly developed, updated and approved Facilities Notification List will be posted on the NPCC secure website.

It should be noted that revisions to the Facilities Notification List will not follow the NPCC Process for Open Review due to the secure nature of the information

contained, and Attachment D is not openly published with this Procedure.

A temporary reconfiguration of the network may result in an outage to one or more facilities not listed in Attachment D having an impact on other NPCC RC Areas. It is the responsibility of the RC experiencing the condition to notify impacted RCs in a timely manner and provide updated status reports during the condition.

4.3 Notifications of Transmission **Element** Outages:

4.3.1 Notification requirements for Transmission **Element** Outages should be defined in interconnection coordination agreements. The time frames identified below are the minimum notification requirements.

4.3.2 Reliability Coordinators will advise affected RCs of all planned and unplanned outages of **elements** on the Facilities Notification List and those multiple transmission **element** outages that may have an adverse impact on external energy transfers.

All outages to equipment listed in the Facilities Notification List and those multiple transmission **element** outages that may have an adverse impact on external energy transfers should be planned with as much advance notice as practical.

Normally, notification for outages on **elements** covered by this instruction will be submitted to the appropriate RC Areas at least two (2) working days prior to the time the **element** is to be taken out of service.

When an RC Area receives an outage notification from another RC Area, prompt attention will be given to the notification and appropriate comments rendered.

4.3.3 An RC Area will not normally remove from service any transmission **elements,** which might have a **reliability** impact on an RC Area without prior notification to and appropriate review by that RC Area. In the event of an **emergency** condition, each RC Area may take action as deemed appropriate. Other RC Areas should be notified immediately.

An RC Area will make every effort to reschedule routine (non-emergency) transmission outages that severely degrade the reliability of an adjacent RC Area or neighboring system.

4.3.4 Each RC Area will advise the other affected RC Areas of any **protection** outage associated with RC Area tie line facilities Coordination agreements may identify additional reporting requirements associated with **protection** outages.

5.0 Specific Communications

Conditions in an RC Area that may have an impact on another RC Area should be communicated in a clear and timely manner. Specific communications are conducted as follows:

5.1 Weekly

Each Thursday a conference call will be initiated by the NPCC Staff to discuss operations expected during the seven-day period starting with the following Sunday. Operations personnel from the NPCC RC Areas and, as necessary, adjacent RC Areas will participate. In advance of the conference call, each RC Area will prepare the data specified in Attachments A and B, and forward it to the NPCC Staff a minimum of one hour in advance of the scheduled call. The completed "NPCC Weekly Conference Call Generating Capacity Worksheet," Attachment B, together with the list of "Twelve Weeks Projections of Net Margins," will be forwarded to the conference call participants by the NPCC Staff.

Each RC will review its weekly capacity margins for the next twelve week period. If a deficiency or light load condition is identified, the RC will identify the cause of the deficiency or light load condition and discuss proposed mitigation measures.

The NPCC Staff will prepare Conference Call Notes that will be forwarded to the conference call participants and members of the TFCO by the following Friday afternoon.

Items of particular concern that should be ~~discussed~~ addressed during the weekly conference call are described in Attachment C.

5.2 Emergency Preparedness Conference Call

Whenever adverse system operating or weather conditions are expected, any RC Area may request the NPCC Staff to arrange an Emergency Preparedness Conference Call (NPCC Document C-01) to discuss operating details with appropriate operations management personnel from the NPCC RC Areas and neighboring systems.

5.3 Daily Conference Calls

Each of the NPCC Reliability Coordinator Area control rooms participate in a regularly scheduled daily conference call. The goal of this call is to alert NPCC Reliability Coordinators of any potential emerging problems. Subjects for discussion are limited to credible events which could impact the ability of a Reliability Coordinator to serve its load and meet its operating reserve obligations, or which would impose a burden to the Interconnection.

Procedure for Operational Planning Coordination – Attachment A

Load and Capacity Table Instructions
and
Generating Capacity Worksheet Instructions

Week Beginning	The seven day period for which data is to be reported is defined as starting with the Sunday following the conference call through the following Saturday.
Installed Generating Capacity (Line Item 1)	Include all available generation at its maximum demonstrated capability for the appropriate seasonal capability period.
~~Independent Power Producers~~Other Generating Capacity ~~(~~(Line Item 2)	Include all available generation not included in Item#1 .~~Any entity that owns or operates an electricity generating facility that is not included in an electric utility's rate base.~~ This item ~~term~~ includes, but is not limited to, co generators,~~ and~~ small power producers and all other nonutility electricity producers, such as exempt wholesale generators~~,~~ who sell electricity
Firm Purchases (Line Item ~~2~~3)	Include only those transactions where capacity is delivered. Exclude "energy only" transactions.
Firm Sales (Line Item ~~3~~4)	Include only those transactions where capacity is delivered. Exclude "energy only" transactions.
Net Capacity (Line Item ~~4~~5)	Add Installed Generating Capacity and Firm Purchases. Subtract Firm Sales. (Line 1+Line 2-Line3)
Peak Load Forecast (Line Item ~~5~~6)	The peak load forecast along with the day during which the peak is expected to occur should be the best estimate of the RC Area's maximum peak load exposure anticipated for the week reported.
Available Reserve (Line Item ~~6~~7)	Subtract Peak Load Forecast from Net Capacity. (Line 4-Line5.)
Demand Side Management (Line Item ~~7~~8)	Include only maximum capability which can be obtained by operator initialization within four (4)

	hours.

Attachment A (continued)	
Known Unavailable Capacity~~bility~~ (Line Item ~~8~~9)	Include all known outages, as well as those deratings or unit outages presently forced out, unavailable, on extended cold standby or which are anticipated to remain out of service. This would also include capacity unavailable due to transmission constraints.
Net Reserve (Line Item ~~9~~10)	Available Reserve plus Demand Side Management minus Known Unavailable Capacity. (Line 6+Line 7-Line 8)
Required Operating Reserve (Line Item 1~~0~~)	The methodology used by each RC Area in calculating operating reserves should, at a minimum, meet the requirements of NPCC Directory # 5, "Reserve." Methodologies differing from the Directory #5 requirements should be clarified in Attachment B, "NPCC Weekly Conference Call Generating Capacity Worksheet," under the tab for "Operating Reserve."
Gross Margin (Line Item 1~~2~~1)	Subtract Required Operating Reserve from Net Reserve. (Line 9-Line 10)
Unplanned Outages (Line Item 1~~3~~2)	Estimate the amount of generating capacity which will be unavailable. This quantity should be based on historical averages for forced outages and deratings.
Net Resource Capacity Margin (Line Item 1~~4~~3)	Subtract Unplanned Outages from Gross Margin. A positive value reflects surplus reserve. A negative value reflects a deficiency. (Line 11-Line 12)
Forecast High / Low Temperatures and Days (Line Item 1~~5~~4)	Include the expected high and low temperatures for the RC Area for the week, and indicate the day on which they are expected to occur.

Attachment A (continued)	
Seasonal High / Low Temperatures (Line Item 165)	Include the expected high and low forecast seasonal temperatures for the RC Area.
Minimum Load Forecast (Line Item 176)	The minimum load forecast, -indicating the day on which it is ~~they are~~ expected to occur should be the best estimate of the RC Area's minimum load exposure anticipated for the week reported.
Minimum Resources (Line Item 187)	The Minimum Resources are the Reliability Coordinator Area's total expected on-line generator minimum output capability and must-take purchases.
Light Load Margin (Line Item 198)	Subtract Minimum Resources from Minimum Load Forecast. A negative number indicates a light load condition. (Line 176-Line 187)

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Auto

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Auto

Procedure for Operational Planning Coordination – Attachment B

NPCC Weekly Conference Call Generating Capacity Worksheet

The "NPCC Weekly Conference Call Generating Capacity Worksheet" is an active spreadsheet used each week to assist in the calculation of the data discussed during the weekly conference call. A blank template is available from the NPCC office.

Procedure for Operational Planning Coordination - Attachment C

CONDITIONS FOR DISCUSSION

Items of particular concern that should be discussed during a conference call can include, but are not limited to, the following:

- anticipated weather;
- largest first and second contingencies;
- operating reserve requirements and expected available operating reserve;
- capacity deficiencies;
- potential fuel shortages or potential supply disruptions which could lead to energy shortfalls;
- light load margins;
- general and specific voltage conditions throughout each system or RC Area;
- status of short term contracts and other scheduled arrangements, including those that impact on operating reserves;
- additional capability available within twelve hours and four hours;
- generator outages that may have a significant impact on an adjacent RC Area or neighboring system;
- transmission outages that may have an adverse impact on external energy transfers;
- potential need for emergency transfers;
- expected transfer limits and limiting elements;
- a change or anticipated change in the normal operating configuration of the system, such as the temporary modification of relay **protection** schemes so that the usual and customary levels of **protection** will not be provided, or the arming of **special protection systems** not normally armed, or the application of abnormal operating procedures; and
- update of the abnormal status of NPCC Type I **special protection systems** forced out of service

Attachment D

NPCC Facilities Notification List

Attachment D is not publicly available due to the confidential nature of the information presented.

Appendix G - Procedures for Inter Reliability Coordinator Area Voltage Control

1.0 Introduction

This Procedure provides general principles and guidance to Reliability Coordinators and Transmission Operators for effective inter- Transmission Operator Area voltage control, consistent with the NPCC, Directory #1, "Design and Operation of the Bulk Power System". Specific methods to implement this Procedure may vary among Reliability Coordinators and Transmission Operators, depending on local requirements. Coordinated inter- Transmission Operator Area voltage control is necessary to regulate voltages to protect equipment from damage and prevent voltage collapse. Coordinated voltage regulation reduces electrical losses on the network and lessens equipment degradation. Local control actions are generally most effective for voltage regulation. Occasions arise when adjacent Reliability Coordinators and Transmission Operators can assist each other to compensate for deficiencies or excesses of **reactive power** and improve voltage profiles and system security.

2.0 Principles

Each Reliability Coordinator and Transmission Operator operates, in accordance with NPCC, Directory #1, "Design and Operation of the Bulk Power System" criteria, their own individual or joint operating policies, procedures and applicable interconnection agreements. Adjacent Reliability Coordinators and Transmission Operator should be familiar with the respective criteria and procedures of their neighboring Reliability Coordinators and Transmission Operator Areas, and should mutually agree upon procedures for inter- Transmission Reliability Coordinator and Operator Area voltage control.

In the event the system state changes to a condition that requires a voltage or reactive corrective action, the Reliability Coordinator and Transmission Operator for the Area in which the condition is originating from should immediately take corrective action. If the corrective control actions are ineffective, or the Reliability Coordinator and Transmission Operator for the Area have insufficient reactive resources to control the problem, assistance may be requested from other Reliability Coordinators and Transmission Operator Areas.

Whether inter- Reliability Coordinator and Transmission Operator Area voltage control is carried out through specific or general procedures, the following should be considered and implemented if applicable:

2.1 To effectively coordinate voltage control, location and placement of metering for **reactive power** resources and voltage controller status should be the same between adjacent Reliability Coordinators and Transmission Operator Areas;

2.2 the availability of **voltage regulating transformers** in the proximity of **tie lines**;

2.3 voltage levels, limits, and regulation requirements for stations on either side of an inter- Reliability Coordinator and Transmission Operator Area interface;

2.4 the circulation of **reactive power** (export at one tie point in exchange for import at another);

2.5 **tie line** reactive losses as a function of active **power** transfer;

2.6 the sharing of the reactive requirements of **tie lines** and series regulating equipment (either equally or in proportion to line lengths, etc.);

2.7 the transfer of **reactive power** from one Reliability Coordinator and Transmission Operator Area to another

2.8 reactive **reserve** of on-line generators;

2.9 shunt reactive device availability and switching strategy;

2.10 **static VAR compensator** availability, reactive **reserve**, and control strategy;

2.11 each Reliability Coordinator and Transmission Operator Area should anticipate voltage trends and initiate corrective action in advance of critical periods of heavy and light **loads.**

2.12 Each Reliability Coordinator and Transmission Operator Area should maintain a mix of static and dynamic resources, including reactive **reserves**

3.0 Procedure for Triennial Monitoring and Reporting of Inter-Area Voltage Control

3.1 On, or shortly before, the first of July, the Task Force Coordination of Operations (TFCO) Secretary will write to each TFCO member, requesting a written response by the end of July in the form of:

a) A copy of any new or revised procedures, principles, or understandings (such as minutes of an operating committee meeting between Reliability Coordinators and Transmission Operator Areas) between the reporting Reliability Coordinator and adjacent Reliability Coordinators~~.~~, or,

b) a response indicating no change to existing procedures, principles, or understandings currently on file at NPCC.

3.2 The TFCO Secretary will summarize the responses and will forward it to TFCO members at least two weeks prior to the October TFCO meeting.

3.3 Following TFCO review and acceptance of the responses, the TFCO Chairman will forward the summary to the Chairman of the Reliability Coordinating Committee (RCC) for informational purposes. This will normally be forwarded three weeks prior to the next regularly scheduled RCC meeting.

NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

DRAFT 15: May 22nd, 2014
Regional Reliability Reference Directory # 1
Design and Operation of the Bulk Power System

Task Force on Coordination of Planning Revision Review Record:

Clean

CO7/CP11 Revisions to Draft
Based on Open Process Comments

Adopted by the Members of the Northeast Power Coordinating Council, Inc., on December 01, 2009 based on recommendation by the Reliability Coordinating Committee, in accordance with Section VIII of the NPCC Amended and Restated Bylaws dated July 24, 2007 as amended to date.

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

Revision History

Version	Date	Action	Change Tracking (New, Errata or Revisions)
0	December 1, 2009		New
1	4/20/2012	Errata Changes in Appendices B and E.	Errata

Table of Contents

1.0 Introduction 4
1.1 Title: Design and Operation of the Bulk Power System 4
1.2 Directory Number: 1 4
1.3 Objective: 4
1.4 Effective Date: December 1, 2009 4
1.5 Background 4
1.6 Applicability 4
1.6.1 Functional Entities 4
1.6.2 Applicability of NPCC Criteria: 5

2.0 Defined Terms: 5

3.0 NPCC Full Member, More Stringent Criteria: 6

4.0 Compliance: 11

Table 1 - Planning Design Criteria, Contingency events, Fault type, Performance requirements

Table 2 - Planning Criteria: Extreme Contingency and System Conditions, Fault type, Performance assessments

Table 3 - Operating Criteria**,** Contingency events, Fault type, Performance requirements

Appendix A - Reserved for Future Use

Appendix B - Guidelines and Procedures for NPCC Area Transmission Review

Appendix C - Procedure for Testing and Analysis of Extreme Contingencies

Appendix D - Guidelines for Area Review of Resource Adequacy

Appendix E - Guidelines for Requesting Exclusions to Simultaneous Loss of Two Adjacent Transmission Circuits on a Multiple Circuit Tower

Appendix F - Procedure for Operational Planning Coordination

Appendix G - Procedures for Inter Reliability Coordinator Area Voltage Control

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

1.0 Introduction

1.1 Title: Design and Operation of the Bulk Power System

1.2 Directory Number: 1

1.3 Objective:

The objective of this Directory is to provide a "design-based approach" to design and operate the **bulk power system** to a level of reliability that will not result in the loss or unintentional separation of a major portion of the system from any of the contingencies referenced in **R7** and **R14.** The intent of this approach is to avoid instability, voltage collapse and widespread cascading outages. Loss of small portions of a system (such as radial portions) may be tolerated provided these do not jeopardize the reliability of the remaining **bulk power system**.

In NPCC the technique for achieving this level of reliability is to require that the **bulk power system** be designed and operated to meet the performance requirements for the representative **contingencies** as specified in this Directory. Simulations shall be used to assess and analyze these **contingencies. Contingency** events shall be applied on **bulk power system** elements and the resulting performance requirements shall be monitored on the **bulk power system.**

The characteristics of a reliable **bulk power system** include adequate **resources** and transmission to reliably meet projected customer electricity demand and energy requirements as prescribed in this document.

1.4 Effective Date: December 1, 2009

1.5 Background

This Directory was developed from the NPCC A-2 criteria document - *Basic Criteria for the Design and Operation of Interconnected Power Systems* (May 6, 2004 version). Guidelines and Procedures for consideration in the implementation of this Directory are provided in the Appendices.

1.6 Applicability

1.6.1 Functional Entities

Reliability Coordinators
Transmission Operators
Balancing Authorities
Planning Coordinators
Transmission Planners

Resource Planners
Generator Owners
Transmission Owners

1.6.2 Applicability of NPCC Criteria:

The requirements of an NPCC Directory apply only to those facilities defined as NPCC **bulk power system** elements and identified through the performance based methodology of NPCC Document A-10, "*Classification of Bulk Power System Elements*," the list of which is maintained by the NPCC Task Force on System Studies and approved by the NPCC Reliability Coordinating Committee."

Requirements to abide by an NPCC Directory may also reside in external tariff requirements, bilateral contracts and other agreements between facility owners and/or operators and their assigned Reliability Coordinator, Planning Coordinator, Transmission Operator, Balancing Authority and/or Transmission Owner as applicable and may be enforceable through those external tariff requirements, bilateral contracts and other agreements. NPCC will not enforce compliance to the NPCC Directory requirements in this document on any entity that is not an NPCC Full Member.

2.0 Defined Terms:

Unless specifically noted in this document terms in bold typeface are defined in the NPCC Glossary of Terms.

3.0 NPCC Full Member Criteria:

Information for Planning and Operational Assessments

R1 Each Functional Entity that owns equipment shall submit verified information representing the physical or control characteristics of its equipment for system modelling and reliability analysis of the **bulk power system**.

R2 Each Planning Coordinator and Reliability Coordinator shall collect and maintain information needed for system modelling and reliability analysis of the **bulk power system** as submitted in accordance with Requirement R1.

R2.1 This information shall be submitted to NPCC upon request.

R3 Each Reliability Coordinator shall share and coordinate forecast system information d real-time information to enable and enhance the analysis and modeling of the interconnected **bulk power system** by security application software on energy management systems.

Resource Adequacy

R4 Each Planning Coordinator or Resource Planner shall probabilistically evaluate resource adequacy of its Planning Coordinator **Area** portion of the **bulk power system** to demonstrate that the loss of **load** expectation (LOLE) of disconnecting **firm load** due to resource deficiencies is, on average, no more than 0.1 days per year.

R4.1 Make due allowances for demand uncertainty, scheduled outages and deratings, forced outages and deratings, assistance over interconnections with neighboring Planning Coordinator **Areas**, transmission transfer capabilities, and capacity and/or load relief from available operating procedures.

R5 Each Planning Coordinator shall report and obtain Reliability Coordinating Committee (RCC) approval for its Review of **Resource** Adequacy. Appendix D provides guidance for the Area Review of **Resource** Adequacy.

R5.1 The Review of **Resource** Adequacy will be presented to the NPCC Task Force on Coordination of Planning (TFCP). Comprehensive and Interim reviews shall be presented to the TFCP before the beginning of the first time period covered by the assessment.

R5.2 A Comprehensive Review of **Resource** Adequacy is required every three years and will cover a time period of five years. If changes in planned

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

facilities or forecasted system conditions warrant, TFCP may require a Comprehensive Review of **Resource** Adequacy in less than 3 years.

R5.3 In subsequent years, each Planning Coordinator shall conduct an Annual Interim Review of **Resource** Adequacy that will cover, at a minimum, the remaining years studied in the Comprehensive Review of **Resource** Adequacy.

R6 Each Reliability Coordinator shall coordinate outages and deratings of **resources** to verify adequate **resources** will be available to meet the forecasted demand and **reserve** requirements. Appendix F provides guidance for Operational Planning Coordination.

R6.1 A Summer and Winter Reliability Assessment will be presented to the NPCC Task Force on Coordination of Operation (TFCO) every year.

Transmission Planning

R7 Each Transmission Planner and Planning Coordinator shall plan the system to meet the respective performance requirements for the **contingencies** as specified in Table 1 in the design of its **bulk power system**.

R7.1 Credible combinations of system conditions which stress the system shall be modelled including, load forecast, inter-Area and intra-Area transfers, transmission configuration, active and reactive resources, generation availability and other dispatch scenarios.

R8 Each Transmission Planner and Planning Coordinator shall assess the impact of the extreme **contingencies** listed in Table 2. Appendix C provides guidance for testing and analyzing extreme contingencies.

R9 Each Transmission Planner and Planning Coordinator shall assess the impact of extreme system conditions, one condition at a time, subject to contingencies as listed in the “Extreme System Conditions” category of Table 2.

R10 Each Transmission Planner and Planning Coordinator shall have procedures and implement a system design that ensures equipment capabilities are adequate for fault current levels with all transmission and generation facilities in service for all operating conditions which are not prohibited by a procedure and coordinate these procedures with materially affected Transmission Planner and Planning Coordinator Areas.

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

R11 Each Planning Coordinator shall conduct and obtain Reliability Coordinating Committee (RCC) approval for its Transmission Review. Appendix B provides guidance for Transmission Reviews.

R11.1 A Comprehensive Transmission Review is required at least once every five years or if major or pervasive system changes have occurred. If changes in the planned facilities or forecasted system conditions warrant, the Task Force on System Studies (TFSS) may require a Comprehensive Transmission Review in less than five years.

R11.2 The proposal for the type of annual Transmission Review shall be presented to TFSS by March of the year during which the review is conducted. Approval for the type of Transmission Review shall be obtained from the TFSS. The annual Transmission Review shall be presented to the TFSS by April of the following year.

R11.3 If the results of the Transmission Review indicate that the planned **bulk power system** will not be in conformance with NPCC Directory #1, the Transmission Review shall incorporate a corrective action plan to achieve conformance.

Special Protection Systems

R12 Each Functional Entity that proposes a new or modified SPS shall consider the complexity of the scheme and the consequences of correct or incorrect operation as well as its benefits.

R12.1 Provide a rationale and justification to the TFCP including factors such as project delays, temporary construction configurations, unusual combinations of system conditions, equipment outages and infrequent contingencies.

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

Transmission Operation

R13 Each Reliability Coordinator and Transmission Operator shall establish **normal transfer capabilities** and **emergency transfer capabilities, for** its portion of the **bulk power system** to meet the respective performance requirements for the **contingencies** as specified in Table 3.

R14 Each Reliability Coordinator and **Transmission** Operator shall operate to **normal transfer capabilities** unless an **emergency,** in accordance with NPCC Directory# 2, is identified.

R15 Each Reliability Coordinator and Transmission Operator shall make system adjustments once an **emergency** has been identified, including the pre-**contingency** disconnection of **firm load,** to avoid exceeding **emergency transfer capabilities.**

R16 Each Reliability Coordinator and Transmission Operator shall assess the status of the **bulk power system** immediately after the occurrence of any **contingency** and prepare for the next **contingency as specified in Table 3**.

R16.1 Voltage reduction and shedding of firm load shall be deployed to return the system to a secure state, if other system adjustments are not adequate. Voltage reduction need not be initiated and firm load need not be shed to observe a post contingency loading requirement until the **contingency** occurs, provided that adequate response time for this action is available.

R16.2 System adjustments shall be completed as quickly as possible following any **contingency,** but within 30 minutes after the occurrence of any **contingency** specified in Table 3.

R17 Each Reliability Coordinator shall notify the applicable Reliability Coordinators of forced outages of any facility as per the NPCC Transmission Facilities Notification List and of any other condition which may impact inter-Area reliability.

R18 Each Reliability Coordinator shall coordinate scheduled outages of facilities that are on the NPCC Transmission Facilities Notification List sufficiently in advance of the outage to permit the affected Reliability Coordinators to maintain reliability. Appendix F provides guidance for Operational Planning Coordination.

R18.1 Review and update its Facilities Notification List and submit the list to the NPCC Task Force on Coordination of Operation (TFCO) annually.

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

R19 Each Reliability Coordinator shall coordinate voltage control between Transmission Operator Areas. Appendix G provides guidance for Inter- Reliability Coordinator Area Voltage Control.

R19.1 Metering for **reactive power** resources and voltage controller status shall be consistent between adjacent Transmission Operators.

R19.2 Upon request from the TFCO, perform an Inter-Area Voltage Control Assessment.

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

4.0 Compliance:

Compliance with the requirements set forth in this Directory will be in accordance with the NPCC Criteria Compliance and Enforcement Program (CCEP).

Compliance with Directory#1 shall be demonstrated for all requirements that are not required for compliance with the NERC Reliability Standards and NPCC will not enforce duplicate sanctions for the same violation.

Prepared by: Task Force on Coordination of Planning

Review and Approval: Revision to any portion of this Directory will be posted by the lead Task Force in the NPCC Open Process for a 45 day review and comment period. Upon addressing all the comments in this forum, the Directory document will be sent to the remaining Task Forces for their recommendation to seek RCC approval.

Upon approval of the RCC, this Directory will be sent to the Full Member Representatives for their final approval if sections pertaining to the Requirements and Criteria portion have been revised. All voting and approvals will be conducted according to the most current "NPCC. Bylaws" in effect at the time the ballots are cast.

Revisions pertaining to the Appendices or other portions of the document such as links, etc., only require RCC approval.
Errata may be corrected by the Lead Task Force at any time.

This Directory will be updated at least once every three years and as often as necessary to keep it current and consistent with NERC, Regional Reliability Standards and other NPCC documents.

References:
NPCC Glossary of Terms
Emergency Operations (NPCC Directory #2)
Maintenance Criteria for Bulk Power System Protection (NPCC Directory #3)
Bulk Power System Protection Criteria (NPCC Directory #4)
Reserve (NPCC Directory #5)
Special Protection Systems (NPCC Directory #7))
Classification of Bulk Power System Elements (A-10)

This document, when downloaded or printed, becomes UNCONTROLLED. Users should check the NPCC website for the current CONTROLLED version of this document.

Table 1

Planning Design Criteria: Contingency events, Fault type and Performance requirements to be applied to bulk power system elements

Category	**Contingency** events Simulate the removal of all elements that protection systems, including Special Protection Systems, are expected to automatically disconnect for each event that involves an AC fault.	**Fault** type (permanent) **On the listed elements where applicable**	**Performance** requirements
I **Single Event**	1. Fault on any of the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section	Three-phase **fault** with **normal fault clearing**	i. to ix.
	2. Opening of any circuit breaker	No fault	
	3. Loss of single pole of a direct current facility	No fault	
	4. Fault on any of the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section	Phase to ground fault with **delayed fault clearing**	
	5. Fault on a circuit breaker	Phase to ground **fault,** with **normal fault clearing**	
	6. Simultaneous fault on two adjacent transmission circuits on a multiple circuit tower.	Phase to ground **faults** on different phases of each circuit, with **normal fault clearing**	
	7. Simultaneous permanent loss of both poles of a direct current bipolar facility	Without an ac fault	
	8. The failure of a circuit breaker to operate when initiated by a **SPS** after a fault on the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section f. opening of any circuit breaker (without a fault)	Phase to ground **fault**, with **normal fault clearing**	

Category	**Contingency** events Simulate the removal of all elements that protection systems, including Special Protection Systems, are expected to automatically disconnect for each event that involves an AC fault.	**Fault** type (permanent) **On the listed elements where applicable**	**Performance** requirements
II Event(s) after a first loss and after System Adjustment	1. Following the loss of any critical: a. transmission circuit, b. transformer, c. series or shunt compensating device or d. generator e. Single pole of a direct current facility and after System Adjustment, Category I **Contingencies** shall also apply.	Any Category I event as described above.	Performance requirements i to ix apply **Area** generation and **power** flows are adjusted between outages by the use of resources available within ten minutes following notification and other system adjustments such as HVDC and phase angle regulator adjustments that can be made within 30 minutes.

Performance Requirements for the contingencies defined in Table 1:

i. Loss of a major portion of the system or unintentional separation of a major portion of the system shall not occur.

ii. Loss of small or radial portions of the system pre-determined by studies is acceptable provided the performance requirements are not violated for the remaining **bulk power system**.

iii. Voltages and loadings shall be within applicable limits for the pre-**contingency** conditions.

iv. Voltages and loadings shall be within **applicable emergency limits** for post-**contingency** conditions.

v. Adequate reactive power resources and appropriate controls shall be available to maintain voltages within applicable limits.

vi. The **stability** of the **bulk power system** shall be maintained during and following the most severe **contingencies,** with due regard to successful and unsuccessful **reclosing.**

vii. For each of the **contingencies** that involve **fault clearing**, **stability** shall be maintained when the simulation is based on **fault clearing** initiated by the **"system A" protection group** and also shall be maintained when the simulation is based on **fault clearing** initiated by the **"system B" protection group**. When applying this requirement to **contingency** Event ***no 6***, the failure of a **protection group** shall apply only to one circuit at a time.

viii. Regarding **contingency *no 6***, if multiple circuit towers are used only for station entrance and exit purposes and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded. Other similar situations can be excluded on the basis of acceptable risk, provided that the Reliability Coordinating Committee specifically accepts each request for exclusion. (See Appendix E.)

ix. Transient voltage response shall be within acceptable limits established by the Planning Coordinator and the Transmission Planner.

Table 2

Planning Criteria: Extreme Contingency and System Conditions, Fault type and Performance Assessments to be applied to bulk power system elements

.

Category	**Contingency** events Simulate the removal of all elements that protection systems, including Special Protection Systems, are expected to automatically disconnect for each event that involves an AC fault.	**Fault** type (permanent) and/or **condition applied** **On the listed elements where applicable**	**Performance** to be assessed
Extreme Contingency	1. Loss of the entire capability of a generating station.	No Fault	i, ii, iii.
	2. Loss of all transmission circuits emanating from a generating station, switching station, substation or dc terminal.	No Fault	
	3. Loss of all transmission circuits on a common right-of-way.	No Fault	
	4. Fault on of any of the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section	Three-phase **fault** with **delayed fault clearing (**with due regard to successful and unsuccessful **reclosing**.)	
	5. Fault on a circuit breaker	Three-phase **fault**, with **normal fault clearing**	
	6. Sudden loss of a large load or major load center.	No Fault	
	7. The effect of severe power swings arising from disturbances outside the NPCC's interconnected systems.	Fault applied as necessary.	
	8. Failure of a **Special Protection System**, to operate when required following the normal contingencies listed in Table 1, Category I, Single Event.	As listed in Table 1, Category I, Single Event.	
	9. The operation or partial operation of a **Special Protection System** for an event or condition for which it was not intended to operate.	No Fault	
	10. Sudden loss of fuel delivery system to multiple plants, (e.g. gas pipeline contingencies).	No Fault.	
	Any additional extreme contingencies identified by each Planning Coordinator Area.	Fault applied as necessary.	
Extreme System Conditions	Contingency events listed in Table 1, Category I, Single Event	Peak **load** conditions resulting from extreme weather.	i (b, c), ii, iii.
		Generating unit(s) fuel shortage (e.g. gas supply adequacy or low hydro) under normal weather peak conditions	i (c), ii, iii

Category	**Contingency** events Simulate the removal of all elements that protection systems, including Special Protection Systems, are expected to automatically disconnect for each event that involves an AC fault.	**Fault** type (permanent) and/or **condition applied** **On the listed elements where applicable**	**Performance** to be assessed
Extreme System Conditions			

Performance Assessment

i. Model the following pre-contingency conditions:

   a. transfers within or between Transmission Planner and Planning Coordinator Areas should be studied at values not expected to be exceeded more than 25% of the time.

   b. highly probable dispatch patterns of generation for the transfers being studied

   c. appropriate load representation (e.g. active and reactive power as a function of voltage) for transient tests and post transient load flows.

ii. Examine post contingency steady state conditions, as well as stability, overload, cascading outages and voltage collapse to obtain an indication of system robustness and determine the extent of any widespread system disturbance

iii. Where assessment concludes there are serious consequences, an evaluation of implementing a change to design or operating practices to address such contingencies shall be conducted.

Table 3

Operating Criteria: Contingency events, Fault type and Performance requirements to be applied to bulk power system elements to establish transfer capabilities.

	Contingency events Simulate the removal of all elements that protection systems, including Special Protection Systems, are expected to automatically disconnect for each event that involves an AC fault.	**Fault** type (permanent) **On the listed elements where applicable**	**Performance** requirements	
			Normal Transfer Capability	**Emergency** Transfer Capability (only after an **Emergency** is identified)
	1. Fault on any of the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section	Three-phases **fault**, with **normal fault clearing**	i, .ii, iii, iv, v, vi, vii, viii, x, xi.	i, ii, iii, iv, v, vi, vii,viii x, xii.
	2. Opening of any circuit breaker	No fault		
	3. Loss of single pole of a direct current facility	No fault		
	4. Fault on any of the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section	Phase to ground fault, with **delayed fault clearing**	i,ii,iii,iv,vii,viii,ix,x,xi,	Contingency Events 4 through 8 do not apply after an emergency is identified.
	5. Fault on a circuit breaker	Phase to ground **fault,** with **normal fault clearing**		
	6. Simultaneous fault on two adjacent transmission circuits on a multiple circuit tower.	Phase to ground **faults** on different phases of each circuit, with **normal fault clearing**		
	7. Simultaneous permanent loss of both poles of a direct current bipolar facility	Without an ac fault		
	8. The failure of a circuit breaker to operate when initiated by a **SPS** after a fault on the following: a. transmission circuit b. transformer c. shunt device d. generator e. bus section	Phase to ground **fault**, with **normal fault clearing**		

	9. The failure of a circuit breaker to operate when initiated by a SPS after opening of any circuit breaker.	No fault.	i,ii,iii,iv,vii,viii,ix,x,xi,	

Performance Requirements for the contingencies defined in Table 3:

i. Loss of a major portion of the system or unintentional separation of a major portion of the system shall not occur.

ii. Loss of small or radial portions of the system pre-determined by studies is acceptable provided it does not violate the performance requirements for the remaining **BPS**.

iii. Individual Reliability Coordinator Areas shall be operated in a manner such that **Contingencies** and conditions applied can be withstood without causing **significant adverse impact** on other Reliability Coordinator Areas.

iv. Voltages and loadings shall be within applicable limits for the pre-**contingency** conditions.

v. Voltages and loadings shall be within **applicable emergency limits** for post-**contingency** conditions.

vi. Adequate reactive power resources and appropriate controls shall be available to maintain voltages within applicable limits.

vii. The **stability** of the **bulk power system** shall be maintained, with due regard to successful and unsuccessful **reclosing**.

viii. For each of the **contingencies** that involve **fault clearing**, **stability** shall be maintained when the simulation is based on **fault clearing** initiated by the **"system A" protection group**, and also shall be maintained when the simulation is based on **fault clearing** initiated by the **"system B" protection group**. When applying this requirement to **contingency** Event ***no 6***, the failure of a **protection group** shall apply only to one circuit at a time.

ix. Regarding **contingency *no 6***, if multiple circuit towers are used only for station entrance and exit purposes, and if they do not exceed five towers at each station, then this condition is an acceptable risk and therefore can be excluded. Other similar situations can be excluded on the basis of acceptable risk, provided that the Reliability Coordinating Committee specifically accepts each request for exclusion. (See Appendix E.)

x. Appropriate adjustments shall be made to Reliability Coordinator Area operation to accommodate the impact of **protection group outages**, including the **outage** of a **protection group** which is a part of a **Type I special protection system**. For typical periods of forced outage or maintenance of a **protection group**, it can be assumed, unless there are indications to the contrary, that the remaining **protection** will function as designed. If the **protection group** will be out of service for an extended period of time, additional adjustments to operations may be appropriate considering other system conditions and the consequences of possible failure of the remaining **protection group.**

xi. Normal transfer levels shall not require system adjustments before attempting manual reclosing of elements unless specific instructions describing alternate actions are in effect to maintain stability of the **BPS.**

xii. Emergency transfer levels may require system adjustments before attempting manual reclosing of elements to maintain stability of the **bulk power system**.

Operating to the contingencies listed above in Table 3 is considered to provide an acceptable level of **bulk power system** security. However, under high risk conditions, such as severe weather, the expectation of the occurrence of contingencies not listed in Table 3 and/or the associated consequences may be judged to be significantly greater. When these conditions exist, consideration should be given to operating in a more conservative manner.

Appendix A – Reserved for Future Use

Appendix B - Guidelines and Procedures for NPCC Transmission Reviews

1.0 Introduction

NPCC has established a Reliability Assessment Program to bring together work done by NPCC, Transmission Planners and Planning Coordinators relevant to the assessment of **BPS reliability**. As part of the Reliability Assessment Program, the Task Force on System Studies (TFSS) is charged on an ongoing basis with conducting periodic reviews of the **reliability** of the planned **bulk power system** of each Planning Coordinator Area of NPCC The purpose of these reviews is to determine whether each Planning Coordinator Area's planned bulk power transmission system is in conformance with the NPCC Directory #1 *Design and Operation of the Bulk Power System*. The annual Area Transmission Review required in R12 is presented for this purpose. It is expected that this Review will cover Directory #1 requirements as they apply to the **bulk power system**.

2.0 Purpose of Review Presentation

The purpose of the presentation associated with an Area Transmission Review is to demonstrate that the Planning Coordinator's planned **bulk power system** based on its projection of available **demand**, transmission, and **resources**, is in conformance with the Directory #1 criteria. By such a presentation, the Task Force will satisfy itself that the criteria have been met and, in general, that the **reliability** of the NPCC Interconnected Systems will be maintained.

3.0 Study Year To Be Considered

It is suggested that a study year of 4 to 6 years from the reporting date is a realistic one, both from the viewpoint of minimum lead times required for construction, and the ability to alter plans or facilities. The reviews may be conducted for a longer term beyond 6 years to address identified marginal conditions that may have longer lead-time solutions.

4.0 Types and Frequency of Reviews

As described in requirement **R12,** each Planning Coordinator is required to present an annual transmission review to TFSS. However, the review presented by the Planning Coordinator may be one of three types: a Comprehensive (or Full) Review, an Intermediate (or Partial) Review, or an Interim Review.

A Comprehensive Review is a thorough assessment of the Planning Coordinator's entire bulk power transmission system, and includes sufficient analyses to fully address all aspects of an Area Transmission Review as described in **R12.**

In the years between Comprehensive Reviews, Planning Coordinators may conduct either an Interim Review, or an Intermediate Review, depending on the extent of the Planning Coordinator's system changes since its last Comprehensive Review. If the system

changes are relatively minor, the Planning Coordinator may conduct an Interim Review. In an Interim Review, the Planning Coordinator provides a summary of the changes in planned facilities and forecasted system conditions since its last Comprehensive Review and a brief discussion and assessment of the impact of those changes on the bulk power transmission system. No new analyses are required for an Interim Review.

If the Planning Coordinator's system changes since its last Comprehensive Review are moderate or concentrated in a portion of the Planning Coordinator's system, the Planning Coordinator may conduct an Intermediate Review. An Intermediate Review covers all the elements of a Comprehensive Review, but the analyses may be limited to addressing only those issues considered to be of significance, considering the extent of the system changes.

In March of each year, after a Planning Coordinator presents a proposal for the type of review to be conducted during the current year, TFSS will consider each Planning Coordinator's proposal. TFSS will either indicate their concurrence, or require the Planning Coordinator to conduct a more extensive review if the Task Force feels that such is warranted based on the Planning Coordinator's system changes since its last Comprehensive Review.

5.0 Format of Presentation – Comprehensive and Intermediate Review

a) Introduction

- Reference the most recent Area Comprehensive Review and any subsequent Intermediate or Interim reviews as appropriate.
- Describe the type and scope of this review.
- For a Comprehensive Review, describe the existing and planned **bulk power system** facilities included in this review.
- Describe changes in system facilities, **bulk power system elements** and **loads** since the most recent Comprehensive Review.
- Include maps and one-line diagrams of the system showing proposed changes as necessary.
- Describe the demand levels to be studied, according to the range of forecast system demands.
- Identify projected firm transfers and interchange schedules.

b) Present the scope of the analyses. The analyses conducted for a Comprehensive Review should be thorough, but an Intermediate Review may focus on specific

areas of the system, specific system conditions, or a more limited set of "critical" **contingencies**.

c) Steady State Assessment

- Present the **load** model, power factor, demand side management, and other modeling assumptions used in the analysis. Discuss the methodology used in voltage assessments. (An Intermediate Review may refer to the discussion from the last Comprehensive Review.)

- Provide supporting information on the **contingencies** selected for evaluation and an explanation of why **contingencies** not simulated would produce less severe results.

- Provide information on the generation dispatch conditions assumed in the analysis.

- Include plots of "base case" **load** flows with all lines in service for the various conditions studied, e.g., peak, off-peak, and heavy transfers.

- Present the effects of major planned changes on the system.

- Identify applicable transfer limits within and between Planning Coordinator Areas.

- Show the adequacy of voltage performance and voltage control capability for the planned bulk power transmission system.

d) Stability Assessment

Present and/or refer to significant studies showing the effect of **contingencies** on the system and report on the most severe **contingencies** in the following manner:

- Provide supporting information on the **contingencies** selected for evaluation and an explanation of why **contingencies** not simulated would produce less severe results.

- The nature of the **fault** applied, **elements** switched, and **fault clearing** times.

- Plots of angles versus time for significant machines, response of real and reactive power control devices, voltages at significant buses and significant interface flows.

For a Comprehensive or Intermediate Review, present the **load** model and other modeling assumptions used in the analysis. (An Intermediate Review may refer to the discussion from the last Comprehensive Review.)

e) **Fault** Current Assessment

- Present the methodology and assumptions used in the **fault** current assessment. (An Intermediate Review may refer to the discussion from the last Comprehensive Review.)

- Present instances where **fault** levels exceed equipment capabilities and measures to mitigate such occurrences.

- Present changes to **fault** levels at stations adjacent to other Planning Coordinator Areas.

f) Extreme **Contingency** Assessment

- Present the scope of the analyses including a description of the system conditions assessed. The analyses conducted for a Comprehensive Review should be thorough, but an Intermediate Review may focus on specific areas of the system, specific system conditions, or a more limited set of "critical" **contingencies**.

- Provide supporting information on the extreme **contingencies** selected for evaluation and an explanation of why the remaining **contingencies** not simulated would produce less severe results.

- Review the results for widespread cascading due to overloads, instability or voltage collapse caused by extreme **contingencies**

- In the case where **contingency** assessment reveals serious consequences, conduct an evaluation of implementing a change to address such **contingencies**.

g) Extreme System Condition Assessment

- Present the scope of the analyses including a description of the system conditions assessed. The analyses conducted for a Comprehensive Review should be thorough, but an Intermediate Review may focus on specific areas of

the system, specific system conditions, or a more limited set of "critical" **contingencies**.

- Provide the rationale for the loss of fuel supply conditions selected for evaluation and an explanation of why other loss of fuel supply conditions not simulated would produce less severe results.

- Provide supporting information on the **contingencies** selected for evaluation and an explanation of why the remaining **contingencies** not simulated would produce less severe results.

- In the case where extreme condition assessment reveals serious consequences, conduct an evaluation of implementing measures to mitigate such consequences.

h) Review of **Special Protection Systems (SPSs)**

- Present the scope of review. A Comprehensive Review should review all the existing, new, and modified **SPSs** included in its transmission plan. An Intermediate Review may focus on the new and modified **SPSs**, and just those existing **SPSs** that may have been impacted by system changes since they were last reviewed.

- Present the need and utilization for Type I and Type II **SPSs.** For instances where a **SPS** utilization is anticipated to increase, the TFSS should inform the Task Force on Coordination of Planning (TFCP) of this finding.

- Review the validity of the classification of Type III **SPSs**. For instances where a **SPS** which was formerly considered to have only local consequences is identified as having the potential for inter- Planning Coordinator Area effects, for the time period being reviewed, the TFSS should notify the Task Force on Coordination of Planning, System Protection and Coordination of Operation. In such instances a complete review of the **SPS** should be made, as per the *Procedure for NPCC Review of New or Modified Bulk Power System Special Protection Systems (SPS)* in Directory #7.

i) Review of Dynamic Control Systems (DCSs)

Review of potential consequences of failure or misoperation of Dynamic Control Systems (DCS), as defined in NPCC Document C-33 *Procedure for Analysis and Classification of Dynamic Control Systems*. For Type I and Type II DCSs, present

and/or refer to appropriate **stability** studies analyzing the consequences of failure or misoperation in accordance with the Joint Working Group (JWG)-1 report, "Technical Considerations and Suggested Methodology for the Performance Evaluation of Dynamic Control Systems". A Comprehensive Review should address all potentially impactful existing and new DCSs, but an Intermediate Review may focus on new DCSs and only those existing DCSs that may have been impacted by system changes since they were last reviewed.

j) Review of Exclusions to the Directory#1 *Criteria*

Review any exclusions granted under NPCC *Guidelines for Requesting Exclusions to Simultaneous Loss of Two Adjacent Transmission Circuits on a Multiple Circuit Tower* (Appendix E). A Comprehensive Review should address all exclusions, but an Intermediate Review may focus on just those exclusions that may have been impacted by system changes since they were last reviewed.

k) Overview Summary of System Performance for Year Studied

6.0 Format of Presentation - Interim Review

a) Introduction of Interim Review

b) Reference the most recent Comprehensive Review and any subsequent Intermediate or Interim Reviews as appropriate.

c) Changes in Facilities (Existing and Planned) and Forecasted System Conditions Since the Last Comprehensive Review.

- **Load** Forecast
- Generation **Resources**
- **Bulk Power System elements**
- Transmission Facilities
- **Special Protection Systems**
- Dynamic Control Systems
- Exclusions

d) Brief Impact Assessment and Overview Summary

The Planning Coordinator will provide a brief assessment of the impact of these changes on the **reliability** of the interconnected **bulk power system**, based on engineering judgment and internal and joint system studies as appropriate.

7.0 Documentation

The documentation required for a Comprehensive or Intermediate Review should be in the form of a report addressing each of the items of the above presentation format. The report should be accompanied by the Planning Coordinator's **bulk power system** map and one-line diagram, summary tables, figures, and appendices, as appropriate. The report may include references to other studies performed by the Planning Coordinator or by utilities within the Planning Coordinator Area that are relevant to the Area Transmission Review, with appropriate excerpts from those studies.

The documentation required for an Interim Review should be in the form of a short summary report (normally not exceeding 5 pages), containing a description of system changes and a brief assessment on their impact on the **reliability** of the interconnected **bulk power system**

8.0 Task Force Follow-Up Procedures

8.1 Once a Planning Coordinator has presented its Transmission Review report to the TFSS, TFSS will review the Planning Coordinator's report and any supporting documentation and consider whether to accept the report as complete and in full conformance with these Guidelines :

a. If the report is found to be unacceptable, TFSS will indicate to the Planning Coordinator the specific areas of deficiency, and request the Planning Coordinator to address those deficiencies.

b. If there is no concurrence about the results and conclusion(s) of the Planning Coordinator's Review, TFSS will indicate to the Planning Coordinator the specific areas of disagreement, and work with the Planning Coordinator to try to achieve concurrence. If agreement has not been reached within a reasonable period of time, TFSS will prepare a summary of the results of its review, and present the summary to the TFCP.

c. If the report is considered as complete and in full conformance with these Guidelines, TFSS will accept the report.

8.2 If the Area Transmission Review indicates an overall **bulk power system** reliability concern (not specific to the Planning Coordinator's planned bulk power transmission system), TFSS will consider what additional studies may be

necessary to address the concern, and prepare a summary discussion and recommendation to the Task Force on Coordination of Planning

8.3 Upon completion of an Area Review, TFSS will report the results of the review to the Task Force on Coordination of Planning. The TFCP will then review and vote on the completeness and acceptability of the Area Transmission Review and report its finding to the Reliability Coordinating Committee for a final review and approval.

Appendix C - Procedure for Testing and Analysis of Extreme Contingencies

1.0 Introduction

Extreme **Contingencies** (ECs) are tested "as a measure of system strength" in order to identify potential patterns of weakness in the bulk power transmission system. This procedure for the testing and analysis of ECs should be used when testing ECs for NPCC studies or studies submitted for NPCC review.

This procedure applies to transmission planning studies that consider the overall performance of the interconnected systems of the NPCC Planning Coordinator Areas. It principally applies to NPCC - wide studies of the **bulk power system** and generally does not apply to studies normally conducted by NPCC Transmission Planner and Planning Coordinators that concentrate on individual or a limited number of facilities. This procedure also applies to Area Transmission Reviews, and may be applicable to other studies conducted by the Transmission Planner and Planning Coordinators, and even to individual facility investigations, where such studies and investigations consider the overall performance of the interconnected systems of the NPCC Planning Coordinator Areas. Certain Transmission Planners or Planning Coordinators may elect to completely mitigate the effects of specific ECs.

Finally, this procedure should be followed in multi-regional studies in which NPCC is an active participant, to the extent that this is within the scope of such multi-regional efforts.

2.0 Choosing Contingencies for Testing

The ECs are defined as per **Requirement R9.** Testing should focus on those ECs expected to have the greatest potential effect on the interconnected system. Particular attention should be paid to **contingencies** which would result in major angular power shifts, e.g., interruption of shorter transmission paths carrying heavy power flows, leaving longer transmission paths as the only remaining paths. Additionally, **contingencies** which would result in reversal of major power transfers, e.g. loss of major ties in a neighboring region or Area when said region or Area was transferring power away from the area of interest, should be considered for their impact in subjecting the system to severe power swings. In considering specific **contingencies** to be investigated in an NPCC study, all relevant testing done at the Transmission Planner and Planning Coordinator level should first be reviewed.

In general, a **contingency** in a particular Planning Coordinator Area should be studied, if requested by any other Transmission Planner or Planning Coordinator, based on a reasonable surmise that the requesting Entity may be adversely affected.

3.0 Modeling Assumptions

As referenced in Table 2, performance assessment “i” for **R9**, the assumed generation dispatch, transfers levels, load levels and **load** representation are major considerations in EC tests. It is not the intent to test the worst imaginable extreme, but EC tests should be severe.

The specification of appropriate **load** representation applies to long term stability tests or post-transient power flows as well as **transient stability** tests.

4.0 Evaluating Individual Test Results

A question in evaluating the results of a particular test run is - “Does the system "pass" or "fail" for this **contingency**?” While in the final analysis this is a matter of informed engineering judgment, factors which should be considered include:

1. Lines or transformers loaded above **short time emergency ratings**,

2. Buses with voltage levels in violation of **applicable emergency limits**, (which vary depending on the location within the system),

3. Magnitude and geographic distribution of such overloads and voltage violations across the system,

4. Transient generator angles, frequencies, voltages and power,

5. Operation of Dynamic Control Systems and **Special Protection Systems** (**SPS**),

6. Oscillations that could cause generators to lose synchronism or lead to dynamic instability,

7. Net loss of source resulting from any combination of loss of synchronism of one or more units, generation rejection or runback initiated by SPS, or any other defined system separation,

8. Identification of the extent of the Planning Coordinator Area (s) involved for any indicated instability or islanding (the involvement of more than one Planning Coordinator Area, should be a major consideration),

9. **Relay** operations or the proximity of apparent impedance trajectories to **relay** trip characteristics,

10. The angle across opened breakers,

11. Adequacy of computer simulation models and data.

Finally, a judgment should be attempted as to whether a "failure" is symptomatic of a basic system weakness, or just sensitivity to a particular EC. For example, should failures turn up for several EC tests in a particular part of the system, it is likely that a basic system weakness has been identified.

The loss of portions of the system should not necessarily be considered a failed result, provided that these losses do not jeopardize the integrity of the overall **BPS.**

NPCC study groups should avoid characterizations like "successful" and "unsuccessful" when commenting on individual runs. Rather, the specific initial conditions directly causing or related to the failure, the complete description of the nature of the failure (e.g., voltage collapse, instability, system separation, as well as the facilities involved), and the extent of potential impact on other Planning Coordinator Areas should be reported.

5.0 Evaluating the Results of EC Tests

EC test reports should focus on those portions of the system in which basic system weaknesses may be developing, rather than on the results of one specific **contingency**.

Any patterns of weaknesses should be identified, which may include reference to earlier NPCC studies and/or Transmission Planner, Planning Coordinator or member system investigations. There is also a need to distinguish between a "failed" test which indicates sensitivity only to a particular **contingency** run and a "failed" test which indicates a more general system weakness (always keeping in mind the severity of possible consequences of the **contingency**). Actions taken by member systems, Transmission Planners or Planning Coordinators to reduce the probability of occurrence or mitigate the consequences of the **contingency** should also be cited.

NPCC follow-up, after publication of a final report, is appropriate only for instances of possible general system weakness. In these instances, the results should be specifically referred to the affected Transmission Planner(s) or Planning Coordinator(s) for further and more detailed investigation with subsequent reporting to NPCC.

Appendix D - Guidelines for Area Review of Resource Adequacy

1.0 Introduction

NPCC has established a Reliability Assessment Program to bring together work done by the NPCC and Planning Coordinators relevant to the assessment of **bulk power system reliability**. As part of the Reliability Assessment Program, each Planning Coordinator submits to the Task Force on Coordination of Planning its Area Review of Resource Adequacy, which is an annual assessment to demonstrate that the proposed resources of each NPCC Planning Coordinator will meet NPCC resource adequacy planning requirements, consistent with these guidelines. The Task Force is charged, on an ongoing basis, with reviewing and recommending NPCC Reliability Coordinating Committee approval of these reviews of **resource** adequacy of each Planning Coordinator Area of NPCC.

The NPCC role in monitoring conformance with the NPCC Directory #1 - *Design and Operation of Bulk Power System* is essential because under this criterion, each Planning Coordinator determines its resource requirements by considering interconnection assistance from other Planning Coordinators, on the basis that adequate **resources** will be available in those Planning Coordinator Areas. Because of this reliance on interconnection assistance, inadequate **resources** in one Planning Coordinator Area could result in adverse consequences in another Planning Coordinator Area.

It is recognized that all Planning Coordinators may not necessarily express their own **resource** adequacy criterion as stated in Requirements R4, R5, and R6 of the Directory #1 criteria. However, the Directory #1 criteria provide a reference point against which a Planning Coordinator's **resource** adequacy criterion can be compared.

2.0 Purpose of Presentation

The purpose of the presentation associated with a resource adequacy review is to show that each Planning Coordinator's proposed resources are in accordance with the NPCC Directory #1 - Design and Operation of the **Bulk Power System**. By such a presentation, the Task Force will satisfy itself that the proposed resources of each NPCC Planning Coordinator will meet the NPCC Resource Adequacy Requirements, as defined NPCC Directory #1, over the time period under consideration.

3.0 Format of Presentation and Report – Comprehensive Review

Each Planning Coordinator should include in its presentations and in the accompanying report documentation, as a minimum, the information listed below. At its own discretion, the Planning Coordinator may discuss other related issues not covered specifically by these guidelines.

3.1 Executive Summary

3.1.1 Briefly illustrate the major findings of the review.

3.1.2 Provide a table format summary of major assumptions and results.

3.2 Table of Contents

3.2.1 Include listing of all tables and figures.

3.3 Introduction

3.3.1 Reference the previous NPCC Area Review.

3.3.2 Compare the proposed resources and load forecast covered in this NPCC review with that covered in the previous review

3.4 Resource Adequacy Criterion

3.4.1 State the Planning Coordinator's resource adequacy criterion.

3.4.2 State how the Planning Coordinator criterion is applied; e.g., load relief steps.

3.4.3 Summarize resource requirements to meet the criteria for the time period under consideration. If interconnections to other Planning Coordinators and regions are considered in determining this requirement, indicate the value of the interconnections in terms of megawatts. In the calculation of available **resources**, supply- side resources from neighboring systems are limited to firm capacity backed purchases.

3.4.4 Provide either an estimate of the resources required to meet the NPCC criteria or a statement as to the comparison of the two criteria, if the Planning Coordinator criterion is different from the NPCC criterion

3.5 Resource Adequacy Assessment

3.5.1 Evaluate proposed resources versus the requirement to reliably meet projected electricity demand assuming the Planning Coordinator's most likely load forecast.

3.5.2 Evaluate proposed resources versus the requirement to reliably meet projected electricity demand assuming the Planning Coordinator's high load growth scenario.

3.5.3 Describe load and resource uncertainties on projected Planning Coordinator Area reliability and describe mechanisms to mitigate anticipated material adverse effects on reliability.

3.5.4 Describe anticipated effects from proposed major changes to market rules on Planning Coordinator Area reliability.

3.5.5 Summarize resource adequacy studies conducted since the previous Area Review, as appropriate

3.6 Reliability Impacts Due to Environmental Regulations and Fuel Supply Issues.

3.6.1 Discuss anticipated material adverse effects on reliability resulting from the proposed resources fuel supply and transportation.

3.6.2 Discuss anticipated reliability impacts related to an Area's compliance with State, Federal or Provincial requirements (such as environmental, renewable energy, or greenhouse gas reductions).

3.7 Mitigation Measures for Environmental Regulations and Fuel Supply Issues

3.7.1 Describe available mechanisms to mitigate anticipated reliability impacts of resource fuel supply, demand resource response, fuel transportation issues and/or environmental considerations.

4.0 Format of Presentation and Report – Annual Interim Review

The Annual Interim Review should include a reference to the most recent Comprehensive Review; a listing of major changes in: facilities and system conditions, load forecast, generation resources availability; related fuel supply and transportation information, environmental considerations, demand response programs, transfer capability and emergency operating procedures. In addition, the assessment should also include a comparison of major changes in market rules, implementation of new rules, locational

requirements, and installed capacity requirements. Finally, the report should include a brief impact assessment and an overall summary.

The Planning Coordinator will provide a brief assessment of the impact of these changes on the reliability of the interconnected **bulk power system**. This assessment should be based on engineering judgment, internal system studies and appropriate joint interconnected studies. To the extent that engineering judgment or existing studies can be used to clearly demonstrate that a Planning Coordinator Area is expected to meet the NPCC resource adequacy criterion, detailed system LOLE studies are not required.

The documentation for the Annual Interim Review should be in the form of a summary report (normally not exceeding three to five pages.)

Sections A and B should describe the reliability model and program used for the resource adequacy studies discussed in Section 3.5. Section C should describe the Task Force follow-up procedures.

A. Description of Resource Reliability Model

1.1 Load Model

1.1.1 Description of the **load** model and basis of period **load** shapes.

1.1.2 How **load** forecast uncertainty is handled in model.

1.1.3 How the electricity demand and energy projections of interconnected entities within the Planning Coordinator Area that are not members of the Planning Coordinator Area are addressed.

1.1.4 How the effects (demand and energy) of demand-side management programs (e.g., conversion, interruptible demand, direct control **load** management, demand (**load**) response programs) are addressed.

1.2 Supply Side Resource Representation

1.2.1 Resource Ratings

1.2.1.1 Definitions.

1.2.1.2 Criteria for verifying **ratings**. Reference NPCC Directory#9 Verification of Gross and Net Real Power Capability and Directory#10 Verification of Gross and Net Reactive Power Capability.

1.2.2 Unavailability Factors Represented

1.2.2.1 Type of unavailability factors represented; e.g., forced outages, planned outages, partial derating, etc.

1.2.2.2 Source of each type of factor represented and whether generic or individual unit history provides basis for existing and new units

1.2.2.3 Maturity considerations, including any possible allowance for in-service date uncertainty.

1.2.2.4 Tabulation of typical unavailability factors.

1.2.3 Purchase and Sale Representation

1.2.3.1 Describe characteristics and level of dependability of transactions.

1.2.4 Retirements.

1.2.4.1 Summarize proposed retirements.

1.3 Representation of Interconnected System in Multi-Area Reliability Analysis, including which Planning Coordinator Areas and regions are considered, interconnection capacities assumed, and how expansion plans of other Planning Coordinators and regions are considered.

1.4 Modeling of Variable and Limited Energy Sources.

1.5 Modeling of Demand Side Resources and Demand (Load) Response Programs.

1.5.1 Description should include how such factors as in-service date uncertainty, **rating**, availability, performance and duration are addressed.

1.6 Modeling of all Resources.

1.6.1 Description should include how such factors as in-service date uncertainty; capacity value, availability, **emergency** assistance, scheduling and deliverability are addressed.

1.7 Other assumptions i.e., internal transmission limitations, maintenance over-runs, fuel supply and transportation and environmental constraints.

1.8 Incorporate the reliability impacts of market rules.

B. Other Factors, If Any, Considered in Establishing Reserve Requirement Documentation

The documentation required to meet the requirements of the above format should be in the form of summaries of studies performed within a Planning Coordinator Area, including references to applicable reports, summaries of reports or submissions made to regulatory agencies.

C. Task Force Follow-Up Procedures

Once a specific Planning Coordinator has made a presentation or a series of presentations to the Task Force on Coordination of Planning, the latter shall:

1.1 Prepare a brief summary of key issues discussed during the presentation.

1.2 Note where further information was requested and the results of such further interrogations.

1.3 Note the specific items that require additional study and indicate the responsibilities for undertaking these studies.

1.4 Recommend to the Reliability Coordinating Committee whether the Resource Adequacy Review is suitable for approval.

Appendix E - Guidelines for Requesting Exclusions to Simultaneous Loss of Two Adjacent Transmission Circuits on a Multiple Circuit Tower.

1.0 Introduction

Directory #1 allows for requests for exclusion from the simultaneous loss of two adjacent transmission circuits on multiple circuit towers on the basis of acceptable risk. All exclusions must be reviewed by the applicable Task Forces and approved by the Reliability Coordinating Committee (RCC). An acceptance of a request for exclusion is dependent on the successful demonstration that such exclusion is an acceptable risk. These guidelines describe the procedure to be followed and the supporting documentation required when requesting exclusion, and establishes a procedure for periodic review of exclusions of record.

2.0 Documentation

The documentation supporting a request for exclusion to the Criteria includes the following:

2.1 A description of the facilities involved, including geographic location, length and type of construction, and electrical connections to the rest of the interconnected power system;

2.2 Relevant design information pertinent to the assessment of acceptable risk, which might include: details of the construction of the facilities, geographic or atmospheric conditions, or any other factors that influence the risk of sustaining the loss of adjacent transmission circuits on a multiple circuit tower;

2.3 An assessment of the consequences of the loss of adjacent transmission circuits on a multiple circuit tower, including, but not limited to, a discussion of levels of exposure and probability of occurrence of **significant adverse impact** on the **bulk power system** ;

2.4 For existing facilities, the historical outage performance, including cause, for such **contingencies** on the specific facility (facilities) involved as compared to that of other multiple circuit tower facilities;

2.5 For planned facilities, the estimated frequency of adjacent transmission circuit multiple circuit tower **contingencies** based on the historical performance of facilities of similar construction located in an area with similar geographic climate and topography.

3.0 Procedure for obtaining an Exclusion

The following procedure is used to obtain an exclusion:

3.1 The entity requesting the exclusion (the Requestor) submits the request and supporting documentation to the Task Force on System Studies (TFSS) after acceptance has been granted by the Requestor's own Planning Coordinator, if such process is applicable.

3.2 TFSS reviews the request, verifies that the documentation requirements have been met, and determines the acceptability of the request.

3.3 If TFSS deems the request acceptable, TFSS requests the Task Force on Coordination of Planning (TFCP), the Task Force on Coordination of Operation (TFCO), and the Task Force on System Protection (TFSP) to review the request. The Requestor provides copies of the request and supporting documentation to the other Task Forces as directed by TFSS. If additional information is requested by the other Task Forces as part of their assessment, the Requestor provides this information directly to the interested Task Force, with a copy to the TFSS. The other Task Forces review the request and indicate their acceptance or non-acceptance to TFSS.

3.4 If all Task Forces deem the request for exclusion acceptable, the TFSS will forward a recommendation for approval to the RCC.

3.5 Exclusion requests will be effective upon approval by the RCC.

Appendix F – Procedure for Operational Planning Coordination

1.0 Introduction

The Reliability Coordinators (RC) of the Northeast Power Coordinating Council, Inc. (NPCC) require access to the security data specified in this procedure in order to adequately assess the reliability of the NPCC **bulk power system**. All users of the electric systems, including market participants, should supply such data to the NPCC Reliability Coordinators. Coordination among and within the Reliability Coordinator Areas (RC Area) of NPCC is essential to the reliability of interconnected operations. Timely information concerning system conditions should be transmitted by the NPCC RC Areas to other RC Areas as needed to assure reliable operation of the **bulk power system**. One aspect of this coordination is to ensure that adjacent RC Areas and neighboring systems are advised on a regular basis of expected operating conditions, including generator, transmission and system **protection**, including Type I **special protection system,** outages that may materially reduce the ability of an RC Area to contribute to the reliable operation of the interconnected system, or to receive and/or render assistance to another RC Area. To the extent practical, the coordination of outage schedules is desirable in order to limit the severity of such impacts.

To ensure that there is effective coordination for system **reliability** concerns, this document establishes procedures for the exchange of information regarding load/capacity forecasts, including firm sales and firm purchases, generator outage schedules, and transmission outage schedules for those **elements** that may have an adverse impact on other RC Area(s). It also details general action that may be taken to improve the communication of problems as well as specific topics that may be discussed in regularly scheduled conference calls or ad -hoc conference calls arranged in anticipation of problems such as capacity deficiency or inadequate light load margin in one or more RC Areas.

NPCC participants and other recipients of the information provided by processes in this guideline should adhere to the NPCC Critical Energy Infrastructure Information Non – Disclosure agreement.

2.0 Load/Capacity Forecasts

2.1 Twice yearly by May 15th and November 15th respectively, the Operations Planning Working Group (CO 12) will perform a summer and winter assessment for the next season.

The results will be reviewed by the NPCC TFCO and the NPCC Reliability Coordinating Committee (RCC) during the spring and autumn meetings of both groups and documented in the summer and winter NPCC Reliability Assessment reports.

2.2 Each week, each RC Area will review its weekly net resource capacity margin, as defined in Attachment A, for the twelve weeks to follow and forward the information to the NPCC Staff for distribution to all NPCC RC Areas. If an NPCC RC Area identifies a deficiency or light load condition, the RC Area should identify the cause(s) and mitigation measures that have been implemented, or will be implemented, to manage the issue.

3.0 Generator Outage Coordination

3.1 Each RC Area should exchange current and expected generator outages that may have a significant impact on an adjacent RC Area or neighboring systems or a significant impact on the transfer capability between RC Areas.

4.0 Transmission Outage Coordination

4.1 Advance Planning of Transmission Facility Outages

Each RC should exchange critical transmission **element** outages as identified in the coordination agreements with their interconnected neighbors, **elements** identified on the Facilities Notification List and multiple transmission **element** outages that may have an adverse impact on external energy transfers. Each Reliability Coordinator shall minimize the duration of outages to facilities that impact inter-Reliability Coordinator Areas.

4.2 Facilities Notification List

The NPCC Facilities Notification List, Attachment D, has two components:

1) the NPCC Transmission Facilities Notification List; and
2) the list of NPCC Type I **special protection systems**.

The Facilities Notification List is developed by each RC Area and specifies all facilities that, if removed from service, may have a significant, direct or indirect impact on another RC Area's transfer capability. The cause of such impact might include stability, voltage, and/or thermal considerations.

Prior to October 1st of each year, each RC Area will review and update its Facilities Notification List and coordinate necessary changes with other appropriate NPCC RC Areas. Prior to January 1st, and after review by the TFCO, the jointly developed, updated and approved Facilities Notification List will be posted on the NPCC secure website.

It should be noted that revisions to the Facilities Notification List will not follow the NPCC Process for Open Review due to the secure nature of the information

contained, and Attachment D is not openly published with this Procedure.

A temporary reconfiguration of the network may result in an outage to one or more facilities not listed in Attachment D having an impact on other NPCC RC Areas. It is the responsibility of the RC experiencing the condition to notify impacted RCs in a timely manner and provide updated status reports during the condition.

4.3 Notifications of Transmission **Element** Outages:

4.3.1 Notification requirements for Transmission **Element** Outages should be defined in interconnection coordination agreements. The time frames identified below are the minimum notification requirements.

4.3.2 Reliability Coordinators will advise affected RCs of all planned and unplanned outages of **elements** on the Facilities Notification List and those multiple transmission **element** outages that may have an adverse impact on external energy transfers.

All outages to equipment listed in the Facilities Notification List and those multiple transmission **element** outages that may have an adverse impact on external energy transfers should be planned with as much advance notice as practical.

Normally, notification for outages on **elements** covered by this instruction will be submitted to the appropriate RC Areas at least two (2) working days prior to the time the **element** is to be taken out of service.

When an RC Area receives an outage notification from another RC Area, prompt attention will be given to the notification and appropriate comments rendered.

4.3.3 An RC Area will not normally remove from service any transmission **elements,** which might have a **reliability** impact on an RC Area without prior notification to and appropriate review by that RC Area. In the event of an **emergency** condition, each RC Area may take action as deemed appropriate. Other RC Areas should be notified immediately.

An RC Area will make every effort to reschedule routine (non-emergency) transmission outages that severely degrade the reliability of an adjacent RC Area or neighboring system.

4.3.4 Each RC Area will advise the other affected RC Areas of any **protection** outage associated with RC Area tie line facilities Coordination agreements may identify additional reporting requirements associated with **protection** outages.

5.0 Specific Communications

Conditions in an RC Area that may have an impact on another RC Area should be communicated in a clear and timely manner. Specific communications are conducted as follows:

5.1 Weekly

Each Thursday a conference call will be initiated by the NPCC Staff to discuss operations expected during the seven-day period starting with the following Sunday. Operations personnel from the NPCC RC Areas and, as necessary, adjacent RC Areas will participate. In advance of the conference call, each RC Area will prepare the data specified in Attachments A and B, and forward it to the NPCC Staff a minimum of one hour in advance of the scheduled call. The completed "NPCC Weekly Conference Call Generating Capacity Worksheet," Attachment B, together with the list of "Twelve Weeks Projections of Net Margins," will be forwarded to the conference call participants by the NPCC Staff.

Each RC will review its weekly capacity margins for the next twelve week period. If a deficiency or light load condition is identified, the RC will identify the cause of the deficiency or light load condition and discuss proposed mitigation measures.

The NPCC Staff will prepare Conference Call Notes that will be forwarded to the conference call participants and members of the TFCO by the following Friday afternoon.

Items of particular concern that should be addressed during the weekly conference call are described in Attachment C.

5.2 Emergency Preparedness Conference Call

Whenever adverse system operating or weather conditions are expected, any RC Area may request the NPCC Staff to arrange an Emergency Preparedness Conference Call (NPCC Document C-01) to discuss operating details with appropriate operations management personnel from the NPCC RC Areas and neighboring systems.

5.3 Daily Conference Calls

Each of the NPCC Reliability Coordinator Area control rooms participate in a regularly scheduled daily conference call. The goal of this call is to alert NPCC Reliability Coordinators of any potential emerging problems. Subjects for discussion are limited to credible events which could impact the ability of a

Reliability Coordinator to serve its load and meet its operating reserve obligations, or which would impose a burden to the Interconnection.

Procedure for Operational Planning Coordination – Attachment A

Load and Capacity Table Instructions and Generating Capacity Worksheet Instructions

Week Beginning	The seven day period for which data is to be reported is defined as starting with the Sunday following the conference call through the following Saturday.
Installed Generating Capacity (Line Item 1)	Include all available generation at its maximum demonstrated capability for the appropriate seasonal capability period.
Other Generating Capacity(Line Item 2)	Include all available generation not included in Item#1. This item includes, but is not limited to, co-generators, small power producers and all other nonutility electricity producers, such as exempt wholesale generators who sell electricity.
Firm Purchases (Line Item 3)	Include only those transactions where capacity is delivered. Exclude “energy only” transactions.
Firm Sales (Line Item 4)	Include only those transactions where capacity is delivered. Exclude “energy only” transactions.
Net Capacity (Line Item 5)	Add Installed Generating Capacity and Firm Purchases. Subtract Firm Sales. (Line 1+Line 2-Line3)
Peak Load Forecast (Line Item 6)	The peak load forecast along with the day during which the peak is expected to occur should be the best estimate of the RC Area’s maximum peak load exposure anticipated for the week reported.
Available Reserve (Line Item 7)	Subtract Peak Load Forecast from Net Capacity. (Line 4-Line5.)
Demand Side Management (Line Item 8)	Include only maximum capability which can be obtained by operator initialization within four (4) hours.

Attachment A (continued)	
Known Unavailable Capacity (Line Item 9)	Include all known outages, as well as those deratings or unit outages presently forced out, unavailable, on extended cold standby or which are anticipated to remain out of service. This would also include capacity unavailable due to transmission constraints.
Net Reserve (Line Item 10)	Available Reserve plus Demand Side Management minus Known Unavailable Capacity. (Line 6+Line 7-Line 8)
Required Operating Reserve (Line Item 11)	The methodology used by each RC Area in calculating operating reserves should, at a minimum, meet the requirements of NPCC Directory # 5, "Reserve." Methodologies differing from the Directory #5 requirements should be clarified in Attachment B, "NPCC Weekly Conference Call Generating Capacity Worksheet," under the tab for "Operating Reserve."
Gross Margin (Line Item 12)	Subtract Required Operating Reserve from Net Reserve. (Line 9-Line 10)
Unplanned Outages (Line Item 13)	Estimate the amount of generating capacity which will be unavailable. This quantity should be based on historical averages for forced outages and deratings.
Net Resource Capacity Margin (Line Item 14)	Subtract Unplanned Outages from Gross Margin. A positive value reflects surplus reserve. A negative value reflects a deficiency. (Line 11-Line 12)
Forecast High / Low Temperatures and Days (Line Item 15)	Include the expected high and low temperatures for the RC Area for the week, and indicate the day on which they are expected to occur.

Attachment A (continued)	
Seasonal High / Low Temperatures (Line Item 16)	Include the expected high and low forecast seasonal temperatures for the RC Area.
Minimum Load Forecast (Line Item 17)	The minimum load forecast, indicating the day on which it is expected to occur should be the best estimate of the RC Area's minimum load exposure anticipated for the week reported.
Minimum Resources (Line Item 18)	The Minimum Resources are the Reliability Coordinator Area's total expected on-line generator minimum output capability and must-take purchases.
Light Load Margin (Line Item 19)	Subtract Minimum Resources from Minimum Load Forecast. A negative number indicates a light load condition. (Line 17-Line 18)

Procedure for Operational Planning Coordination – Attachment B

NPCC Weekly Conference Call Generating Capacity Worksheet

The "NPCC Weekly Conference Call Generating Capacity Worksheet" is an active spreadsheet used each week to assist in the calculation of the data discussed during the weekly conference call. A blank template is available from the NPCC office.

Procedure for Operational Planning Coordination - Attachment C

CONDITIONS FOR DISCUSSION

Items of particular concern that should be discussed during a conference call can include, but are not limited to, the following:

- anticipated weather;
- largest first and second contingencies;
- operating reserve requirements and expected available operating reserve;
- capacity deficiencies;
- potential fuel shortages or potential supply disruptions which could lead to energy shortfalls;
- light load margins;
- general and specific voltage conditions throughout each system or RC Area;
- status of short term contracts and other scheduled arrangements, including those that impact on operating reserves;
- additional capability available within twelve hours and four hours;
- generator outages that may have a significant impact on an adjacent RC Area or neighboring system;
- transmission outages that may have an adverse impact on external energy transfers;
- potential need for emergency transfers;
- expected transfer limits and limiting elements;
- a change or anticipated change in the normal operating configuration of the system, such as the temporary modification of relay **protection** schemes so that the usual and customary levels of **protection** will not be provided, or the arming of **special protection systems** not normally armed, or the application of abnormal operating procedures; and
- update of the abnormal status of NPCC Type I **special protection systems** forced out of service

Attachment D

NPCC Facilities Notification List

Attachment D is not publicly available due to the confidential nature of the information presented.

Appendix G - Procedures for Inter Reliability Coordinator Area Voltage Control

1.0 Introduction

This Procedure provides general principles and guidance to Reliability Coordinators and Transmission Operators for effective inter- Transmission Operator Area voltage control, consistent with the NPCC, Directory #1, "Design and Operation of the **Bulk Power System**". Specific methods to implement this Procedure may vary among Reliability Coordinators and Transmission Operators, depending on local requirements. Coordinated inter- Transmission Operator Area voltage control is necessary to regulate voltages to protect equipment from damage and prevent voltage collapse. Coordinated voltage regulation reduces electrical losses on the network and lessens equipment degradation. Local control actions are generally most effective for voltage regulation. Occasions arise when adjacent Reliability Coordinators and Transmission Operators can assist each other to compensate for deficiencies or excesses of **reactive power** and improve voltage profiles and system security.

2.0 Principles

Each Reliability Coordinator and Transmission Operator operates, in accordance with NPCC, Directory #1, "Design and Operation of the **Bulk Power System**" criteria, their own individual or joint operating policies, procedures and applicable interconnection agreements. Adjacent Reliability Coordinators and Transmission Operator should be familiar with the respective criteria and procedures of their neighboring Reliability Coordinators and Transmission Operator Areas, and should mutually agree upon procedures for inter- Transmission Reliability Coordinator and Operator Area voltage control.

In the event the system state changes to a condition that requires a voltage or reactive corrective action, the Reliability Coordinator and Transmission Operator for the Area in which the condition is originating from should immediately take corrective action. If the corrective control actions are ineffective, or the Reliability Coordinator and Transmission Operator for the Area have insufficient reactive resources to control the problem, assistance may be requested from other Reliability Coordinators and Transmission Operator Areas.

Whether inter- Reliability Coordinator and Transmission Operator Area voltage control is carried out through specific or general procedures, the following should be considered and implemented if applicable:

2.1 To effectively coordinate voltage control, location and placement of metering for **reactive power** resources and voltage controller status should be the same between adjacent Reliability Coordinators and Transmission Operator Areas;

2.2 the availability of **voltage regulating transformers** in the proximity of **tie lines**;

2.3 voltage levels, limits, and regulation requirements for stations on either side of an inter- Reliability Coordinator and Transmission Operator Area interface;

2.4 the circulation of **reactive power** (export at one tie point in exchange for import at another);

2.5 **tie line** reactive losses as a function of active **power** transfer;

2.6 the sharing of the reactive requirements of **tie lines** and series regulating equipment (either equally or in proportion to line lengths, etc.);

2.7 the transfer of **reactive power** from one Reliability Coordinator and Transmission Operator Area to another

2.8 reactive **reserve** of on-line generators;

2.9 shunt reactive device availability and switching strategy;

2.10 **static VAR compensator** availability, reactive **reserve**, and control strategy;

2.11 each Reliability Coordinator and Transmission Operator Area should anticipate voltage trends and initiate corrective action in advance of critical periods of heavy and light **loads.**

2.12 Each Reliability Coordinator and Transmission Operator Area should maintain a mix of static and dynamic resources, including reactive **reserves**

3.0 Procedure for Triennial Monitoring and Reporting of Inter-Area Voltage Control

3.1 On, or shortly before, the first of July, the Task Force Coordination of Operations (TFCO) Secretary will write to each TFCO member, requesting a written response by the end of July in the form of:

a) A copy of any new or revised procedures, principles, or understandings (such as minutes of an operating committee meeting between Reliability Coordinators and Transmission Operator Areas) between the reporting Reliability Coordinator and adjacent Reliability Coordinators, or,

b) a response indicating no change to existing procedures, principles, or understandings currently on file at NPCC.

3.2 The TFCO Secretary will summarize the responses and will forward it to TFCO members at least two weeks prior to the October TFCO meeting.

3.3 Following TFCO review and acceptance of the responses, the TFCO Chairman will forward the summary to the Chairman of the Reliability Coordinating Committee (RCC) for informational purposes. This will normally be forwarded three weeks prior to the next regularly scheduled RCC meeting.

NPCC, Inc.

NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

May 22nd, 2014

Subject: Posting of TFSP Technical Comparison and Directory#3 Retirement Recommendation

NPCC Full Member Committee:

On March 20th, 2014 FERC issued a Final Rule approving Reliability Standard PRC -005-2 *Protection System Maintenance*. The revised standard provides latitude for time and performance based relay maintenance programs in addition to incorporating the new definition of Protection Systems.

Concurrent with the development of PRC -005-2 the NPCC Task Force on System Protection (TFSP) has completed a technical evaluation of the criteria in Directory#3 *Maintenance Criteria BPS Protection* in order to insure that the criteria is not inconsistent with the revised version of PRC -005-2.

The TFSP comparison examined all aspects of the Directory#3 criteria including : 1) Maintenance on Protection Assemblies 2) DC Circuit Trip Testing 3)Battery Bank and Charger Testing 4) Breaker Trip Testing 5) Telecommunication Testing 6) UFLS Systems Testing.

Accordingly, the TFSP has concluded that subject to the Canadian Provincial adoption of PRC -005-2 and within NPCC no significant reliability gaps exist with regard to maintenance intervals and activities and the criteria in Directory#3 can be retired.

Please find attached the following documents for your review and comment:

- TFSP Technical Comparison and Recommendation.
- Mapping document demonstrating where the Directory#3 criteria maps to in PRC-005-2.
- A TFSP comment form containing questions designed to facilitate Member feedback to the TFSP.

In accordance with the NPCC Directory Development and Revision Manual the TFSP will review all comments in order to gauge Full Member sentiment on this issue and comments will be received for forty five days through July 7th, 2014.

The NPCC Open Process review may be accessed through the following link:

https://www.npcc.org/Standards/SitePages/NonStandardsList.aspx

Please contact me with questions regarding Directory content or document review.

Thanks.

Gerry Dunbar
Northeast Power Coordinating Council, Inc.
212.840.1070 (p)
gdunbar@npcc.org

On behalf of:

Paul DiFilippo P. Eng.
Chair – NPCC Task Force on System Protection
Manager Protection Reliability and Standards.
Transmission Projects Development
Hydro One Networks Inc
Office: 416-345-5042 Cell: 647-328-7068
paul.difilippo@HydroOne.com

NPCC, Inc.
NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

TASK FORCE ON SYSTEM PROTECTION

Review of

NPCC BULK POWER SYSTEM MAINTENANCE CRITERIA - DIRECTORY NO. 3

As Compared to

NERC PROTECTION SYSTEM MAINTENANCE STANDARD PRC-005-2

And

Task Force on System Protection RECOMMENDATION to Retire DIRECTORY NO. 3

May 22, 2014

Executive Summary

The Northeast Power Coordinating Council (NPCC) has had a long history of establishing Regional reliability requirements for Operations, Planning and also for Bulk Power System protection maintenance. The original set of NPCC's Regional reliability requirements were first established in1969 and, through the years, NPCC has revised, maintained, and enforced this program of more stringent reliability requirements, part of which are contained in the NPCC Directory 3, "Bulk Power System Maintenance Criteria."

NPCC under the NERC Regional Delegation Agreement "RDA" must adhere to the NERC Rules of Procedure (ROP). In the current ROP, Appendix 2, NERC has defined Regional Criteria to mean *"..reliability requirements developed by a Regional Entity that are necessary to implement, to augment, or to comply with Reliability Standards, but which are not Reliability Standards. Such Regional Criteria may be necessary to account for physical differences in the Bulk Power System but are not inconsistent with Reliability Standards nor do they result in lesser reliability. Such Regional Criteria are not enforceable pursuant to NERC delegated authorities, but may be enforced through other available mechanisms. Regional Criteria may include specific acceptable operating or planning parameters, guides, agreements, protocols or other documents."* As part of NPCC's responsibilities under the RDA, NPCC must adhere to the ROP and continually evaluate the regional reliability requirements contained in the criteria documents against all new and revised NERC Reliability Standards. This evaluation must determine if, as defined above, the Regional reliability requirements need revision or continue to be needed to implement, augment or comply with Reliability Standards, and also to ensure that the Regional reliability requirements are not inconsistent with the Reliability Standards.

With the recent approval of the NERC Maintenance and Testing Standard PRC-005-2 by FERC set for implementation starting on April 1, 2015, the Task Force on System Protection (TFSP) has initiated and completed a comprehensive review of Directory 3 against the requirements of the PRC-005-2. This new results-based NERC standard contains a comprehensive set of maximum maintenance intervals and minimum maintenance activities for all BES protections. The review by TFSP was initiated upon approval of the PRC-005-2 by the NERC Board of Trustees and to fulfill the responsibilities as outlined in NPCC's RDA and the NERC ROP. In addition, with the more stringent version of NERC reliability standard requirements now appearing in PRC-005-2, it was identified by the TFSP that there may no longer be a justifiable reliability related need for continuance of the Regional reliability requirements contained in Directory 3. Additionally the TFSP identified that with the implementation of the new standard, entities within NPCC could be subjected to two sets of compliance requirements, one for NPCC BPS protections and one for BES protections (under the new BES definition).

TFSP has concluded that while some of the protection maintenance intervals specified in Directory 3 are more stringent than those in PRC-005-2, most of the maintenance interval increases specified in PRC-005-2 are either minor increases or justifiable based on technical merit. There are two protection system maintenance activities identified in PRC-005-2 that have significantly longer intervals than those in Directory 3, however, based on experience and judgment, TFSP believes that these extended intervals do not pose a significant risk to reliability. TFSP will initiate the addition of requirements to Directory 4 that will dictate additional monitoring for the two protection system components referenced above. These additional requirements will apply to new or modified NPCC BPS protections.

Based on this technical review, TFSP is recommending the retirement of the criteria portion of Directory 3. In addition, and in conformance with the NPCC Board of Directors expectation that the NPCC Regional reliability requirements are, and will remain cost effective. TFSP's review of PRC-005-2 vs. Directory 3 considered costs. This determination by TFSP to retire Directory 3 was also supported by cost-benefit considerations. The remaining Regional reliability requirements in Directory 3 will no longer be cost effective and of sufficient reliability benefit to retain (when also considering the above referenced revisions envisioned for Directory 4) upon implementation of PRC-005-2.

I. Background

In 1969, NPCC had established the Minimum Maintenance Practices for Protective Relays and Associated Devices. These minimum maintenance practices were based on the results of a special questionnaire/survey of maintenance practices of NPCC members and consideration of practices of utility companies outside of NPCC. This document served as a guide until 1986.

In 1986 this guide was renamed a Criteria document "A-4 Maintenance Criteria for Bulk Power System Protection". Its applicability was limited to those relays and associated devices comprising the protective relaying systems associated with the NPCC Bulk Power System, which was defined in the NPCC Bulk Power System Protection Philosophy, established in 1970, as the interconnected electrical network "comprising generation and transmission facilities of the member companies on which faults or disturbance can have a significant effect outside of the local area." Minimum maintenance of protective relay systems and associated devices includes verifying inputs and outputs, making visual inspections, checking for proper operating characteristics including a designated significant coordinating point, and performing trip tests as required to ensure satisfactory operation of the protective equipment as a system.

In 1995, NPCC implemented revised maintenance intervals for protective relays based on a report provided by the TFSP's SP-5 Working Group on the Bulk Power System Protection Maintenance Practices and Intervals. This comprehensive study, based on the Markov modeling technique and using actual members' data, resulted in a calculated optimal interval of approximately 10 years for microprocessor-based relays. Taking a very conservative approach, the interval was changed from 2 years for all protective systems to the following maintenance intervals which considered the protection design technology and the BPS element to be protected:

	Maintenance Intervals for Protection Technology		
Protection Groups for	Electromechanical	Solid-State	Microprocessor-Based
Transmission Line	2 years	2 years	4 years
Transformer, Bus, Shunt Reactor, and Capacitor	4 years	4 years	4 years
All other	2 years	2 years	2 years

In 2004, an update to the SP-5 study was performed by an Ad Hoc Working Group of TFSP members. The intervals for microprocessor-based relays were subsequently extended from 4 years to 6 years. Note that TFSP continued to take a cautious approach even though the updated study result reaffirmed the optimal interval to be approximately 10 years for all the protection groups based on the updated data for Mean-Time-To-Failure (MTTF) and probability of protection group failure being hidden (P_H) parameters.

In 2008, further revisions were made by the Task Force in an effort to align the NPCC criteria with the maintenance practices and intervals recommended in the NERC Technical Reference Paper on Protection System Maintenance developed by the NERC System Protection and Control Task Force (SPCTF). The SPCTF had also used the Markov model to calculate the optimal interval for microprocessor-based relays and had come up with similar conclusion as the NPCC Ad Hoc Working Group. The NPCC protection system maintenance criteria were then revised to incorporate the following six maintenance activities and intervals for all protection systems of the bulk power system were further extended as follows:

1. Protection Assembly Testing (modified as Table 1 below)
2. DC Circuit Trip Testing
3. Battery Banks and Chargers Testing
4. Breaker Trip Testing
5. Telecommunication Testing
6. Underfrequency Load Shedding and Generator Underfrequency Tripping

Table 1 - INTERVALS FOR PROTECTION ASSEMBLY TESTING

	Non-Self Monitored **Protection Assembly** Note (1)	Microprocessor-Based **Protection Assembly** Note (2)	Microprocessor-Based **Protection Assembly** Note (3)
All **Protection Groups**	**4 years**	**6 years**	**8 years**

Notes:

*(1) Non-Self Monitored **protection** assemblies include electromechanical **relays** and solid state **relays**.*

*(2) Microprocessor-based **protection** assemblies where the principal fault-sensing and logic components include self-monitoring or self- checking, and the failure alarm is annunciated to a 24/7 staffed Operations Center that can initiate an investigation of the problem.*

*(3) Microprocessor-based **protection** assemblies as per Note (2), plus additional self - monitoring or self- checking of ac voltage and current input integrity, and the failure alarm is annunciated to a 24/7 staffed Operations Center that can initiate an investigation of the problem.*

In 2009 Directory 3 was again reviewed through the NPCC Open Process ending with a number of clarifying and editorial changes and no changes to any of the existing testing requirements in the document itself. Additional language was also incorporated into Appendix B of the document to provide guidance that credit can be obtained for normal breaker operations if the equipment design permits verification and documentation of breaker tripping by each individual trip coil.

II. Review of NPCC Criteria against NERC Standard

In April 2013 NPCC Standard Staff conducted a preliminary comparison of the criteria contained within Directory#3 *Maintenance Criteria for BPS Protection* against the requirements in the PRC-005-2 *Protection System Maintenance* which at that time had just been approved by the NERC Board of Trustees. The comparison indicates instances where PRC-005-2 provides more granularity in the approach to testing of specific components within a protection system however there were instances where the D3 criteria appears to be more specific or more stringent than PRC-005-2.

A formal review of Directory 3 against PRC-005-2 was initiated by the TFSP at the November 2013 meeting and again at the January 2014 meeting. The results of TFSP's review for each requirement in Directory 3 are as follows:

Part 1 - Maintenance on Protection Assembly (Directory 3, Section 5.2) compared to Protective Relay (PRC-005-2, Table 1-1)

With testing intervals on Protection Assembly shown in Table 1 above, Directory 3 maintenance includes:

1. Making visual inspection
2. Verify inputs and outputs
3. For microprocessor based relays, confirm that the intended version of software is installed.
4. Verify correct protection operation
5. Verify the integrity of current and voltage transformers and associated circuitry. This verifies that the correct secondary quantities are input to the relay. For microprocessor relays, verify the internal analog inputs with an independent source.

<u>TFSP Review:</u> The testing and maintenance activities in Directory 3 and NERC PRC-005-2 are similar with the sole exception of the need for visual inspections in Directory 3. TFSP concluded that there is no explicit need to have this as an activity since it occurs

regularly in the course of protection maintenance and is likely represented in evidence as nothing more than a check-box.

The most significant difference is the 12-year maximum maintenance interval for monitored relays in PRC-005-2 vs. 6 years and 8 year intervals in Directory 3. However, Directory 3 allows for a 5 month grace period for the scheduled testing of protective relays. In order to meet the 12 year interval of PRC-005-2 (with no grace period) most entities will need to schedule this testing well in advance of the 12 year maximum interval or risk being in non-compliance. So in fact this is in alignment with the 10-year intervals derived in prior analysis by SP-5 and the ad hoc working group using the Markov model. TFSP concludes that the maximum maintenance intervals prescribed in PRC-005-2 are adequate for BPS protection.

As an added note, not all relay components in a microprocessor based relay are necessarily a part of the self-monitoring and that there is an IEEE working group on relay self-monitoring that will address this area.

Part 2 - DC Circuit Trip Test (Directory 3, Section 5.3) and Breaker Trip Test (Directory 3, Section 5.5) compared to Control Circuitry Associated with Protective Function (PRC-005-2, Table 1-5)

Directory 3, Section 5.3 requires DC Circuit Trip tests to verify the protection equipment operation from the trip outputs of the protection assembly up to the breaker trip coil at intervals of 4 years for non-monitored and 6 years for monitored DC circuits (6 years in cases where DC circuit continuity through to the trip coil is alarmed and annunciated upon loss of continuity to a 24/7 staffed operations center that can initiate an investigation of the problem).

Directory 3, Section 5.5 requires the testing of the breaker to trip via each trip coil every two years except for Nuclear plant BPS unit breaker trip tests where they shall be completed at an interval not to exceed three years.

<u>TFSP Review</u>: The table below compares the DC circuit tests prescribed in PRC-005-2 versus those found in Directory 3.

DC Circuit Tests	***PRC-005-2 Intervals***	***Directory 3 Intervals***
DC circuitry up to the trip coils (unmonitored)	*6*	*4*
DC circuitry up to the trip coils (monitored)	*6*	*6*
Actuators of circuit breakers(trip coils), interrupting devices, or mitigating devices	*6*	*2**
Electromechanical lockout devices (unmonitored)	*6*	*4*

Electromechanical lockout devices (monitored)	*6*	*6*
Unmonitored control circuitry	*12*	*4*
Monitored control circuitry	*None*	*6*

**3 years for BPS nuclear unit breakers*

Note that PRC-005-2 mandates operation of each trip coil on a 6 year interval compared to the 2 years for Directory 3. This appears to be a four years difference, however there are no grace periods allowed in PRC-005-2 meaning these tests would likely need to be scheduled on something less than a 6 year time frame. In addition, TFSP members consulted internal breaker experts at their utilities and the conclusion is that extended time for breaker trip coil testing does not pose a significant gap in reliability. In many cases, members do provide trip coil monitoring for breakers that are part of BPS protections and in light of this, TFSP will propose adding a requirement for trip coil monitoring in D4 to these breakers to enhance protection design reliability.

Although a large difference is shown for maximum maintenance intervals for unmonitored DC control circuitry between PRC-005-2, which allows for 12 years between testing periods and the 4 years mandated by Directory 3, TFSP review indicates that PRC-005-2 has taken the approach that DC wiring has a low probability of failure that does not require frequent maintenance. TFSP agrees with the approach taken in PRC-005-2. TFSP also has no data to support the necessity for the current 4 years testing interval required in Directory 3. In addition, a review of the NPCC Misoperations data from 2011 through the 3rd Quarter of 2013 by SP-7 indicated that of the 544 misoperations, 43, or approximately 8%, were caused by problems in the DC System. Almost all of these were unnecessary trips due to grounded wires, induced transients on DC wiring, or water damage. There was no evidence of failure to trip misoperations due to DC wiring. It is likely that very few of these misoperations would have been prevented by use of conventional DC circuit monitoring or increased maintenance frequency.

Part 3 - Battery Banks and Chargers Testing (Directory 3, Section 5.4) compared to Station DC Supply Tests (PRC-005-2, Tables 1-4(a) through 1-4(f))

Directory 3 requires monthly voltage verification of non-monitored station battery bank(s) and no testing required for monitored battery bank voltage alarms that are annunciated to a 24/7 staffed Operations Center that can initiate an investigation of the problem.

TFSP Review: The battery testing in PRC-005-2 is much more comprehensive. In addition an entity can take credit for increased battery monitoring to perform less direct maintenance. Increased monitoring results in a more reliable component overall so TFSP is supportive of this approach.

Part 4 – Breaker Trip Testing (Directory 3, Section 5.5)

TFSP Review: See Part 2 above.

Part 5 – Telecommunication Testing (Directory 3, Section 5.6) Compared to Communication Systems Testing (Table 1-2)

Section 5.6.1: Directory 3 requires testing of terminal equipment using the same intervals as for the protection assembly.

Section 5.6.2: Testing of channel health is required as follows:

> For telecommunication system channels that are not continuously monitored, the signal adequacy shall be tested every month and the ability of a channel to perform its intended function shall be verified every twelve months. An example of such a system is On/Off Power Line Carrier.
>
> For trip equipment which uses frequency shift keying (FSK) mode of communication and the channel (for example, Guard Signal) is continuously monitored, the ability to perform its intended trip function shall be verified every twelve months. Failure of the channel shall be annunciated to a 24/7 staffed Operations Center that can initiate an investigation of the problem.
>
> For telecommunication system channels that are continuously monitored and continuously provide verification of trip capability to an Operator, no additional testing is necessary. Failure of the channel or of the trip capability shall be annunciated to a 24/7 staffed Operations Center that can initiate an investigation of the problem.

TFSP Review:

The maintenance intervals and activities described in PRC-005-2 for the terminal teleprotection equipment are in alignment with maintenance activities for protective relays. The same rationale applies for both Directory 3 Section 5.6.1 and PRC-005-2 Table 2 so TFSP is satisfied with this approach for the same reasons as discussed in Part 1 above.

For telecommunication system channels that are not continuously monitored, PRC-005-2 requires testing at 4 month intervals as opposed to 1 month in Directory 3 Section 5.6.2. It is observed that this change does not create a significant reliability gap since there are no grace periods allowed in PRC-005-2. This means that maintenance activities must be scheduled well before the maximum maintenance intervals, likely in 2 month intervals or so, in order to ensure compliance.

For teleprotection equipment which uses frequency shift keying (FSK) mode of communication and the channel is continuously monitored by a guard signal, PRC-005-2 has established a philosophy that communication systems are analogous to the DC connection from the relay to the trip coil (p.85 of Supplementary Reference). Therefore the intervals established for unmonitored communication systems is set at 6 years, forcing more frequent maintenance than for monitored systems which is set at 12 years. This is a significant deviation from Directory 3 which requires yearly verification of channel performance. In Directory 3 this activity is entitled Channel Health but in reality, it is actually a check of terminal equipment performance in addition to channel health. TFSP believes more credit should be given in recognition for monitoring of channel health and supports the approach taken in PRC-005-2 for this activity. TFSP will propose adding a requirement to utilize only monitored teleprotection circuits in D4 to BPS protections to enhance protection design reliability. TFSP also noted that we now have formal thorough misoperations reporting framework at the NPCC and NERC levels. If as a result of increasing this maintenance interval, there is a noticeable increase in misoperations due to telecommunication equipment or communication channel failure, it will become evident to SP-7, TFSP, and/or NERC SPCS. These groups will then be tasked to address the issue.

It should be noted in PRC-005-2 fully monitored communication systems still must be verified every 12 years which is actually more stringent than Directory 3 which requires no testing.

Part 6 – Underfrequency Load Shedding and Generator Underfrequency Tripping (Directory 3, Section 5.7) Compared to Maintenance Activities and Intervals for Distributed UFLS and Distributed UVLS Systems Testing (Table 3)

Directory 3 requires testing of the UFLS relay on the same frequency as other BPS protection relays based on relay technology. However because of the distributed nature of this load shedding protection, DC circuit tests, DC battery/charger tests and breaker test trips need not take place more often than tests for other protections on that same breaker. For generators rated 20 MW and above, Directory 3 requires the correct calibration of generator underfrequency tripping relays be verified at an interval not exceeding that specified in Table1 above for the Protection Assembly.

<u>TFSP Review</u>: The testing requirements for UFLS in PRC-005-2 for protective relays are in alignment with intervals and activities for BES protective relays. PRC-005-2 does not require any testing of DC circuitry between the protective relay/EM auxiliary or lockout relays and the trip coils of non-BES devices. Elimination of this testing, which is required in Directory 3, does not pose a reliability risk because of the distributed nature of the underfrequency load shedding protection where random failures to trip do not

compromise the objectives of the UFLS program. TFSP concludes that the testing activities and intervals described in PRC-005-2 for UFLS are adequate.

Generator UF relays for generators part of the BES are included in PRC-005-2 and will be on the same maintenance schedule as other BES protective relays.

Conclusion and Recommendations

1. Most of the maximum maintenance intervals (and corresponding maintenance activities) identified in NERC standard PRC-005-2 are not vastly different than those intervals prescribed in NPCC Directory 3. The new results based continent wide standard is a large improvement over PRC-005-1 and is much more specific than its predecessor standard. Furthermore the intervals established in PRC-005-2 for maintenance on the relays themselves are very much in line with the comprehensive report furnished by the SP5 working group on the Bulk Power System Protection Maintenance Practices and Intervals, which was updated in 2004. This report was delivered to TFSP, who at the time, decided to initially take a conservative approach which NPCC members were willing to accept, with the understanding that data would be periodically reviewed with the intent to extend the maintenance interval if appropriate. The subsequent review in 2004 resulted in maintenance intervals being further extended from the original interval.

2. Two requirements in Directory 3 that are significantly more stringent than related PRC-005-2 requirements are:
   a) Section 5.5 - The ability of the breaker(s) to trip via each trip coil shall be verified every two years in Directory 3 vs. a maximum 6-year interval in PRC-005-2
   b) Section 5.6.2 - For trip equipment which uses frequency shift keying (FSK) mode of communication and the channel (for example, Guard Signal) is continuously monitored, the ability to perform its intended trip function shall be verified every twelve months vs. the 12 year testing requirement in PRC-005-2.

   For item 2a) above, TFSP determined that this is not a significant gap as there are no grace periods allowed in PRC-005-2 meaning these tests must be scheduled on something less than a 6 year time frame or the entity would risk violating this requirement. In addition, TFSP members consulted internal breaker experts at their utilities and the conclusion is that extended time for breaker trip coil testing does not pose a gap in reliability.

   For item 2b) above TFSP resolved that monitoring of communication circuit health should provide entities lengthier maintenance intervals. The current test specified in Directory 3 is actually a check of terminal equipment performance in addition to channel health.

   TFSP also noted that we now have formal thorough misoperations reporting framework at the NPCC and NERC levels. If as a result of increasing this

maintenance interval, there is a noticeable increase in misoperations due to telecommunication equipment or communication channel failure, it will become evident to SP-7, TFSP, and/or NERC SPCS. These groups will then be tasked to address the issue.

3. Based on this review, the Task Force intends to supplement the two items noted above with a proposal to enhance the design requirements in Directory 4 for these issues namely:

   - Establish design requirements for monitoring all BPS communication circuits used in protection systems with a provision for fail-safe alarms.
   - Establish design requirement for breaker trip coil monitoring on breakers used for BPS protections.

   TFSP acknowledges that these design requirements will not improve reliability of existing protection facilities; however, they will be applicable to new or revised BPS protections. The communication systems may also be controlled by a third party, thus may require members to mitigate any reliability issues as deemed appropriate by corrective actions in the analysis of protection system Misoperations.

In conclusion, TFSP determined from this review, comparing Directory 3 and PRC-005-2, that there would be minimal, if any impact to reliability of the NPCC Bulk Power System. TFSP recommends the following actions;

a. the criteria portion in Directory 3 containing the Regional reliability requirements, be retired effective April 1, 2015 to coincide with the FERC approved enforcement implementation start date of PRC-005-2,
b. Directory 4 be revised as discussed above prior to the retirement to ensure no reliability gaps exist
c. any remaining guideline or procedural document which may be of benefit to NPCC be retained as a resource document(s).

Proposed Mapping of NPCC Directory 3 - Maintenance Criteria for Bulk Power System Protection

Section	Criteria/Requirement in The Directory	PRC-005-2 Equivalent	Rationale/Justification
Section 5.1	**General criteria** (Criteria/requirement language not excerpted herein)	None. This Section can be removed since it does not stipulate any specific criteria or requirements.	No specific criteria or requirements. Sections 5.2 to 5.7 provide the specific criteria and requirements for protection system maintenance.
Section 5.2	**Protection Assembly Testing Requirement**s There are 5 sub-sections under this Section, and a Table 1 that specifies the maintenance intervals.	See below.	See below.
	5.2.1 Make visual inspections	None. This Section can be removed for reasons indicated under the Rationale column.	This maintenance activity is not required in the NERC PRC-005-2 standard. However, elimination of the requirement to actually record this activity does not pose a risk to reliability as other mandated testing activities would likely reveal deficiencies. In addition, this is an activity that is likely carried out anyway by entities in the course of protection maintenance to varying degrees.
	5.2.2 Verify inputs and outputs, 5.2.3 Confirm that the intended version of software is installed (microprocessor-based relays),	Table 1-1. These Sections can be removed.	The criteria/requirements in Sections 5.2.2 to 5.2.4 are covered by the verification details in Table 1-1 of the NERC PRC-005-2 standard.

Section	Criteria/Requirement in The Directory	PRC-005-2 Equivalent	Rationale/Justification
	5.2.4 Verify correct protection operation, 5.2.5 Verify the integrity of current and voltage transformers and associated circuitry. This verifies that the correct secondary quantities are input to the relay. For microprocessor relays, verify the internal analog inputs with an independent source.		
	Table 1 – Interval for Protection Assembly Testing (Not per verbatim) Requires that protection Assembly testing be performed on an interval not exceeding that specified in Table 1 for bulk power system protection groups. Table 1 stipulates that, for all protection groups, the maintenance interval for: Self Monitored Protection Assembly – 4 year Microprocessor-Based Protection Assembly – 6 years, where the principal fault-sensing and logic components include self monitoring or self checking, and the failure alarm is annunciated to a 24/7 staffed Operations Center that can initiate an investigation of the problem. Microprocessor-Based Protection Assembly – 8 years for additional self monitoring or self checking of ac voltage and current input integrity, and the failure alarm is annunciated to a 24/7 staffed Operations Center that can initiate an investigation of the problem.	Table 1-1. Table 1 of Directory 3 can be removed.	There are no grace periods allowed in the NERC PRC-005-2 standard, meaning that maintenance activities must be scheduled well before the maximum maintenance intervals, likely 18 months or so or the entity will risk non-compliance. The perceived differences in maintenance intervals on protective relays between Directory 3 and PRC-005-2 will not pose a reliability gap. Also, similar to the previous work performed by both NPCC SP-5 WG and the Ad Hoc working group back in 2003, the NERC SPCS and PRC-005-2 drafting team used data from across NERC as well as Markov modeling – which were used to determine optimal maintenance intervals. The numbers that were generated were in line with the previous recommendations from SP-5 WG and the Ad Hoc working group: 10 years for transmission lines and 10 years for transformers, buses, etc. On this basis, it is TFSP's view that the intervals established in PRC-005-2 are justified. .
Section 5.3	**Protection Group DC Circuits Testing Requirements** Tests performed in Section 5.2 above verify the operation of the ac signaling, measuring relays, and verify a protection assemblies' ability to initiate a trip output(s). However, to	Table 1-5. This Section can be removed.	While the NPCC criteria appear to be more stringent than the NERC PRC-005-2 standard, which allows for 12 years between testing periods for all DC circuitry, PRC-005-2 has taken the approach that DC wiring is a low risk item that does not require more frequent maintenance as the risk

Section	Criteria/Requirement in The Directory	PRC-005-2 Equivalent	Rationale/Justification
	verify operation of the protection group as a system, DC circuit testing is required. These tests verify the protection equipment operation from the trip outputs of the protection assembly up to breaker trip coils. DC circuit testing can be achieved by verifying overlapping protection group equipment zones, normally bound by test switches, or by test tripping the protection group. DC circuit test tripping shall be performed on an interval not exceeding that specified in Table 2 for bulk power system protection groups: Table 2 (Not per verbatim) For dc circuit tripping, the testing intervals shall be 4 years and 6 years for non-monitored and monitored circuitry, respectively.		posed by failed wiring is low. TFSP agrees with the approach taken in PRC-005-2 and has no evidence to support the need for more frequent maintenance intervals for DC circuit testing. Misoperations data going back to 2011 was reviewed and there was no evidence of failure to trip misoperations due to DC wiring.
Section 5.4	**Battery Banks and Chargers Testing Requirements** Voltage verification of the station battery bank(s) shall be performed on an interval not exceeding that specified in Table 3 for bulk power system protection groups: Table 3 (Not per verbatim) Non-monitored battery bank voltage shall be tested once a month. There is no requirement for testing monitored battery bank voltage providing that battery bank Voltage alarms are annunciated to a 24/7 staffed Operations Center that can initiate an investigation of the problem.	Table 1-4(a) to Table 1-4(c). This Section can be removed.	The battery testing in the NERC PRC-005-2 standard is much more comprehensive than the Directory 3 requirement. In addition, an entity can take credit for increased battery monitoring to perform less direct maintenance. Increased monitoring results in a more reliable component overall. TFSP is supportive of this approach, and assesses that there is no reliability gap if the NPCC criteria for battery bank testing were to be removed.
Section 5.5	**Breaker Trip Testing Requirements** The ability of the breaker(s) to trip via each trip coil shall be verified every two years with the following exception: Nuclear plant bulk power system unit breaker trip tests shall	Table 1-5. This Section can be removed.	The NERC PRC-005-2 standard mandates operation of each trip coil on a 6 year interval compared to the 2 years for Directory 3. This is not a significant gap as there are no grace periods allowed in PRC-005-2 meaning these tests must be scheduled on something less than a 6 year

Section	Criteria/Requirement in The Directory	PRC-005-2 Equivalent	Rationale/Justification
	be completed at an interval not to exceed three years.		interval. In addition TFSP members were asked to solicit advice internally from breaker experts and the conclusion is that extended time for breaker trip coil testing outlined in PRC-005-2 versus Directory 3 does not pose a gap in reliability. However TFSP will address this perceived gap by proposing the addition of a requirement for trip coil monitoring to Directory 4 to enhance protection design reliability for NPCC BPS breaker trip coils.
Section 5.6	**Telecommunication Testing Requirements** There are two sub-sections under Section 5.6.		
	5.6.1 Terminal Equipment Telecommunications terminal equipment shall be tested on the same time interval as the protection assemblies as per Table 1 above. (See requirements in Table 1 under Section 5.2, above)	Table 1-2 This Section can be removed.	The maintenance intervals (6, 12 years) and activities described in the NERC PRC-005-2 standard for the telecommunication terminal equipment are in alignment with the similar activities for protective relays (Section 5.2, above). The same rationale applies.
	5.6.2 1. For telecommunication system channels that are not continuously monitored, the signal adequacy shall be tested every month and the ability of a channel to perform its intended function shall be verified every twelve months. An example of such a system is On/Off Power Line Carrier. 2. For trip equipment which uses frequency shift keying (FSK) mode of communication and the channel (for example, Guard Signal) is continuously monitored, the ability to perform its intended trip function shall be verified every twelve months. Failure of the channel shall be annunciated to a 24/7 staffed Operations Center that can initiate an investigation of the problem.	Table 1-2. This Section can be removed.	1. The maintenance activity for unmonitored communication channels is actually set at 4 months in the NERC PRC-005-2 standard and a change in this interval does not create a significant reliability gap. There are no grace periods allowed in PRC-005-2 meaning that maintenance activities must be scheduled well before the maximum maintenance interval likely 2 months or so. 2. PRC-005-2 has established a philosophy that communication systems are analogous to the DC connection from the relay to the trip coil (p.85 of Supplementary Reference). Therefore the maintenance intervals established for unmonitored communication systems is set at 6 years, forcing more

Section	Criteria/Requirement in The Directory	PRC-005-2 Equivalent	Rationale/Justification
	3. For telecommunication system channels that are continuously monitored and continuously provide verification of trip capability to an Operator, no additional testing is necessary. Failure of the channel or of the trip capability shall be annunciated to a 24/7 staffed Operations Center that can initiate an investigation of the problem.		frequent maintenance than for monitored systems which is set at 12 years. This is a significant deviation from the yearly activities prescribed by Directory 3. However TFSP believes more credit should be given by providing for longer maintenance intervals for monitored channel health of communication channels. In addition, TFSP will propose the addition of a requirement to Directory 4 requiring the use of monitored communication channels for lines at NPCC BPS stations. 3. Fully monitored communication systems still must be maintained every 12 years in PRC-005-2which is actually more stringent than Directory 3.
5.7	**Underfrequency Load Shedding and Generator Underfrequency Relay Testing Requirements** There are two sub-sections under Section 5.7.		
	5.7.1 Protection group DC circuit tests, battery bank and charger tests and breaker trip tests for protection required by the NPCC Automatic Underfrequency Load Shedding Program, need not be performed more frequently than the protection group DC circuit tests, battery bank and charger tests and breaker trip tests for other protection on the same breaker. Because of the distributed nature of this load shedding protection, random failures to trip do not compromise the objectives of the NPCC Automatic Underfrequency Load Shedding Program.	Table 3. This Section can be removed.	The testing requirements for UFLS in the NERC PRC-005-2 standard for protective relays are in alignment with intervals and activities for BES protective relays. TFSP supports these intervals as previously outlined in the above rationale. PRC-005-2 does not require any testing of DC circuitry between the protective relay/electromechanical auxiliary or lockout relays and the trip coils of non-BES devices. Elimination of this testing which is alluded to in Directory 3 does not pose a significant reliability risk for the very reason outlined in the last sentence of 5.7.1.
	5.7.1 Protection group DC circuit tests, battery bank and	Table 3.	Generator UF relays for generators part of the BES are in

Section	Criteria/Requirement in The Directory	PRC-005-2 Equivalent	Rationale/Justification
	charger tests and breaker trip tests for protection required by the NPCC Automatic Underfrequency Load Shedding Program, need not be performed more frequently than the protection group DC circuit tests, battery bank and charger tests and breaker trip tests for other protection on the same breaker. Because of the distributed nature of this load shedding protection, random failures to trip do not compromise the objectives of the NPCC Automatic Underfrequency Load Shedding Program.	This Section can be removed.	fact included in NERC PRC-005-2 standard and will be on the same maintenance schedule as other BES protective relays. Removing this requirement from Directory 3 does not leave a reliability gap.
Appendix A	**Definition of Terms**	NPCC Glossary of Terms	With the deletion of this Directory, this Appendix no longer serves any purpose.
Appendix B	**Guideline and Procedure for Maintenance of Bulk Power System Protection** This Appendix provides the guidelines and procedures for consideration in the implementation of this Directory. Excerpt of the appendix is not extracted herein.	A stand-alone B or C Document, to be determined.	To be provided.

TFSP Technical Comparison
Directory#3 Maintenance Criteria BPS Protection
PRC-005-2 Protection System Maintenance

Background Information

On March 20th, 2014 FERC issued a Final Rule approving Reliability Standard PRC -005-2 *Protection System Maintenance*.

Accordingly, the TFSP has concluded that subject to the provincial adoption of PRC -005-2 within NPCC no significant reliability gaps exist and the criteria in Directory#3 can be retired.

1. The TFSP has determined that the Directory#3 criteria regarding the frequency of trip coil testing is more stringent than PRC-005-2 (2 years vs. 6 years in the standard). However, for the reasons referenced in the attached report, TFSP concluded that this is not a significant reliability gap and the criteria while more stringent than the standard can be retired.

   Do you agree with the TFSP conclusion?

   Yes ☐

   No ☐

Comments:

2. Currently for teleprotection equipment using Frequency Shift Keying whose channel health is continuously monitored the Directory#3 criteria require verification of the trip function every 12 months vs. the 12 year requirement in PRC-005-2. However the TFSP has concluded that teleprotection equipment whose channel health is continuously monitored can support PRC-005-2 maintenance intervals. Therefore the TFSP has concluded that this is not a significant reliability gap and the criteria while more stringent than the standard can be retired.

   Do you agree with the TFSP conclusion?

   Yes ☐

   No ☐

Comments:

TFSP Technical Comparison
Directory#3 Maintenance Criteria BPS Protection
PRC-005-2 Protection System Maintenance

3. TFSP has recommended the retirement of the criteria portion of Directory 3 on April 1, 2015, which coincides with effective date of PRC-005-2.

   Do you agree with the TFSP recommendation?

   Yes ☐

   No ☐

Comments:

4. Please provide any other comments (that you have not already provided) regarding the TFSP recommendation to retire Directory#3 *Maintenance Criteria for BPS Protection*.

   Yes ☐

   No ☐

Comments:

TFSP Technical Comparison
Directory#3 Maintenance Criteria BPS Protection
PRC-005-2 Protection System Maintenance

Background Information

On March 20th, 2014 FERC issued a Final Rule approving Reliability Standard PRC -005-2 *Protection System Maintenance*.

Accordingly, the TFSP has concluded that subject to the provincial adoption of PRC -005-2 within NPCC no significant reliability gaps exist and the criteria in Directory#3 can be retired.

1. The TFSP has determined that the Directory#3 criteria regarding the frequency of trip coil testing is more stringent than PRC-005-2 (2 years vs. 6 years in the standard). However, for the reasons referenced in the attached report, TFSP concluded that this is not a significant reliability gap and the criteria while more stringent than the standard can be retired.

   Do you agree with the TFSP conclusion?

   Yes ☐

   No ☐

Comments:

2. Currently for teleprotection equipment using Frequency Shift Keying whose channel health is continuously monitored the Directory#3 criteria require verification of the trip function every 12 months vs. the 12 year requirement in PRC-005-2. However the TFSP has concluded that teleprotection equipment whose channel health is continuously monitored can support PRC-005-2 maintenance intervals. Therefore the TFSP has concluded that this is not a significant reliability gap and the criteria while more stringent than the standard can be retired.

   Do you agree with the TFSP conclusion?

   Yes ☐

   No ☐

Comments:

TFSP Technical Comparison
Directory#3 Maintenance Criteria BPS Protection
PRC-005-2 Protection System Maintenance

3. TFSP has recommended the retirement of the criteria portion of Directory 3 on April 1, 2015, which coincides with effective date of PRC-005-2.

   Do you agree with the TFSP recommendation?

   Yes ☐

   No ☐

Comments:

4. Please provide any other comments (that you have not already provided) regarding the TFSP recommendation to retire Directory#3 *Maintenance Criteria for BPS Protection*.

   Yes ☐

   No ☐

Comments:

NPCC Directory Development and Revision Manual
Comments Requested

Background Information

Consistent with NPCC's overall recognition of industry's concern regarding the balance between cost and incremental reliability benefit, the Regional Standards Committee (RSC) has approved revisions to the Directory Development and Revision Manual used to develop and revise the NPCC Criteria. These revisions will incorporate aspects of the NPCC Cost Effectiveness and Analysis Procedure (CEAP) into the Directory Manual.

Additionally, other revisions to the Manual are being proposed in response to separate concerns expressed by NPCC Full Members in various forums.

The following questions have been developed by NPCC Staff in order to solicit further comment from NPCC Members during the Open Process posting to consider these changes.

1. During its review of NPCC Directory#1 the CO7/CP11 Working Group proposed a change to the overall Directory format described in the Directory Manual.

   This change would result in the removal from all NPCC Directories of the section within each Directory that lists the individual NERC Standards associated with the subject Directory.

   Additionally, the CO7/CP11 Working Group also recommended omitting the language within each Directory that refers to more stringent criteria since this language may no longer be accurate given that NERC standards are evolving beyond the criteria.

   CO7/CP11 reasoned that since the criteria contained within a Directory is applicable to the A-10 defined NPCC Bulk Power System (BPS), lists of ERO Standards within a Directory are no longer appropriate.

   Similarly, CO7/CP11 felt that the blanket statement……'These criteria are in addition to, more stringent than, and more specific than NERC standard requirements"….was no longer absolutely true since in some cases the NERC requirements could be more stringent than the criteria.

   Do you agree with the CO7/CP11 suggestion to revise the Directory Manual, such that the lists of individual NERC standards and the language referencing more stringent criteria are removed from each Directory?

   Yes ☐

   No ☐

Comments:

DRAFT

NPCC Directory Development and Revision Manual
Comments Requested

2. The section of the Manual that describes revisions to the Appendix section of a Directory has been revised.

   Formerly, a revision to the Appendix section of a Directory required RCC approval

   The Manual has been revised such that for changes to **only** the Appendix section of a Directory only Task Force approval of such revisions will be required.

   Do you agree with this revision to the Manual?

   Yes ☐

   No ☐

Comments:

3. Regarding the future disposition of NPCC 'B' Guidelines and 'C' Procedures incorporated within Directories as an Appendix and stand- alone B and C Guidelines and Procedures that were never incorporated within a Directory, it has been suggested that all such documents should be contained in a NPCC Reference document.

   The purpose of the Reference document would be to house all documents that support the criteria in one location. In this manner revisions to these documents could be achieved outside the more rigorous approval process for the criteria.

   Do you agree that Appendices should be removed from each of the Directories and included along with remaining B and C documents into a single NPCC Reference document?

   Yes ☐

   No ☐

Comments:

DRAFT

NPCC Directory Development and Revision Manual
Comments Requested

4. Please provide any other comments (that you have not already provided) regarding the RSC proposed revisions to the NPCC *Directory Development and Revision Manual.*

Comments:

DRAFT

NPCC, Inc.

NORTHEAST POWER COORDINATING COUNCIL, INC.
1515 BROADWAY, NEW YORK, NY 10036-8901 TELEPHONE: (212) 840-1070 FAX: (212) 302-2782

Northeast Power Coordinating Council, Inc.

Directory Development and Revision Manual

RSC Approval for Open Process Posting Redlined

June XX, 2014

Approved by the Reliability Standards Committee

October 26, 2011

Revision History

Version	Date	Action	Change Tracking (New, Errata or Revisions)
0	**10/26/2011**	**Effective Date**	**New**
1	**12/5/2013**	**Revised**	**Revised Interpretation Approval Process**

DIRECTORY DEVELOPMENT and REVISION MANUAL

Table of Contents

I. EXECUTIVE SUMMARY 3

II. BACKGROUND ..... ERROR! BOOKMARK NOT DEFINED.

III. APPLICABILITY OF NPCC CRITERIA……..……5

IV. TASK FORCE ROLES AND RESPONSIBILITIES 6

V. DIRECTORY DEVELOPMENT AND REVISION PROCEDURE 7

1. NEW DIRECTORY 7

2. DIRECTORY REVISIONS 10

a. Revisions to the Criteria Section of a Directory 10

b. Revisions to the Appendix Section of a Directory 12

c. Revisions to the NPCC Glossary Of Terms 14

d. Withdrawal of Revision Requests 17

3. DIRECTORY RETIREMENT 17

4. MAINTENANCE OF ERRATA AND LINKS 14

VI. DIRECTORY CLARIFICATION PROCESS 18

a. *Request for Criteria Clarification* 18

b. *Appeals*……..16

VII. REVIEW AND APPROVAL OF THE NPCC DIRECTORY MANUAL 20

VIII. DIRECTORY FORMAT AND VERSION CONTROL 21

IX. REFERENCES: 21

APPENDIX A - DIRECTORY FORMAT TEMPLATE 22

APPENDIX B – NPCC REQUEST FOR CLARIFICATION 26

I. EXECUTIVE SUMMARY

The purpose of the Northeast Power Coordinating Council, Inc. ("NPCC") is to enhance the reliability of the international, interconnected bulk power system in Northeastern North America through the development of more stringent and regionally specific criteria.

NPCC Directories have been developed in order to provide a consistent and comprehensive set of reliability requirements for the Northeast, while consolidating related information for NPCC Criteria, Guidelines, Procedures as well as FERC and NERC approved Regional Standards into one document.

~~NPCC Directories and the criteria contained within, apply only to NPCC Full Members. However, there may be additional requirements within tariffs or interconnection agreements that hold non-Members responsible for complying with the criteria within each Directory.~~

This document provides guidance to NPCC Task Forces~~,~~ and NPCC Full Members when establishing a new or revised Directory~~, or~~ when retiring or consolidating an existing Directory and also clarifies the roles and responsibilities of the NPCC Task Forces responsible for Directory content.

The NPCC Regional Standards Committee (RSC) working with the lead Task Force for each Directory has overall responsibility for managing the Directory project. Individual Directories are under the control of a lead NPCC Task Force which is responsible for coordinating review among all other Task Forces which have jurisdiction over either a portion of the criteria or one or more of the Appendices in the Directory.

NPCC also recognizes the industry concern surrounding the cost of maintaining the more stringent or more specific NPCC criteria contained within the NPCC Directories and the the NPCC Board of Directors has expressed strong support for the appropriate balance between the incremental reliability benefit achieved by the criteria versus the cost to maintain or implement those criteria.

Accordingly, the fundamental review methodology of the NPCC Cost Effectiveness Analysis Procedure (CEAP) has been incorporated into the Directory Development and Revision Manual.

II. BACKGROUND

NPCC Directories have been developed consistent with the NPCC Bylaws which provide for the establishment of regionally specific reliability criteria, guidelines and procedures and within each Directory NPCC's reliability criteria has been reviewed and translated to insure that the criteria is not inconsistent with the ERO standards as required by the NERC Rules of Procedure.

Each Directory also contains former B and C documents which have been renamed as Appendices and are functionally relevant to the documents criteria. Consistent with NPCC Document A-1 *Criteria for Review and Approval of Documents* the purpose of an Appendix continues to support the achievement of system performance related to the criteria and the consistent implementation, interpretation and monitoring of the criteria requirements.

Phase 1 of the Directory Project was initiated by the NPCC Reliability Coordinating Committee (RCC) in order to demonstrate consistency with NERC Standards and to effectively group documents together according to functional topics. During Phase 1 an initial translation of the existing criteria document was performed in addition to identifying and eliminating language within the criteria that duplicated existing NERC Reliability Standards.

Also during Phase 1, Functional Model language was introduced and the corresponding 'B' Guidelines and 'C' Procedures were incorporated into each Directory as Appendices.

The resulting Directory created a single source reference for all entities while providing a method to demonstrate consistency with NERC Standards.

Phase 2 of the Directory Project was initiated in order to reformat the Criteria section of each document into specific and measurable NERC style requirements which will promote the NPCC regional criteria as more specific or more stringent within each Directory. Phase 2 will also facilitate the development of the NPCC Criteria Compliance Enforcement Program (CCEP) by providing the respective requirements of that program.

A mapping document has been provided on the Directory page of the NPCC Website and has been organized in a manner that provides guidance on where a Directory's content originated (A Criteria, B Guideline, or C Procedure). The mapping document provides tracking of specific content language from documents that were translated or replaced by

Directories and their Appendices. A link to the Directory Flowchart and the Directory Mapping documents is provided in the References section of this manual.

All of NPCC'S A criteria documents except A-1 (*Criteria for Review and Approval of Documents*), A-10 (*Classification of BPS Elements*) and A-15 (*Disturbance Monitoring Equipment Criteria)* documents, all of NPCC's A criteria documents have been translated into the Directories. However, although ma ny of the B Guideline and C Procedure documents have been transferred to Directories as Appendices in support of the relevant criteria, not all B and C documents were determined to be related to a Directory and as a result some stand- alone B Guideline and C Procedure documents will remain at the conclusion of the Directory project.

~~The NPCC Regional Standards Committee (RSC) working with the lead Task Force for each Directory has overall responsibility for managing the Directory project.~~

~~The Directories are organized to demonstrate that NPCC regional criteria are more specific than and/or more stringent than and consistent with NERC Reliability Standards.~~

~~Each Directory contains an Introduction, along with sections that identify NERC ERO Standards and NPCC Regional Standards that are associated with the Directory~~.

~~Additionally, each Directory is comprised of a section that describes the NPCC regionally specific criteria and was developed from the related NPCC 'A' documents.~~

~~The appropriate Type 'B' Guideline and Type 'C' Procedure documents are also included within each Directory as Appendices. Although the Appendices in a Directory are functionally associated with the subject criteria in the document, they do not contain NPCC criteria and are included within the Directory in order to achieve acceptable performance and consistent implementation of the criteria.~~

~~A mapping document has been provided on the Directory page of the NPCC Website and has been organized in a manner that provides guidance on where a Directory's content originated (A Criteria, B Guideline, or C Procedure).~~

~~The mapping document provides tracking of specific content language from documents that were translated or replaced by Directories and their Appendices. A link to the Directory Flowchart and the Directory Mapping documents is provided in the References section of this manual.~~

~~Phase 1 of the Directory Project was initiated by the NPCC Reliability Coordinating Committee (RCC) in order to demonstrate consistency with NERC Standards and to effectively group documents together according to functional topics.~~

~~During Phase 1 an initial translation of the existing criteria document was performed in addition to identifying and eliminating language within the criteria that duplicated existing NERC Reliability Standards.~~

~~Additionally, Functional Model language was introduced and the corresponding 'B' Guidelines and 'C' Procedures were incorporated into each Directory as appendices.~~

~~The resulting Directory created a single source reference for all entities while providing a method to demonstrate consistency with NERC Standards.~~

~~Phase 2 of the Directory Project was initiated in order to reformat the Criteria section of each document into specific and measurable NERC style requirements which will~~

~~promote the NPCC regional criteria as more specific or more stringent within each Directory.~~

~~Phase 2 will also facilitate the development of the NPCC Criteria Compliance Enforcement Program (CCEP) by providing the respective requirements of that program.~~

~~Although the Regional Standards Committee is responsible for the overall Directory program, individual Directories are under the control of a lead NPCC Task Force which is responsible for coordinating review among all other Task Forces which have jurisdiction over either a portion of the criteria or one or more of the Appendices in the Directory.~~

~~IV.~~III. APPLICABILITY OF NPCC CRITERIA

The requirements of an NPCC Directory apply only to those facilities defined as NPCC bulk power system elements and identified through the performance based methodology of NPCC Document A-10, "Classification of Bulk Power System Elements," the list of which is maintained by the NPCC Task Force on System Studies and approved by the NPCC Reliability Coordinating Committee.

Requirements to abide by an NPCC Directory may also reside in external tariff requirements, bilateral contracts and other agreements between facility owners and/or operators and their assigned Reliability Coordinator, Planning Coordinator, Transmission Operator, Balancing Authority and/or Transmission Owner as applicable and may be enforceable through those external tariff requirements, bilateral contracts and other agreements. NPCC will not enforce compliance to the NPCC Directory requirements in this document on any entity that is not an NPCC Full Member.

IV. TASK FORCE ROLES AND RESPONSIBILITIES:

Formatted: Heading 1, Numbered + Level: 1 + Numbering Style: I, II, III, … + Start at: 1 + Alignment: Right + Aligned at: 0" + Indent at: 0.25"

Formatted: Font: (Default) New York, Font color: Black

With the development of the Directories it has been recognized that in certain cases the jurisdictional boundaries of Task Force ownership have been crossed and additional guidance when coordinating Directory review among Task Forces is necessary.

In general, revisions and clarifications to a Directory shall be coordinated by the Lead Task Force of the document. Revisions to a Directory can be initiated in a fully bi-directional manner; that is either by the Lead Task Force responsible for the document or by another Task Force who is responsible for some portion (criteria or appendices) of the document.

This process will allow each Directory to remain under the control of the respective Lead Task Force which has the necessary expertise to keep each document current and accurate while also providing a means to coordinate component review of those segments of the Directory that may be under the control of another Task Force.

The Lead Task Force can initiate a full revision of the Directory in accordance with the NPCC Reliability Assessment Program (NRAP) date of approval or some need to revise the criteria section of the document. A link to the NRAP documents is provided in the References section of this manual.

The Lead Task Force will also notify other Task Forces under whose jurisdiction either a portion of the criteria or Appendices exists in order to coordinate the total document review and revision. Similarly, a Task Force which is not the Lead Task Force of the Directory, but is responsible for some portion of the document, shall coordinate a necessary revision to their section of the document through the Lead Task Force of the Directory.

V. DIRECTORY DEVELOPMENT AND REVISION PROCEDURE

1. NEW DIRECTORY

Any NPCC Full Member may request the development of a new Directory.

The request shall be made to the NPCC Manager of Reliability Criteria via email and shall contain the background and justification for the development of the new Directory. The NPCC Manager of Reliability Criteria shall forward the request to the Regional Standards Committee (RSC) in order for the RSC to review the request and assign its development to the appropriate NPCC Task Force.

Included in the transmittal of the request to the RSC, the NPCC Manager of Reliability Criteria shall request the RSC to authorize a Cost Effectiveness Analysis utilizing the NPCC CEAP procedure for this evaluation. The Lead Task Force responsible for developing the new Directory shall draft an initial version of the document consistent with the Directory template in Attachment A.

The RSC working with the NPCC Standards Program Area shall utilize the NPCC CEAP to perform an initial analysis of the cost benefit of the proposed Directory via the Cost Benefit Analysis (CBA) section of the CEAP. Subsequent to RSC review and approval of the CBA the NPCC Manager of Reliability Criteria shall post the draft Directory to the NPCC Open Process for 45 days.

At the conclusion of the 45 day Open Process ~~,~~ period, the Lead Task Force will discuss the comments submitted and deliberate on whether the criteria requirements are developed enough to begin the Cost Effectiveness Analysis (CEA) portion of the CEAP and where appropriate request the RSC to initiate the CEA.

~~post responses to comments on the NPCC Open Process portal.~~

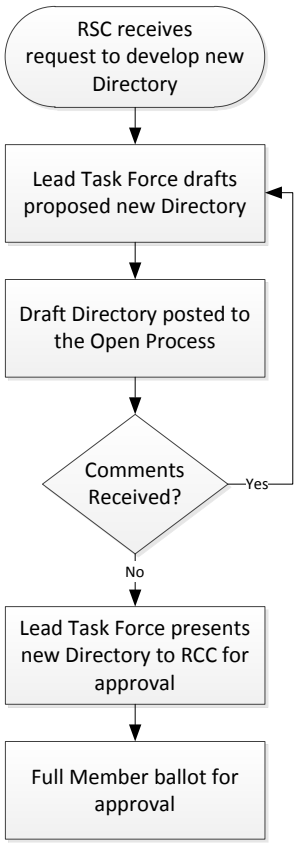
If the responses to comments received on the draft result in substantive changes to the document, then the revised draft shall be reposted to the Open Process for a successive 45 day posting period. Alternatively, i~~I~~f no substantive changes are developed which would require additional postings of a revised draft, the new Directory is presented to the Reliability Coordinating Council (RCC) for approval.

Additionally, the RSC in accordance with the CEAP will use the responses to the CEA survey to develop a recommendation based on the cost effectiveness of the proposed Directory. Upon RCC approval the document is submitted for a ballot to the NPCC Full Member Representatives along with the RCC recommendation of approval.[1]

The process for establishing a new Directory is represented below in Figure 1:

[1] Approval of a new or revised Directory requires a 2/3rd majority of Full Member voting representatives in accordance with the NPCC Bylaws.

Figure 1: New Directory



2. DIRECTORY REVISIONS

a. REVISIONS TO THE CRITERIA SECTION OF A DIRECTORY

Any NPCC Full Member may request a revision to the criteria within a Directory. A request to revise the criteria section of an NPCC Directory shall be submitted to the Lead Task Force responsible for the document. The Lead Task Force shall notify each affected NPCC Task Force which has jurisdiction over either a portion of the criteria or one or more of the appendices within the Directory that a request to revise the criteria in the document has been received.

The Lead Task Force shall review the request to revise the criteria and shall also consider conforming changes to appendices as a result of the criteria revision if necessary.

The NPCC Manager of Reliability Criteria shall post the Directory containing the revised criteria to the NPCC Open Process review for 45 days.

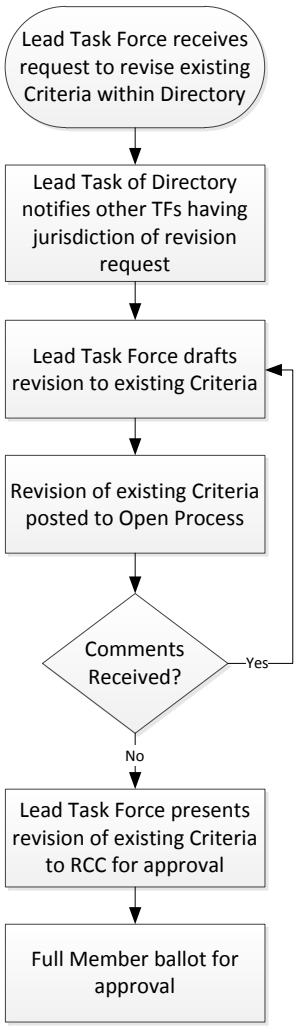
At the conclusion of the 45 day Open Process, the Lead Task Force will discuss the comments submitted and post responses to comments on the NPCC Open Process portal. If the responses to the comments received on the criteria revision result in substantive changes to the document, then the revised Directory criteria shall be reposted to the Open Process for a successive 45 day posting period.

Alternatively, i~~I~~f no substantive changes are developed which would require additional postings of a revised draft of the Directory, then the Directory is presented to the Reliability Coordinating Council (RCC) for approval.Upon RCC approval the document is submitted for a ballot to the NPCC Full Member Representatives along with the RCC recommendation of approval.

Approval of the revised Directory criteria requires a 2/3rd majority of Full Member voting representatives in accordance with the NPCC Bylaws.

The process for revisions to the criteria in an existing Directory is represented below in Figure 2:

Figure 2: Revisions to Criteria



b. REVISIONS TO THE APPENDIX SECTION OF A DIRECTORY

Any NPCC Full Member may request an Appendix within a Directory to be revised or retired. Revisions or retirements of Appendices shall only require Task Force ~~RCC~~ approval.

A request to revise or retire an Appendix of a NPCC Directory shall be submitted to the Task Force responsible for the Appendix. The Task Force responsible for the Appendix shall notify the Lead Task Force of the Directory that a request to revise or retire an appendix within the document has been received.

The Lead Task Force of the Directory shall be responsible for notifying all Task Forces which have jurisdiction over either the criteria or one or more of the other Appendices within the Directory that a request to revise or retire an appendix has been received.

After the Task Force responsible for the revised Appendix request reviews the subject appendix they will forward the Directory containing the draft revised Appendix to the Lead Task Force of the Directory.The Lead Task Force shall be responsible for posting the Directory which contains the revised or retired Appendix to the NPCC Open Process review for 45 days. **Additionally, although the entire Directory will be posted to the open process, the Lead Task Force will limit the comments solicited to only the subject Appendix.**

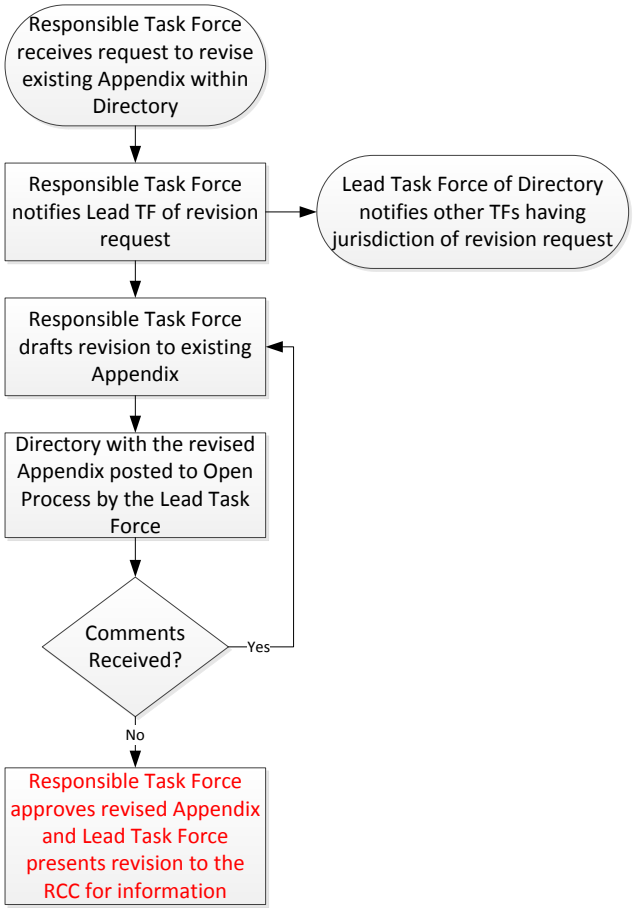
Formatted: Font: Bold

At the conclusion of the 45 day Open Process, the Lead Task Force will forward the comments submitted on the Appendix to the Task Force responsible for the revised or retired Appendix. If the responses to the comments received on the revised or retired Appendix result in substantive change (s) to the Appendix, then the Directory containing the revised or retired Appendix shall be reposted to the Open Process for a successive 45 day review period by the Lead Task Force of the entire Directory. Alternatively, ~~;~~ if no substantive changes are developed which would require additional postings the revised or retired Appendix shall be voted on by the Task Force responsible for the Appendix.

The lead Task Force for the Directory containing the revised or retired Appendix shall distribute the Directory containing the revised or retired Appendix to the Reliability Coordinating committee for informational purposes.~~entire Directory containing the draft of the revised or retired Appendix will be presented to the Reliability Coordinating Council (RCC) for approval~~.

The process for revisions to the appendices within an existing Directory is represented below in Figure 3:

Figure 3: Revisions to Appendices


Responsible Task Force receives request to revise existing Appendix within Directory
Responsible Task Force notifies Lead TF of revision request
Lead Task Force of Directory notifies other TFs having jurisdiction of revision request
Responsible Task Force drafts revision to existing Appendix
Directory with the revised Appendix posted to Open Process by the Lead Task Force
Comments Received?
Yes
No
Responsible Task Force approves revised Appendix and Lead Task Force presents revision to the RCC for information

c. REVISIONS TO THE NPCC GLOSSARY OF TERMS

The NPCC Glossary of Terms contains the definitions of all terms found within the NPCC Directories, Criteria, Guidelines, and Procedures and which are not already defined in the NERC Glossary of Terms or are regionally specific. The Glossary of Terms is intended to be a repository of all NPCC defined terms and contains the Full Member approved definition of that term as developed by the Task Force responsible for the Directory in which the term resides.

The Glossary is organized into two sections, one containing all defined terms within the Directories (including Appendices) which support the NPCC Criteria and another section for definitions found within remaining B and C documents.

The process of establishing or revising a NPCC defined term shall be considered a revision to the Directory in which the term resides in order to capture the context of its use within the document. Accordingly, the entire Glossary is not subject to the Open Process for a revision to an individual definition.

The development and review of a new definition or a revision to an existing NPCC specific definition contained within the Glossary will be coordinated by the Lead Task Force for the Directory in which the defined term resides.

Any NPCC Full Member may request that a new or revised term be added to the NPCC Glossary of Terms by forwarding a request to the Lead Task Force for the Directory in which the defined term resides. When the subject term resides in multiple Directories, the requestor shall forward the request to each of the Task Forces for the Directories in which the defined term resides and the individual Task Forces shall coordinate their review of the request, by assigning one of the Task Forces as the Lead Task Force for the review.

After the Lead Task Force in which the defined term resides has completed its review they will post the subject Directory containing the new or revised term to the NPCC Open Process for 45 days. When the new or revised term appears in multiple Directories, the designated Lead Task Force for the review shall include in the posting notice a comprehensive list of references to all occurrences of the defined term in other NPCC Directories, including each Directory in which the term resides.

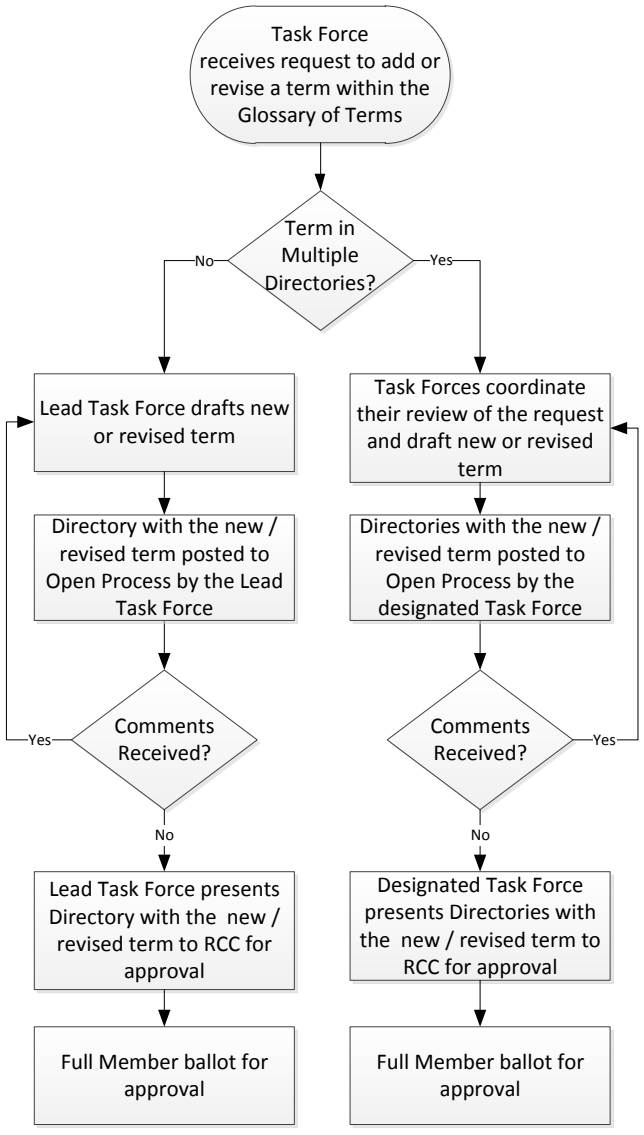
At the conclusion of the 45 day Open Process, if responses to comments received on the new or revised term result in further substantive change to the term, then the Directory containing the new or revised term shall be reposted to the Open Process for a successive 45 day posting period by the Lead Task Force for the subject Directory. Alternatively, ~~;~~ if no substantive changes to the term are developed which would require an additional

posting, then the Directory containing the new or revised term will be presented to the Reliability Coordinating Council (RCC) by the Lead Task Force for approval.

Upon RCC recommendation the Directory containing the new or revised term will be balloted by the Full Members. Upon Full Member approval of the new or revised term the Glossary will be updated by the Lead Task Force of the document in which the term resides.

The process for revisions to the Glossary of Terms is represented below in Figure 4:

Figure 4: Revisions to the NPCC Glossary of Terms



d. Withdrawal Of Revision Requests

Any NPCC Full Member which has initiated a request to develop a new Directory, revise an existing Directory or revise an NPCC Glossary Term may withdraw the request by notifying the NPCC Manager of Reliability Criteria.

3. Directory Retirement

Upon identification of the need to retire an existing Directory, the Lead Task Force responsible for the Directory shall notify the NPCC Manager of Reliability Criteria of its proposal to retire a Directory.

The proposal shall include the rationale for the retirement and a statement regarding the impact of retirement on the reliability of the Bulk Power System. The NPCC Manager of Reliability Criteria shall post the proposal, along with supporting documentation to the NPCC Open Process for 45 days.

At the conclusion of the 45 day Open Process, the Lead Task Force will review the comments submitted and post responses on the NPCC Open Process portal. The NPCC Manager of Reliability Criteria shall present the proposal to retire the Directory to the Reliability Coordinating Council (RCC) for approval.

Upon RCC approval the proposal to retire the Directory will be submitted for a ballot to the NPCC Full Member Representatives along with the RCC recommendation to retire the document.

4. Maintenance of Links and Errata

The maintenance of Links and the correction of errors found in a Directory or its Appendices shall be the responsibility of NPCC Standards staff. An error may be classified as Errata provided its correction does not change the scope or intent of the Directory and has no impact on the end user of the Directory.

Errata and Link revisions are updated as needed and require only the Lead TF approval prior to publishing and notifications to the applicable regulatory jurisdictions if required.

NPCC staff will also maintain a record of the change on the Directory Revision History page within the document.

VI. DIRECTORY CLARIFICATION PROCESS

a. REQUEST FOR CRITERIA CLARIFICATION

Any NPCC Full Member may request a clarification of the criteria within a Directory.

The NPCC Full Member seeking the clarification shall submit a ***Request for Criteria Clarification*** form [2] to the NPCC Manager of Reliability Criteria explaining the clarification required and the specific circumstances surrounding the request. The NPCC Manager of Reliability Criteria shall review the request and work with the originator to make certain that the request is clearly written, seeks clarity regarding the intent or purpose of the criteria and is not a question on a compliance aspect of the criteria.

The Manager of Reliability Criteria shall notify the originator of the *Request for Criteria Clarification* if the Request has been denied by providing the originator with a written response explaining the circumstances of the denial.

The Manager of Reliability Criteria will forward an approved *Request for Criteria Clarification* to the NPCC Task Force designated as the Lead Task Force for the subject Directory. The Lead Task Force shall notify each NPCC Task Force which has jurisdiction over either another portion of the criteria and /or one or more of the appendices within the subject Directory, that a ***Request for Criteria Clarification*** has been received. The Lead Task Force shall also forward the request to the affected Task Force(s).

The Lead Task Force for the Directory or the Task Force having jurisdiction shall review the request among its Members and provide a response to the NPCC Manager of Reliability Criteria within 60 calendar days. The Manager of Reliability Criteria shall post the ***Request for Criteria Clarification***, along with the response(s) provided by the Lead Task Force to the NPCC Open Process for 45 days.

[2] The Request for Clarification Form is included in Appendix B of this document.

The Lead Task Force will consider all comments received on the posted clarification and if necessary revise the clarification based on these comments. If the Lead Task Force revises the clarification substantively on the basis of comments received the clarification shall be reposted to the NPCC Open Process for a successive 45 day posting period.

The Manager of Reliability Criteria will coordinate a response to all commenters on behalf of the Lead Task Force.The Lead Task Force response to a Directory clarification request shall provide the requested explanation without expanding on the criteria and should be sufficiently concise to eliminate any ambiguity.

The NPCC Manager of Reliability Criteria shall review the clarification provided by the Lead Task Force or the Task Force having jurisdiction to insure that it is clear and provides the requested explanation without expanding on the criteria.

The Lead Task Force response to a ***Request for Criteria Clarification*** shall be presented to the NPCC Reliability Coordinating Committee (RCC) for final approval prior to posting the clarification to the NPCC website.

The detailed results of the ***Request for Criteria Clarification*** shall be retained by the Lead Task Force and the NPCC Standards Staff along with a recommendation on whether the language within the document should be revised in order to provide additional clarity.

b. APPEALS

Any NPCC Full Member that has submitted a ***Request for Clarification*** may appeal the rendered Task Force response.

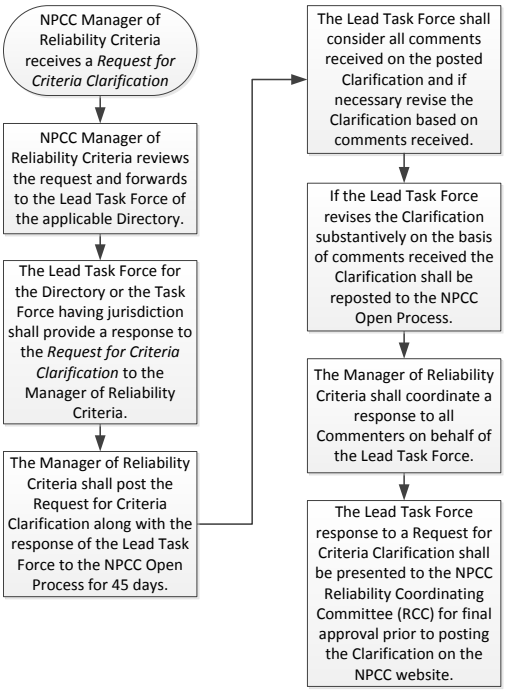
The appellant shall submit a written complaint to the NPCC Manager of Reliability Criteria describing the substantive or procedural action or inaction associated with the Clarification Request process.

The appellant shall also describe in the complaint the actual or potential adverse impact to the appellant.

Assisted by any necessary NPCC Standards Staff and Lead Task Force resources, the NPCC Manager of Reliability Criteria shall prepare a written response addressed to the appellant as soon as practical, but not more than forty-five (45) calendar days after receipt of the complaint.

The process for a Criteria Clarification Request is represented below in Figure 5:

Figure 5: Request for Criteria Clarification



VII. REVIEW AND APPROVAL OF THE NPCC DIRECTORY DEVELOPMENT AND REVISION MANUAL

The NPCC Directory Development and Revision Manual will be reviewed for possible revisions at least once every five (5) years or more frequently if required.

A notification of a pending RSC review and re-approval of the Manual shall be posted on the NPCC website. All revisions to this Manual shall be posted to the NPCC Open Process Review for 45 days.

The Regional Standards Committee (RSC) shall respond to all comments received and shall have final approval over the revised document.

VIII. DIRECTORY FORMAT AND VERSION CONTROL

Each Directory will be formatted in accordance with the Directory Template in Appendix A of this document.

The Task Force Revision Review Record on the cover page of each Directory shall contain the date of the most recent version of the Directory as approved by the Full Members of NPCC.

The Revision History record on page 2 of each Directory shall contain a record of all revisions to the document, including maintenance of errata and links.

IX. REFERENCES:

1. https://www.npcc.org/Standards/Directories/Directory_Flowchart.pdf.
2. https://www.npcc.org/Standards/Directories/Directory_Mapping.pdf.
3. https://www.npcc.org/Library/NRAP/Forms/Public%20List.aspx

APPENDIX A - DIRECTORY FORMAT TEMPLATE

NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

NPCC
Regional Reliability Reference Directory # XX

Task Force XXXXX Revision Review Record:
XX/XX, 20XX

Adopted by the Members of the Northeast Power Coordinating Council, Inc. June 26th, 2009 based on recommendation by the Reliability Coordinating Committee, in accordance with Section VIII of the NPCC Amended and Restated Bylaws dated July 24, 2007 as amended to date.

Revision History

Version	Date	Action	Change Tracking (New, Errata or Revisions)
0		**Effective Date**	**New**

Format for NPCC Directories (Phase 2)

Effective Dates (Denotes date of adoption by the Membership)

Revision History (Depicts revision history and tracks key changes)

Table of Content (Self-explanatory)

A. Introduction

Title: Self-explanatory

Directory #: Self-explanatory

Objective: State the reliability objective that this Directory intended to meet (i.e., achieving specific performance target/outcome, mitigating particular risks, establishing the minimum capability level, etc.)

Effective Date: Identify which parts of the Directory become effective on which dates.

Background: Provide information related to this creation or revision of this Directory, e.g., which A, B or C documents are mapped into this Directory; the general basis of the Directory, etc.

Applicability: Identify the entities that are assigned reliability requirements and/or which facilities need to conform to the stipulated criteria.

B. NERC ERO Reliability Standard Requirements

A list of the NERC standards associated with this Directory.

C. NPCC Regional Reliability Standard Requirements

A list of NPCC Regional Standards associated with this Directory.

D. NPCC Full Member, More Stringent Requirements, Criteria and Measures

Requirements

List the requirements and criteria that the applicable entities or facilities must comply with.

E. Compliance

Compliance with the requirements set forth in this Directory will be in accordance with the NPCC Criteria Compliance and Enforcement Program (CCEP).

Measures and corresponding Levels of Non Compliance for these requirements are contained within the compliance template associated with this Directory.

Prepared by:	Task Force XX (Lead Task Force for the Directory)
Review and Approval:	Revision to any portion of this Directory will in accordance with the NPCC Directory Development and Revision Manual and will be posted by the Lead Task Force in the NPCC Open Process for a 45 day review and comment period. Upon satisfactorily addressing all of the comments in this forum, the Directory will be sent to the RCC for its approval. Upon approval of the RCC, this Directory will be sent to the Full Member Representatives for their final approval if sections pertaining to the Requirements and Criteria portion have been revised. All voting and approvals will be conducted according to the most current "NPCC. Bylaws" in effect at the time the ballots are cast. Revisions pertaining to the Appendices or any other portion of the document such as links, glossary terms, etc., only RCC Members will need to conduct the final approval ballot of the document. This Directory will be updated at least once every three years and as often as necessary to keep it current and consistent with NERC, Regional Reliability Standards and other NPCC documents.

APPENDIX B – NPCC REQUEST FOR CLARIFICATION

NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

NPCC Request for Criteria Clarification

Note: an Interpretation cannot be used to revise a Directory.

Request for Criteria Clarification of a Directory
Date clarification request submitted: Date clarification response provided:
Contact information for person requesting the clarification:
Name:
Organization:
Telephone:
E-mail:
Identify the Directory that needs clarification:
Directory Number :
Directory Title:
Identify specifically what portion of the Criteria needs clarification:
Text of Requirement:
Identify the material impact associated with this clarification:
Identify the material impact to your organization or others caused by the lack of clarity within this Directory:

Submit completed Request for Criteria Clarification forms to the NPCC Manager of Reliability Criteria.

Clarification: Response to Request for Clarification of Directory XX for the XXXX Corporation
The following clarification of Directory was developed by the Task Force on XXXXX
Directory Number and Text of Requirement
Question 1
Response to Question 1
Question 2
Response to Question 2

NPCC, Inc.

NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

June 11th, 2014

Members Regional Standards Committee

Re: NPCC Directory Development and Revision Manual

Ladies and Gentlemen:

Consistent with NPCC's overall recognition of the need to balance cost and incremental reliability benefit, the Directory Development and Revision Manual has been revised to incorporate provisions of the NPCC Cost Effectiveness and Analysis Procedure (CEAP) into the section of the Manual that governs the development of new criteria.

Accordingly, the concept of cost consideration has been introduced into the Executive Summary section of the Manual, along with specific steps related to the CEAP in the section of the Manual that addresses the development of new criteria.

Additionally, other revisions to the Manual are being proposed in response to separate concerns expressed by NPCC Full Members in various forums including:

- The addition of a new section addressing the applicability of NPCC criteria.
- Clarification of the disposition of NPCC B Procedures and C Guideline documents (or Appendices when contained within a Directory.) in the Background section of the Manual.
- Revisions to the approval process for Directory Appendices.
- Elimination of the section of a Directory that lists the associated NERC Standards.

The RSC has overall responsibility for managing the NPCC Directories and upon RSC endorsement these revisions will be posted to the NPCC Open Process to receive Full Member comments.

Very truly yours,

Gerry Dunbar
Manager, Reliability Criteria
Northeast Power Coordinating Council, Inc.

cc: RSC, Regional Standards Committee

REGIONAL STANDARDS COMMITTEE

Chairman:

Guy V. Zito
Assistant Vice President - Standards
Northeast Power Coordinating Council, Inc.
Tel. (212) 840-1070
Email: gzito@npcc.org

Co-Vice Chairman:

Gregory A. Campoli
Supervisor, Reliability Compliance & Assessment
New York Independent System Operator
Tel. (518) 356-6159
Email: gcampoli@nyiso.com

Co-Vice Chairman:

Bruce Metruck
NERC Compliance Program Manager II
New York Power Authority
F.R. Clark Energy Center
6520 Glass Factory Road
Marcy, NY 13403
Tel. (315) 792-8213
Email: bruce.metruck@nypa.gov

Sector 1 - Transmission Owners

Hydro One Networks, Inc.

Primary
Ayesha Sabouba, P. Eng., MBA
Manager - Policy and Reliability Standards Compliance
Tel. (416) 345-5267
Email: asabouba@HydroOne.com

Alternate
Muhammed Ali
Network Management Engineer – Reliability Standards and Compliance Department
Tel. (416) 345-5856
Email: muhammed.ali@hydroone.com

Consolidated Edison Company of New York, Inc.

Primary
Christopher L. de Graffenried
Senior Engineer Transmission Planning
Room 1300, 13th Floor - Northwest
Tel. (212) 460-2925
Email: degraffenriedc@coned.com

Alternate
Peter Yost
Manager, Standards & Compliance
Tel. (212) 460-2889
Fax (212) 529-1130
Email: yostp@coned.com

National Grid

Primary
Brian Shanahan
Tel. (315) 460-2346
Email: brian.shanahan@nationalgrid.com

Alternate
Michael Jones
Lead Analyst – FERC Compliance
40 Sylvan Road
Waltham, Massachusetts 02451
Tel. (781) 907-2404
Email: michael.jones@nationalgrid.com

New Brunswick Power Corporation

Primary
Alan MacNaughton, P.Eng.
Senior Compliance Engineer
Tel. (506) 443-6577
Email: amacnaughton@nbpower.com

Alternate

The United Illuminating Company

Primary
Robert J. Pellegrini
ES Asset Management
Manager Protection &Control/ SCADA
180 Marsh Hill Road
Orange, Connecticut 06477
Tel. (203) 499-2413
Email: Robert.pellegrini@uinet.com

Alternate

Hydro-Quebec TransÉnergie

Primary
Sylvain Clermont
Manager Transmission Services
Tel. (514) 879-4648
Email: clermont.sylvain@hydro.qc.ca

Alternate
Si Truc Phan
2 Complexe Desjardins, 19th floor, East Tower
Montreal, Québec, Canada H5B 1H7
Tel. (514) 879-4100 Ext. 3610
Email: phan.si_truc@hydro.qc.ca

Orange & Rockland Utilities, Inc.

Primary
Ben Wu
Transmission & Substation Engineering
Tel. (845) 577-3713
Email: WUB@oru.com

Alternate

Northeast Utilities

Primary
Mark J. Kenny
Program Manager - Reliability Compliance
Tel. (781) 441-8179
Email: Mark.Kenny@nu.com

Alternate

Sector (2) - Reliability Coordinators

New York Independent System Operator

Primary
Gregory A. Campoli
Supervisor, Reliability Compliance & Assessment
Tel. (518) 356-6159
Email: gcampoli@nyiso.com

Alternate
James (Jim) Grant
Reliability Senior Engineer
Tel. (518) 356-6128
Email: jgrant@nyiso.com

ISO New England, Inc.

Primary
Kathleen M. Goodman
Senior Operations Compliance Coordinator
Tel. (413) 535-4111
Email: kgoodman@iso-ne.com

Alternate
Matthew Goldberg
Director of Reliability & Operations Compliance
Tel. (413) 535-4029
Email: mgoldberg@iso-ne.com

Independent Electricity System Operator

Primary
Helen Lainis
Senior Engineer/Technical Officer
Tel. (905) 855-4106
Email: helen.lainis@ieso.ca

Alternate
Scott Berry
Senior Engineer/Technical Officer
Tel. (905) 403-6912
Email: scott.berry@ieso.ca

Hydro-Quebec TransÉnergie

Primary
Si Truc Phan
2 Complexe Desjardins, 19th floor, East Tower
Montreal, Québec, Canada H5B 1H7
Tel. (514) 879-4100 Ext. 3610
Email: phan.si_truc@hydro.qc.ca

Alternate
Chantal Mazza
Direction Contrôle des Mouvements d'énergie
C.P. 10000, succ. pl Desjardins
Complexe Desjardins 19th floor
Montréal, QC H5B 1H7
Tel. (514) 879-4100 Ext. 5499
Email: mazza.chantal@hydro.qc.ca

Sector (3) - Transmission Dependent Utilities ("TDUs"); Distribution Companies and Load-Serving Entities ("LSEs")

Consolidated Edison Company of New York, Inc.

Primary
Peter Yost
Manager, Standards & Compliance
Tel. (212) 460-2889
Fax (212) 529-1130
Email: yostp@coned.com

Alternate
Christopher L. de Graffenried
Senior Engineer Transmission Planning
Room 1300, 13th Floor - Northwest
Tel. (212) 460-2925
Email: degraffenriedc@coned.com

National Grid

Primary
Michael Jones
Lead Analyst – FERC Compliance
40 Sylvan Road
Waltham, Massachusetts 02451
Tel. (781) 907-2404
Email: michael.jones@nationalgrid.com

Alternate
Brian Shanahan
Tel. (315) 460-2346
Email: brian.shanahan@nationalgrid.com

Orange & Rockland Utilities, Inc.

Primary
David Burke
Senior Specialist - Compliance
Tel. (845) 577-2841
Fax (845) 577-2840
Email: burkeda@oru.com

Alternate
Thomas Neglia
Senior Specialist – Compliance
Tel. (845)-577-2839
Email: NegliaT@oru.com

Sector (4) - Generator Owners

New York Power Authority

Primary
Wayne Sipperly
NERC Compliance Program Manager II
Tel. (914) 287-3753
Email: wayne.sipperly@nypa.gov

Alternate
Shivaz Chopra
RSC Engineer II, Technical Compliance
Tel. (914) 681-6828
Email: shivaz.chopra@nypa.gov

PSEG Power Connecticut, LLC

Primary
Christy Koncz
NERC Compliance Specialist
80 Park Plaza, T2B
Newark, NJ 07102
Tel. (973) 430-7576
Email: christina.koncz@pseg.com

Alternate

Dominion Resources Services, Inc.

Primary
Mike Garton
NERC Compliance Policy Manager
120 Tredegar Street, RS-6th
Richmond, VA 23219
Tel. (804) 819-2336
Email: mike.garton@dom.com

Alternate

Ontario Power Generation, Inc.

Primary
David Ramkalawan, P.Eng.
Senior Manager - Reliability Compliance
Tel. (416) 592-6089
Email: david.ramkalawan@opg.com

Alternate

NextEra Energy, LLC

Primary
Silvia Parada Mitchell
Director Reliability Standards & Compliance
Tel. (561) 694-4414
Email: silvia.parada.mitchell@fpl.com

Alternate

Sector (5) - Marketers, Brokers and Aggregators

New York Power Authority

Primary
Bruce Metruck
NERC Compliance Program Manager II
F.R. Clark Energy Center
6520 Glass Factory Road
Marcy, NY 13403
Tel. (315) 792-8213
Email: bruce.metruck@nypa.gov

Alternate
Daniella Piper
Reliability Standards & Compliance Engineer
Tel. (914) 681-6595
Email: daniella.piper@nypa.gov

Utility Services, Inc.

Primary
Brian Robinson
Compliance Analyst
Tel. (802) 552-4022
Email: brian.robinson@utilitysvcs.com

Alternate
Brian Evans-Mongeon
President/CEO
Tel. (802) 552-4022
Email: brian.evans-mongeon@utilitysvcs.com

Sector (6) – State and Provincial Regulatory and/or Governmental Authorities

New York State Department of Public Service

Primary
Vijay Puran
Utility Engineer 3
Tel. (518) 486-5948
Email: vijay.puran@dps.ny.gov

Alternate
Diane J. Barney
Chief, Bulk Electric Systems
Tel. (518) 486-2943
Email: diane.barney@dps.ny.gov

Sector 7 – Sub-Regional Reliability Councils, Customers and Other Regional Entities and Interested Entities

New York State Reliability Council, LLC

Primary
Alan Adamson
Independent Consultant
2104 Braxton Street
Clermont, FL 34711
Tel. (352) 989-4653
Email: aadamson@nycap.rr.com

Alternate

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

May 15, 2013

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

RE: Errata to Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standards COM-001-2 and COM-002-4
Docket No. RM14-13-000

Dear Ms. Bose:

On May 14, 2014, the North American Electric Reliability Corporation ("NERC") filed a Petition for approval of proposed Reliability Standards COM-001-2 and COM-002-4 with the Federal Energy Regulatory Commission. The Petition incorrectly notes that Requirement R1 of Reliability Standard EOP-008-1 is proposed for retirement. The Implementation Plans referenced in the Petition list the correct proposed retirements for approval. The following changes in strikethrough font illustrate the necessary corrections to the language in the Petition. NERC is not requesting retirement of EOP-008-1, Requirement R1.

Page 22

> Of particular note in the Implementation Plan, the standard drafting team concluded that Requirement R5 in COM-001-1.1 is redundant with EOP-008-1, Requirement R1 and, therefore, has not been carried forward in proposed COM-001-2. ~~As a result, NERC proposes EOP-008-1, Requirement R1 for retirement.~~

Pages 1-2

> NERC also requests approval of: (i) new defined terms "Operation Instruction", "Interpersonal Communication", and "Alternative Interpersonal Communication" for inclusion in the NERC Glossary of Terms; (ii) the Implementation Plans for the proposed Reliability Standards (Exhibits C and D); (iii) the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibits A, B, K, and L); and (iv) the retirement

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

of the currently-effective Reliability Standards COM-001-1.1~~, EOP-008-1 (Requirement R1),~~ and COM-002-2 as listed in the Implementation Plans.

Page 45

- approve the retirement of the currently effective Reliability Standards COM-001-1.1~~, EOP-008-1 (Requirement R1),~~ and COM-002-2, as proposed in the Implementation Plans.

Respectfully submitted,

/s/ William H. Edwards

William H. Edwards
Counsel for North American Electric Reliability Corporation

cc: Official service list in Docket No. RM14-13-000.

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 15th day of May, 2014.

/s/ William H. Edwards

William H. Edwards
Counsel for North American
Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability	**)**	
Corporation	**)**	**Docket No. FA11-21-000**

COMPLIANCE FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

The North American Electric Reliability Corporation ("NERC")[1] submits this compliance filing in accordance with the Commission's January 16, 2013 Order in Docket No. FA11-21-000.[2] In the January 16 Order, the Commission approved a Settlement Agreement between the Office of Enforcement ("Enforcement") and NERC related to Enforcement's findings and recommendations arising out of its 2012 performance audit of NERC. Specifically, Section II.7(b)(i) of the Settlement Agreement requires that:

> Within forty-five days of the end of each quarter, beginning with the quarter ending March 31, 2013, NERC will file with the Commission the unaudited report of the NERC budget-to-actual spending variances during the preceding quarter. This report will include information regarding sources and uses of operating and working capital reserves and will match or exceed the level of detail of the quarterly budget-to-actual variance report of NERC expenditures attached to the agenda of NERC Board of Trustees Finance and Audit Committee's October 2012 meeting.[3]

Attached hereto is the unaudited report of NERC's budget-to-actual variance information for the first quarter of 2014, in accordance with the January 16 Order. This variance information was

---

[1] NERC was certified by FERC as the electric reliability organization ("ERO") authorized by Section 215 of the Federal Power Act. FERC certified NERC as the ERO in its order issued July 20, 2006 in Docket No. RR06-1-000. *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (2006) ("ERO Certification Order").

[2] *See North American Electric Reliability Corporation, Order Approving Settlement Agreement*, 142 FERC ¶ 61,042 (2013) ("January 16 Order").

[3] *Id.*

posted on NERC's website and reviewed in open session at the May 6, 2014 meeting of the NERC Finance and Audit Committee. The unaudited report was accepted by the NERC Board of Trustees at its meeting on May 7, 2014.

I. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to:[4]

Michael Walker*
Senior Vice President and Chief Financial and Administrative Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-9740
(404) 467-0474 – facsimile

Willie L. Phillips*
Assistant General Counsel
Meredith M. Jolivert*
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
willie.phillips@nerc.net
meredith.jolivert@nerc.net

*Persons to be included on the Commission's official service list

[4] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203 (2012), to allow the inclusion of more than two persons on the service list in this proceeding.

II. CONCLUSION

NERC respectfully requests that the Commission accept this filing as compliant with Section II.7(b)(i) of the Settlement Agreement and the Commission's January 16 Order in Docket No. FA11-21-000.

Respectfully submitted,

/s/ Meredith M. Jolivert

Michael Walker
Senior Vice President and Chief Financial and Administrative Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-9740
(404) 467-0474 – facsimile

Willie L. Phillips
Assistant General Counsel
Meredith M. Jolivert
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
willie.phillips@nerc.net
meredith.jolivert@nerc.net

Counsel for North American Electric Reliability Corporation

Dated: May 15, 2014

ATTACHMENT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Summary of Results as of March 31, 2014

Through March 31, 2014, NERC was $1.5M, 10.2%, under its expense and fixed asset budget. As reflected in the following table and as further explained below, NERC is projecting to be approximately $939.1k, 1.7%, under budget at year end, due primarily to projected: (i) lower than budgeted personnel expense related to timing of hiring open positions; (ii) lower than budgeted travel expense after taking into account 2013 actual results, which reflected the implementation of various travel and expense control initiatives, and projected staffing levels; and, (iii) reduced office costs, primarily related to lower than budgeted expense for maintenance and service agreements. It's important to keep in mind that this projection is preliminary and subject to change. This year end projection will be utilized in preparation of the initial draft of NERC's 2015 business plan and budget, which will be posted on May 16th. It will be further refined and updated as part of the second quarter variance report and the final draft of the 2015 business plan and budget which is scheduled to be posted on July 15th.

YTD Actual versus YTD Budget and 2014 Projection versus 2014 Total Budget by Category

	2014 Actual	2014 Budget	2014 Variance Over(Under)	%	2014 Projection	2014 Annual Budget	2014 Projected Variance from Budget Over(Under)	%
TOTAL FUNDING	**13,612,918**	**13,653,595**	**(40,677)**	**-0.3%**	53,735,382	53,735,382	-	0.0%
BUDGET - EXPENSES and FIXED ASSETS								
PERSONNEL EXPENSES	8,535,155	8,850,363	(315,210)	-3.6%	33,642,577	34,059,654	(417,077)	-1.2%
MEETINGS, TRAVEL and CONFERENCE CALLS	857,031	950,632	(93,601)	-9.8%	3,551,995	3,789,526	(237,531)	-6.3%
CONSULTANTS and CONTRACTS	1,399,286	1,926,665	(527,380)	-27.4%	6,851,046	6,828,973	22,073	0.3%
RENT	660,658	654,325	6,333	1.0%	2,617,300	2,617,300	-	0.0%
OFFICE COSTS, PROFESSIONAL SERVICES and MISCELLANEOUS	1,367,413	1,460,974	(93,561)	-6.4%	5,590,908	5,832,854	(241,946)	-4.1%
Other Non-Operating Expenses	2,863	36,000	(33,137)	-92.0%	79,367	144,000	(64,633)	-44.9%
FIXED ASSET PURCHASES (excludes the credit for depreciation)	345,216	779,448	(434,232)	-55.7%	3,117,789	3,117,789	-	0.0%
TOTAL BUDGET	**13,167,621**	**14,658,406**	**(1,490,788)**	**-10.2%**	**55,450,983**	**56,390,096**	**(939,113)**	**-1.7%**
FTEs	**177.09**	**188.78**	**(11.69)**	**-6.2%**	**186.76**	**189.53**	**(2.77)**	**-1.5%**

Following is a brief summary of variances by major categories:

- Personnel expenses were under budget $315.2k, 3.6%, and are projected to be $417.1k, 1.2% under budget at year end due primarily to timing of hiring open positions. There were 11.7, 6.2%, fewer FTEs on staff than budgeted through March 31, 2014. The 2014 budget for personnel expenses and total FTEs reflects a 4% adjustment to account for attrition and timing of hiring open positions.
    - Salaries expense, which consists of salaries, incentive compensation, employment agency fees and temporary office services, was $214.6k, 3.3%, under budget through March 31st,

and is projected to be under budget $200.5k, 0.8%, at year end due primarily to having fewer FTEs on staff than budgeted.

- Payroll taxes were over budget $91.8k, 14%, through March 31st, and are projected to be over budget $137.0k, 8.7%, at year end due to a higher maximum salary subject to taxes in 2014 than was budgeted. Higher than budgeted expense through March 31st was also due to timing related to payroll taxes paid in February in connection with the payout of incentive compensation.
- Employee Benefits were $106.6k, 12.6%, under budget due to having fewer FTEs on staff than budgeted and due to lower employee relocation costs than budgeted. Benefits are projected to be under budget $185.0k, 5.5%, at year end due to having fewer FTEs on staff and lower than budgeted renewal costs.
- Retirement costs were $85.8k, 10.8%, under budget due to having fewer FTEs on staff. Retirement costs are projected to be $168.6k, 5.8%, under budget at year end due to timing of hiring open positions which delays eligibility in the savings and investment plan.

- Meeting, travel and conferencing expenses were collectively under budget $93.6k, 9.8%, through March 31st, and are projected to be $237.5k, 6.3%, under budget at year end. Travel expenses were under budget $51.8k through March, 2014, and are projected to be $198.2k under budget at year end after taking into consideration 2013 actual costs. Total travel expense in 2013 was $2.0M, approximately $400k less than the amount budgeted for 2014.
- Consultant and Contract expenses were $527.4k, 27.4%, under budget primarily due to timing of the budget versus actual payments for numerous projects throughout the organization. Total year end expenses are projected to be close to budget. The following table summarizes existing and projected over budget variances by department.
  - Regional Oversight for Compliance – The over budget projection is for additional consulting support in connection with regional RAI pilot program oversight.
  - RAPA - The over budget projection is related to: (i) contract support for data modeling and analysis needed due to staff vacancies, and which is offset by lower than budgeted personnel expenses and, (ii) change orders related to generation databases that were approved in 2013, but were not completed and fully invoiced until 2014.
  - Human Resources – The over budget projection is related to higher than budgeted consulting costs for executive and staff training and development.

SUMMARY OF CONSULTANT AND CONTRACT EXPENSES BY DEPARTMENT

	As of March 31, 2014					
CONSULTANTS and CONTRACTS	Actual	Budget	Over(Under)	2014 Projection	2014 Annual Budget	Variance from Budget Over(Under)
STANDARDS	-	-	-	-	-	-
COMPLIANCE ANALYSIS and CERTIFICATION	-	-	-	-	-	-
REGIONAL OVERSIGHT for COMPLIANCE	76,419	57,740	18,679	480,240	400,000	80,240
COMPLIANCE ENFORCEMENT	-	-	-	-	-	-
RELIABILITY ASSESSMENTS and PERFORMANCE ANALYSIS	89,770	229,521	(139,751)	692,652	638,085	54,567
RELIABILITY RISK MANAGEMENT	557,914	533,203	24,711	1,277,583	1,289,108	(11,525)
CRITICAL INFRASTRUCTURE DEPARTMENT	27,514	47,503	(19,989)	190,000	190,000	-
ES-ISAC	169,380	265,800	(96,420)	753,750	786,450	(32,700)
TRAINING, EDUCATION and OPERATOR CERTIFICATION	40,600	186,333	(145,733)	787,330	848,830	(61,500)
GENERAL and ADMINISTRATIVE and EXECUTIVE	-	-	-	-	-	-
POLICY and EXTERNAL AFFAIRS	-	18,750	(18,750)	75,000	75,000	-
LEGAL and REGULATORY	-	-	-	-	-	-
INFORMATION TECHNOLOGY	310,268	488,066	(177,798)	1,932,491	1,944,000	(11,509)
HUMAN RESOURCES	74,971	44,750	30,221	262,000	257,500	4,500
FINANCE and ACCOUNTING	52,449	55,000	(2,551)	400,000	400,000	-
TOTAL CONTRACTS and CONSULTANTS	**1,399,286**	**1,926,665**	**(527,380)**	**6,851,046**	**6,828,973**	**22,073**

- Office Costs, Professional Services and Miscellaneous expenses were $93.6k, 6.4%, under budget due to: (i) lower than budgeted costs for maintenance and service agreements; and (ii) lower than budgeted costs for attorney fees. These lower than budgeted costs were offset by slightly higher than budgeted costs related to closing the capital financing loan. Office costs are projected to be $238.4k, 6.8%, under budget due to lower than budgeted costs for maintenance and service agreements.
- Other Non-Operating Expenses were $33.1k, 92.0%, under budget through March 31st, and are projected to be $64.6k, 44.9%, under budget at year end due to a lower than budgeted interest expense and a delay in closing the capital financing program loan. The actual interest rate on the loan, which closed in January, 2014 instead of fourth quarter, 2013, is 2.9%. The 2014 budget was developed using an interest rate of 3.5%.
- Fixed Asset Purchases, which excludes the credit for depreciation, were $434.2k, 55.7%, under budget due to timing of expenses.

The following table summarizes contract and consulting cost incurred through March 31, 2014 related to the development of various enterprise software applications, including use of reserves.

Total project spending as of 3/31/2014

	2013			2014			Total		
Project	Actual	Budget	Use of Reserves	Actual	Budget	Use of Reserves	Actual	Budget	Use of Reserves
BES	822,327	644,736	177,591	153,595	200,000	-	975,922	844,736	177,591
SBS	250,131	245,000	5,131	216,735	215,000	-	466,866	460,000	5,131
EIDS	638,755	432,500	206,255	23,461	325,000	-	662,216	757,500	206,255
TOTAL	1,711,213	1,322,236	388,977	393,791	740,000	-	2,054,854	2,062,236	388,977

The development of the EIDS application is on hold. A technical audit of the vendor's code revealed significant architecture issues. The company is re-evaluating and will be consulting with the Regional Entities regarding the future approach to development of this application. The costs incurred through March 31,2014 in the development of this application expensed, rather than capitalized after a technical review of the code developed by the vendor revealed that (1) the software is not useable in its current form, (2) significant changes and costs would need to be incurred to attempt to make the application useable and even assuming that could be done, operation and maintenance of the software would be unduly expensive and cumbersome, (3) costs to complete or modify the software to attempt to make it useable will significantly exceed budget and (4) the likely path forward for the development this application will be to use a completely different architecture and starting platform. A more detailed discussion of the results of the company's technical audit of the vendor's code, as well as steps to strengthen the management and oversight of the development of this and other enterprise applications is included in the background materials for the May 6, 2015 Standards Oversight and Technology Committee meeting. Management is undertaking a review of capital spending needs and priorities for the balance of the year. The plan is to work within the confines of the overall 2014 fixed asset budget.

OPERATING RESERVE ANALYSIS

The December 31, 2013 working capital and operating reserve balance was $6.3M, inclusive of the adjustment for future liabilities. The 2013 ending balance was approximately $2.0M less than budgeted as a result of: (i) an error in the calculation of the projected year-end 2013 balance that occurred during development of the 2014 business plan and[1]; and (ii) the delay in closing the capital financing loan until January, 2014. The beginning year shortfall was partially offset by $808.2k, which is the non-current portion of the proceeds from the initial capital financing draw which took place on January 31st. Management has revised its internal control procedures to prevent reoccurrence of this error in the future.

As of March 31, 2014, the balance in available working capital and operating reserves was approximately equal to budget. Through March 31st, management approved the use of $139.7k of Unknown Contingency Reserves for contract and consulting support related to: (1) $80.2k for review of the regional entity RAI pilot programs; (2) $55.0k for data modeling and change orders related to generation databases; and (3) $4.5k for executive and staff training and development. The current balances in the Known Contingency Reserve, Unknown Contingency Reserve and the System Operator Reserves as of March 31, 2014 were $1.0M, $942.6k, and $1.5M, respectively.

The current year-end projected reserve balance is $2.1M, $635.9k less than budget and which is primarily due to the lower than budgeted actual starting reserve balance described above. The projected year-end balances in Known Contingency Reserves, Unknown Contingency Reserves and the System Operator Reserves is $1.0M, $74.8k, and 1.1M, respectively.

[1] In the preparation of the projected working capital and operating reserves as part of the 2014 budget development process, an incorrect assumption was made that the release of the penalty funding from restriction per applicable accounting policy increased the available operating reserve balance. However, when the restriction expires, the penalty funds are transferred from restricted cash to unrestricted cash to fund current year operations and only represent an increase in working capital or operating reserves when assessments are not reduced by an equivalent amount. This was not the case in the 2013 budget where penalty funds were used to reduce assessments as required by NERC's current penalty fund policy.

OPERATING RESERVE ANALYSIS - March 31, 2014

	2014 Actual	2014 Budget*	Variance - Actual to Budget	2014 Projection as of 3/31/2014	2014 Budget*	Variance - Projection to Budget	2014 Current Reserve Balances: Known Contingency Reserves	2014 Current Reserve Balances: Unknown Contingency Reserves	2014 Current Reserve Balances: System Operator Reserves
WORKING CAPITAL and OPERATING RESERVES									
Balance as of 12/31/13	6,264,672	8,217,862	(1,953,190)	6,264,672	8,217,862	(1,953,190)			
Less: Adjustment for future liabilities	(3,817,478)	(3,788,645)	(28,833)	(3,817,478)	(3,788,645)	(28,833)			
Beginning Available Operating Reserves	**2,447,194**	**4,429,217**	**(1,982,023)**	**2,447,194**	**4,429,217**	**(1,982,023)**	**1,000,000**	**(69,672)**	**1,516,866**
Proceeds from Financing Activities (non-current portion only)	808,194		808,194	1,752,187	943,993	808,194		808,194	
Change in Reserves from Current Year Operations	445,297	(1,004,811)	1,450,111	(1,715,602)	(2,654,715)	939,113	-	480,762	(35,465)
Other adjustments to reserves**	(276,673)		(276,673)	(351,209)	49,999	(401,208)		(276,673)	
Available Reserve Balance 3/31/14	**3,424,012**	**3,424,406**	**(391)**	**2,132,571**	**2,768,494**	**(635,924)**	**1,000,000**	**942,611**	**1,481,401**

*The 2014 budget includes a $1.2M reduction in Known and Unknown reserves and a $438.3k planned reduction in the System Operator Reserves, for a total budgeted reduction in reserves of $1,660,724.

**Represents transactions recorded only on the Statement of Financial Position (balance sheet) and do not impact the Statement of Activities (income statement), including debt services and true-up of current versus non-current deferred rent obligation

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Statement of Activities and Fixed Assets Budget
(Unaudited)
For the period ended 03/31/2014

	2014 Actual	2014 Budget	2014 Variance Over(Under)	%	2014 Projection	2014 Annual Budget	2014 Projected Variance from Budget Over(Under)	%
Funding								
Assessments	12,850,346	12,850,345	0		51,401,382	51,401,382	-	
Penalties	290,000	290,000	(0)		290,000	290,000	-	
Testing	382,918	405,000	(22,083)		1,620,000	1,620,000	-	
Services & Software	7,000	12,500	(5,500)		50,000	50,000	-	
Workshop Fees	82,000	90,750	(8,750)		354,000	354,000	-	
Interest	598	5,000	(4,402)		20,000	20,000	-	
Miscellaneous	58	-	58		-	-	-	
Total Funding	13,612,918	13,653,595	(40,677)	-0.3%	53,735,382	53,735,382	-	0.0%
Expenses								
Personnel Expenses								
Salaries	6,340,058	6,554,645	(214,587)		26,018,122	26,218,572	(200,450)	-0.8%
Payroll Taxes	746,619	654,855	91,764		1,707,968	1,570,954	137,014	8.7%
Employee Benefits	739,879	846,477	(106,598)		3,200,898	3,385,917	(185,019)	-5.5%
Savings & Retirement	708,599	794,388	(85,789)		2,715,589	2,884,211	(168,622)	-5.8%
Total Personnel Expenses	8,535,155	8,850,363	(315,210)	-3.6%	33,642,577	34,059,654	(417,077)	-1.2%
Meeting Expenses								
Meetings	233,439	266,288	(32,849)		1,050,980	1,052,150	(1,170)	-0.1%
Travel	553,065	604,881	(51,816)		2,221,330	2,419,525	(198,195)	-8.2%
Conference Calls	70,527	79,463	(8,936)		279,685	317,851	(38,166)	-12.0%
Total Meeting Expenses	857,031	950,632	(93,601)	-9.8%	3,551,995	3,789,526	(237,531)	-6.3%
Operating Expenses								
Consultants and Contracts	1,399,286	1,926,665	(527,380)	-27.4%	6,851,046	6,828,973	22,073	0.3%
Rent & Improvements	660,658	654,325	6,333	1.0%	2,617,300	2,617,300	-	0.0%
Office Costs	851,969	880,484	(28,515)	-3.2%	3,267,628	3,506,074	(238,446)	-6.8%
Professional Services	513,599	571,365	(57,766)	-10.1%	2,290,280	2,290,280	-	0.0%
Miscellaneous	1,846	9,125	(7,279)	-79.8%	33,000	36,500	(3,500)	-9.6%
Depreciation	496,637	583,252	(86,615)	-14.9%	2,137,192	2,333,006	(195,814)	-8.4%
Total Operating Expenses	3,923,994	4,625,216	(701,222)	-15.2%	17,196,446	17,612,133	(415,687)	-2.4%
Other Non-Operating Expenses	2,863	36,000	(33,137)	-92.0%	79,367	144,000	(64,633)	-44.9%
Total Expenses	13,319,042	14,462,211	(1,143,171)	-7.9%	54,470,386	55,605,313	(1,134,927)	-2.0%
Net Change in Assets	**293,876**	**(808,615)**	**1,102,493**	**-136.3%**	**(735,004)**	**(1,869,931)**	**1,134,927**	**-60.7%**
Fixed Assets								
Depreciation	(496,637)	(583,252)	86,615		(2,137,192)	(2,333,006)	195,814	
Computer & Software CapEx	293,061	726,198	(433,136)		2,904,790	2,904,790	-	
Furniture & Fixtures CapEx	-	-	-		-	-	-	
Equipment CapEx	52,154	53,250	(1,096)		213,000	213,000	-	
Leasehold Improvements	-	-	-		-	-	-	
Incr(Dec) in Fixed Assets	**(151,421)**	**196,196**	**(347,617)**	**-177.2%**	**980,597**	**784,783**	**195,814**	**25.0%**
Total Budget (Expenses plus Incr(Dec) in Fixed Assets)	**13,167,621**	**14,658,406**	**(1,490,788)**	**-10.2%**	**55,450,983**	**56,390,094**	**(939,113)**	**-1.7%**
FTE's	177.09	188.78	(11.69)	-6.2%	186.76	189.53	(2.77)	-1.5%

NORTH AMERICAN ELECTRIC RELIABILITY COPORATION
STATEMENT OF FINANCIAL POSITION
(Unaudited)

			Available Working Capital	
	3/31/2014	12/31/2013	3/31/2014	12/31/2013
ASSETS				
Cash	31,288,523	26,182,060	31,288,523	26,182,060
Trade Accounts receivable, net of allowance for uncollectible accounts of 0 and 62,573 in 2013 and 2012	18,424,462	3,353,895	18,424,462	3,353,895
Prepaid expenses and other current assets	711,362	869,876	711,362	869,876
Security deposit	99,136	99,136		
Cash value of insurance policies	-	-		
Employee Fiduciary - 457b	320,660	320,660		
Property and equipment	5,493,695	5,645,116		
Total Assets	56,337,838	36,470,743		
LIABILITIES AND NET ASSETS				
Liabilities				
Current Portion				
Accounts payable and accrued expenses (includes vacation accrual)	3,547,498	2,917,303	(3,547,498)	(2,917,303)
Accured incentive compensation	990,140	4,025,979	(990,140)	(4,025,979)
Deferred rent-current	193,572	182,421	(193,572)	(182,421)
Deferred compensation - current	14,257	20,386	(14,257)	(20,386)
Capital lease obligations - current	47,108	47,108	(47,108)	(47,108)
Accrued retirement liabilities	835,776	1,788,624	(835,776)	(1,788,624)
Debt service - current portion	421,667		(421,667)	-
Deferred income	17,908,399	5,287,044	(17,908,399)	(5,287,044)
Deferred revenue - penalties	0	-	(0)	-
Deferred revenue - other	5,000		(5,000)	-
Regional assessments	19,115,052	9,427,293	(19,115,052)	(9,427,293)
Total Current Portion	43,078,469	23,696,159		
Long-Term Portion				
Deferred compensation[1]	320,660	597,514		
Long-Term Debt	808,194			
Deferred Rent-non-current	3,767,047	3,817,478	(3,767,047)	(3,817,478)
Capital lease obligations - non-current	-	-		
Total Long-Term Portion	4,895,901	4,414,992		
Total Liabilities	47,974,370	28,111,151		
Net Assets - unrestricted	8,208,469	7,914,592		
Net Assets - restricted	155,000	445,000	(155,000)	(445,000)
Total Liabilities and Net Assets	56,337,838	36,470,743	3,423,832	2,447,194
[1]Includes 457b liability, life insurance for former executive, and retiree medical				
Working Capital	**7,190,878**	**6,264,672**		
Less: Restriction for future liabilities	(3,767,047)	(3,817,478)		
Available Working Capital	3,423,832	2,447,194		

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 15th day of May, 2014.

/s/ Meredith M. Jolivert

Meredith M. Jolivert
Counsel for North American
Electric Reliability Corporation

June 6, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose, Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

Re: Petition of the North American Electric Reliability Corporation for Approval of Amendments to Exhibit B of the Delegation Agreement with SERC Reliability Corporation – Amendments to the SERC Reliability Corporation Bylaws
Docket No. RR14-___-000

Dear Ms. Bose:

The North American Electric Reliability Corporation ("NERC") respectfully submits the "Petition of the North American Electric Reliability Corporation for Approval of Amendments to Exhibit B of the Delegation Agreement with SERC Reliability Corporation – Amendments to the SERC Reliability Corporation Bylaws." The primary purpose of these amendments is to: 1) support SERC Reliability Corporation's ("SERC's") application for tax-exempt status under § 501(c)(6) of the Internal Revenue Code; and 2) clarify and modify certain SERC-specific corporate governance matters. After examination, NERC concurs with SERC's determination that the amendments to the SERC Bylaws do not affect any of the qualifications for the delegation of authority from NERC to SERC, and will not adversely impact SERC's ability to function as a Regional Entity. The amended SERC Bylaws continue to satisfy the five governance criteria specified in Exhibit B of the SERC Regional Delegation Agreement ("SERC RDA").

This filing consists of: (1) this transmittal letter; (2) the narrative text of the Petition which follows this transmittal letter; and (3) Attachments 1, 2, and 3 to the Petition which respectively contain: i) SERC's March 3, 2014 letter to NERC requesting approval of the amendments and explaining their purpose; ii) a clean version of the amended Exhibit B of the SERC RDA; and iii) a redlined version of the amended Exhibit B of the SERC RDA. All of these documents are transmitted in a single PDF file.

Please contact the undersigned if you have any questions concerning this filing.

Respectfully submitted,

/s/ Thomas DeVita
Thomas DeVita
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3021
(202) 420-8795 – facsimile
thomas.devita@nerc.net

UNITED STATES OF AMERICA
Before the
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)** **)**	**Docket No. RR14-__-000**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF AMENDMENTS TO EXHIBIT B OF THE DELEGATION AGREEMENT WITH SERC RELIABILITY CORPORATION – AMENDMENTS TO THE SERC RELIABILITY CORPORATION BYLAWS

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

Charles A. Berardesco
Senior Vice President and General Counsel
Willie L. Phillips
Assistant General Counsel
Thomas DeVita
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
willie.phillips@nerc.net
thomas.devita@nerc.net

Counsel for North American Electric Reliability Corporation

June 6, 2014

TABLE OF CONTENTS

I. INTRODUCTION 1

II. NOTICES AND COMMUNICATIONS 2

III. PROPOSED AMENDMENTS TO THE DELEGATION AGREEMENT BETWEEN NERC AND SERC RELIABILITY CORPORATION 3

IV. SERC RELIABILITY CORPORATION AND NERC APPROVALS FOR THE PROPOSED AMENDMENTS 5

V. CONCLUSION 6

ATTACHMENTS

Attachment 1: SERC Reliability Corporation's March 3, 2014 Letter Identifying and Explaining the Proposed Amendments to the SERC Reliability Corporation Bylaws and Requesting North American Electric Reliability Corporation Approval

Attachment 2: Amended Exhibit B of the Delegation Agreement Between North American Electric Reliability Corporation and SERC Reliability Corporation – Clean version

Attachment 3: Amended Exhibit B of the Delegation Agreement Between North American Electric Reliability Corporation and SERC Reliability Corporation – Redlined version

I. INTRODUCTION

Pursuant to § 215(e)(4) of the Federal Power Act[1] ("FPA") and 18 C.F.R. §§ 39.8 and 39.10 (2012), the North American Electric Reliability Corporation ("NERC") respectfully requests the Federal Energy Regulatory Commission's (the "Commission's") approval of amendments to the Amended and Restated Regional Delegation Agreement between NERC and the SERC Reliability Corporation ("SERC"), one of the eight NERC Regional Entities (the "SERC RDA"). The proposed amendments to the SERC RDA consist exclusively of amendments to Exhibit B, the SERC Bylaws. The SERC Bylaws are "Regional Entity Rules" as defined in 18 C.F.R. § 39.1,[2] and amendments to the SERC Bylaws thereby require Commission approval in accordance with 18 C.F.R. § 39.10(a).[3]

Attachment 1 to this Petition is SERC's March 3, 2014 letter to NERC requesting approval of the amendments to the SERC Bylaws, and explaining the purposes of the amendments. **Attachments 2** and **3** are clean and redlined versions, respectively, of the proposed amended Exhibit B of the SERC RDA.

[1] 16 U.S.C. §824o (2005).
[2] The term "Regional Entity Rule" is defined as "…the bylaws, a rule of procedure or other organizational rule or protocol of a Regional Entity."
[3] "A Regional Entity shall submit a Regional Entity Rule or Rule change to the Electric Reliability Organization and, if approved by the Electric Reliability Organization, the Electric Reliability Organization shall file the proposed Regional Entity Rule or Rule change with the Commission for approval."

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to:

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

Charles A. Berardesco*
Senior Vice President and General Counsel
Willie L. Phillips*
Assistant General Counsel
Thomas DeVita*
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
willie.phillips@nerc.net
thomas.devita@nerc.net

*Persons to be included on the Commission's official service list

III. PROPOSED AMENDMENTS TO THE DELEGATION AGREEMENT BETWEEN NERC AND SERC RELIABILITY CORPORATION

On March 3, 2014, NERC received correspondence from SERC requesting approval of the amendments to the SERC Bylaws, and explaining the purposes of the amendments. This letter is featured as **Attachment 1** to this petition. As described more fully in **Attachment 1**, the amendments to the SERC Bylaws may be summarized as follows:

1. *Cover Page and Table of Contents*

    a. *Cover Page*
        i. Changed the date on the cover page to reflect the most recent date of approval by the SERC Board of Directors. This updated date appears on every subsequent page of the Bylaws.

    b. *Table of Contents*
        i. Changed various numbers in the table of contents to reflect changes in pagination caused by the amendments to the SERC Bylaws.

2. *Article II - Membership*

    a. *Section 2.2 - Eligibility*
        i. Added language clarifying that, for purposes of the SERC Bylaws, the terms "Bulk Power System," "Reliability Standards," and "Regional Entity" shall be as defined in 16 U.S.C. § 824o.
        ii. Added a reference to Section 3.2 (SERC's Geographic Region) for additional clarity regarding the identification of entities eligible for membership in the Corporation.

    b. *Section 2.6 - Powers*
        i. Added a section to clarify that, notwithstanding any other provisions of the Bylaws, Member Companies shall be non-voting members and shall have no power or authority or right to vote with respect to the actions of the Corporation (including the dissolution or merger of the Corporation). This language specifically includes an exception for the appointment of SERC Directors.[4]

[4] Exhibit B of the SERC RDA is composed of five distinct governance criteria, in addition to the SERC Bylaws. The second governance criterion requires that "[t]he Regional Entity has established rules that assure its independence of the users and owners and operators of the bulk power system, while assuring fair stakeholder representation in the selection of its directors." *See also* 16 U.S.C. §§ 824(o) (c)(2)(A) and (e)(4)(B), 18 C.F.R. § 39.8(c)(2), and Order No. 672 at P 728.

3. *Article IV - Board of Directors*

    a. *Section 4.2 – Composition and Eligibility*
        i. **Added** language requiring that corporate affiliates consolidate and coordinate their representation on the SERC Board and any SERC Board-level committees.

    b. *Section 4.13 - Duties*
        i. **Capitalized** the "C" of "Corporation's" in subsection (b).

4. *Article XI - Dissolution*

    a. *Section 11.2 - Distribution of Assets*
        i. **Changed** the language of this provision to replace the reference to "Section 501(c)(3)" of the Internal Revenue Code with "Section 501(c)(6)."
        ii. **Added** "1986" to specify the version of the Internal Revenue Code being referred to.
        iii. **Deleted** language authorizing the assets of SERC, upon corporate dissolution, to be transferred to federal, state or local governments.

5. *Article XIII - Indemnification*

    a. *Section 13.1 - Indemnification of Directors, Committee Members, Officers, Employees and Agents*
        i. **Added** the categories of "Alternate Directors" and "Customer Advisors" to the indemnification provision of Article XIII.

6. *Article XIV - Amendment of the Bylaws*
        i. **Added** "Articles of Incorporation" to the procedure governing amendments to the SERC Bylaws, thereby extending this procedure to amendment of the SERC Articles of Incorporation as well.

IV. SERC RELIABILITY CORPORATION AND NERC APPROVALS FOR THE PROPOSED AMENDMENTS

The proposed amendments to the SERC Bylaws were approved by the SERC Board of Directors in October 2012 and October 2013, and were approved by the NERC Board of Trustees on May 7, 2014. In making the determination to approve the proposed amendments to the SERC Bylaws, NERC determined that the amended SERC Bylaws continue to satisfy the five Governance criteria stated in Exhibit B of the SERC RDA.

V. CONCLUSION

Accordingly, NERC respectfully requests that the Commission approve the proposed amendments to the SERC RDA shown in **Attachment 3** to this Petition as amendments to Regional Entity Rules.

Respectfully submitted,

/s/ Thomas DeVita

Charles A. Berardesco
Senior Vice President and General Counsel
Willie L. Phillips
Assistant General Counsel
Thomas DeVita
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
willie.phillips@nerc.net
thomas.devita@nerc.net

Counsel for North American Electric Reliability Corporation

Dated: June 6, 2014

ATTACHMENT 1

SERC RELIABILITY CORPORATION'S

MARCH 3, 2014 LETTER IDENTIFYING AND EXPLAINING

THE PROPOSED AMENDMENTS TO

THE SERC RELIABILITY CORPORATION BYLAWS

AND REQUESTING

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

APPROVAL

Marisa A. Sifontes, General Counsel
SERC Reliability Corporation
2815 Coliseum Centre Drive | Suite 500
Charlotte, NC 28217
704.357.7372 | Fax 704.357.7914 | www.serc1.org

March 3, 2014 **Via E-Mail**

Charles A. Berardesco
Senior Vice President, General Counsel and Corporate Secretary
North American Electric Reliability Corporation
1325 G Street, NW, Suite 600
Washington, DC 20005-3801

Re: Amendments to the SERC Reliability Corporation Bylaws

Dear Charlie:

In accordance with the Amended and Restated Delegation Agreement dated June 12, 2012 ("Delegation Agreement") between the North American Electric Reliability Corporation ("NERC") and SERC Reliability Corporation ("SERC"), I am providing you with amended SERC Bylaws for its North Carolina corporation, which were approved by the SERC Board of Directors ("Board") on October 24, 2012 and October 23, 2013. The nature of and reasons for the amendments are set forth below. The amendments do not affect any of the qualifications for the delegation of authority from NERC to SERC, and will not have any adverse impact on the ability of SERC to function as a Regional Entity under the Delegation Agreement.

Accordingly, SERC requests that: (1) NERC approve the amended SERC Bylaws as consistent with the Delegation Agreement; (2) the amended SERC Bylaws be forwarded to the Federal Energy Regulatory Commission ("FERC") for approval; and (3) upon FERC approval, the amended SERC Bylaws become effective as part of the Delegation Agreement.

I. Background

SERC is in the process of transitioning from an Alabama non-profit corporation to a North Carolina non-profit corporation, in consideration of its current base of operations and lack of substantial nexus to the state of Alabama. As part of this, SERC has formed a North Carolina corporation. In October 2012, the SERC Board approved the Articles of Incorporation and initial Bylaws for the North Carolina non-profit corporation. At this time, the Board directed staff to consider whether it would be appropriate to seek tax exempt status under Section 501(c)(3) of the Internal Revenue Code, rather than under Section 501(c)(6), the current status of the Alabama corporation. The initially approved Bylaws of the North Carolina corporation contained language necessary to support the 501(c)(3) application. The Bylaws approved by the Board in October 2012 also contained other minor changes as discussed below.

After consideration, it was decided that it would be preferable to maintain the same tax status for the North Carolina corporation, rather than to seek tax exempt status under Section 501(c)(3), and in October 2013, the SERC Board unanimously approved amendments to the SERC Bylaws to codify this decision. Further details on the amendments to the Bylaws are discussed below.

Clean and redlined versions of the amended Bylaws reflecting the comprehensive changes made are provided as Attachments 1 and 2 to this letter. Upon approval, the amended Bylaws would become Exhibit B to the Delegation Agreement.

SERC Reliability Corporation

II. Change to support 501(c)(6)application

In section 11.2, the "Distribution of Assets" provision was amended to remove language necessary for 501(c)(3) status. Section 501(c)(6) of the Internal Revenue Code requires different language in the Bylaws than is required under Section 501(c)(3). The changes necessary to support this recommendation are needed prior to filing an application for tax exempt status for the North Carolina corporation.

III. Other Changes

(1) Table of Contents (updating to reflect changes in pagination caused by the amendments to the Bylaws)
(2) Section 2.2 (adding language to state that the terms "Bulk Power System", "Reliability Standards" and "Regional Entity" shall be as defined in 16 U.S.C. § 824o)
(3) Section 2.6 (adding this Section to clarify that Member Companies shall be non-voting members and shall have no power or authority or right to vote with respect to the actions of the Corporation)
(4) Section 4.2 (adding language to require corporate affiliates to consolidate and coordinate their representation on the Board and any Board level committees)
(5) Section 13.1 (adding "Alternate Director" and "Customer Advisor" to reflect that this Section applies to these representatives)
(6) Article 14 (expanding this Article to apply to the Articles of Incorporation)

IV. Conclusion

As detailed above, the amendments to the SERC Bylaws do not impact SERC's qualifications to serve as a Regional Entity with delegated authority from NERC and do not affect the ability of SERC to function as a Regional Entity under the Delegation Agreement. Accordingly, SERC requests that NERC approve the amended Bylaws as consistent with the Delegation Agreement, and forward the amended Bylaws to FERC for approval and adoption as a replacement for Exhibit B to the Delegation Agreement.

Please contact me if you have any questions.

Sincerely,

Marisa Sifontes

Digitally signed by Marisa Sifontes
DN: cn=Marisa Sifontes, o=SERC, ou, email=msifontes@serc1.org, c=US
Date: 2014.03.03 15:11:51 -05'00'

Marisa A. Sifontes

Enclosures

cc: R. Scott Henry

ATTACHMENT 2

AMENDED EXHIBIT B OF THE DELEGATION AGREEMENT

BETWEEN

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

AND

SERC RELIABILITY CORPORATION

CLEAN VERSION

AMENDED AND RESTATED

BYLAWS

OF

SERC RELIABILITY CORPORATION

A North Carolina Nonprofit Corporation

Approved by the Board of Directors on _____, 2013

TABLE OF CONTENTS

ARTICLE I - OFFICES 1
1.1 **Principal Office** 1
1.2 **Other Offices** 1

ARTICLE II - MEMBERSHIP 1
2.1 **General** 1
2.2 **Eligibility** 1
2.3 **Termination** 2
2.4 **Sectors** 2
2.5 **Transfer of Membership** 3
2.6 **Powers** 3

ARTICLE III - PURPOSES 3
3.1 **General Purposes** 3
3.2 **Geographic Area** 4
3.3 **Other Statutory Functions** 4

ARTICLE IV - BOARD OF DIRECTORS 4
4.1 **General Powers** 4
4.2 **Composition and Eligibility** 5
4.3 **Regular Meetings of the Board** 5
4.4 **Special Meetings of the Board** 6
4.5 **Notice of Special Meetings** 6
4.6 **Election of Board Officers and Executive Committee** 6
4.7 **Agenda** 6
4.8 **Voting Definitions** 6
4.9 **Determination of Adjusted Weighted Vote** 7
4.10 **Voting; Manner of Acting; Voting Rights; Quorum; Proxies** 8
4.11 **Compensation** 8
4.12 **Informal Action by Directors** 8
4.13 **Duties** 9

ARTICLE V - CORPORATE OFFICERS 9
5.1 **Corporate Officers** 9
5.2 **President & Chief Executive Officer** 9
5.3 **Vice President** 10
5.4 **Secretary** 10
5.5 **Treasurer** 10

ARTICLE VI - EXECUTIVE COMMITTEE 11
6.1 **Executive Committee Representatives** 11
6.2 **Ex Officio Representatives** 11
6.3 **Authority of Executive Committee** 11
6.4 **Action** 11

ARTICLE VII - OTHER COMMITTEES 12
7.1 **Designation by Board** 12
7.2 **Rules for Governance** 12
7.3 **Ad-Hoc Support Committees** 12

ARTICLE VIII - MISCELLANEOUS 12
8.1 **Conflicts of Interest** 12
8.2 **Contracts** 12
8.3 **Checks, Drafts, etc.** 12
8.4 **Deposits** 13
8.5 **Books and Records** 13
8.6 **Seal** 13
8.7 **Fiscal Year** 13

ARTICLE IX - EXPENSES 13
9.1 **Allocation of Specific Expenses** 13
9.2 **Statutory Functions** 13
9.3 **Non-Statutory Functions** 13

ARTICLE X - DISPUTE RESOLUTION PROCESS 14
10.1 **Dispute Resolution** 14

ARTICLE XI - DISSOLUTION 14
11.1 **Dissolution** 14
11.2 **Distribution of Assets** 14

ARTICLE XII - WAIVER OF NOTICE 14
12.1 **Waiver** 14

ARTICLE XIII - INDEMNIFICATION 15
13.1 **Indemnification of Directors, Committee Members, Officers, Employees and Agents** 15

ARTICLE XIV – AMENDMENT OF THE BYLAWS AND ARTICLES OF INCORPORATION 15
14.1 **Amendment of the Bylaws and Articles of Incorporation** 15

AMENDED AND RESTATED

BYLAWS

OF

SERC RELIABILITY CORPORATION
[Hereinafter referred to as the "Corporation"]

A North Carolina Nonprofit Corporation

ARTICLE I - OFFICES

1.1 **Principal Office**. The principal office of the Corporation shall be located in the City of Charlotte, Mecklenburg County, North Carolina. The Board of Directors may by resolution change the location of this office from time to time.

1.2 **Other Offices**. The Corporation may have other offices at such place or places as the Board of Directors may from time to time appoint or the business of the Corporation may require.

ARTICLE II - MEMBERSHIP

2.1 **General**. The Corporation shall be a membership corporation. Entities that meet the eligibility requirements and apply for membership in the Corporation shall hereinafter be referred to individually as a "Member Company" and collectively as "Member Companies".

2.2 **Eligibility**. Membership in the Corporation is open to any entity in the SERC Region (defined in Section 3.2 below) that is a user, owner or operator of the Bulk Power System and is subject to the jurisdiction of the Federal Energy Regulatory Commission for the purpose of complying with Reliability Standards established under Section 215 of the Federal Power Act and all amendments thereto. Membership in the Corporation is voluntary; however, membership is predicated on mandatory acceptance of the responsibility to promote, support, and comply with Reliability Standards of the Corporation and the North American Electric Reliability Corporation ("NERC"), and to assist the Corporation in its compliance with the terms and provisions of a Delegation Agreement (a "Delegation Agreement") with NERC, by which NERC delegates authority to propose and enforce Reliability Standards, pursuant to 16 U.S.C. § 824o or the corresponding provisions of any subsequent U.S. Code revisions. For purposes of

these Bylaws, the terms “Bulk Power System”, “Reliability Standards” and “Regional Entity” shall be as defined in 16 U.S.C. § 824o or the corresponding provisions of any subsequent U.S. Code revisions.

2.3 **Termination**. A Member Company may terminate its membership in the Corporation by giving the Board of Directors at least thirty (30) days written notice of its intent to terminate such membership (such Member Companies shall hereinafter be referred to as "Terminated Member Companies"). Terminated Member Companies shall nevertheless continue to be liable for any and all obligations incurred prior to the end of the calendar year in which such notice is given, including, but not limited to, the obligation to pay a pro rata share of any Corporation expense. In addition to termination of membership by the Member Company, the Board of Directors, following notice to the Member Company, may terminate the membership of a Member Company if in the judgment of the Board of Directors that Member Company has violated its obligations and responsibilities to the Corporation. The termination of the membership of a Member Company by the Board of Directors shall require a Supermajority vote, as defined in these Bylaws.

2.4 **Sectors.** Each Member Company shall be classified by the Executive Committee in one of the following seven (7) Sectors (each a “Sector”, and collectively, the “Sectors”):

(a) Investor-Owned Utility Sector – This Sector includes any investor-owned entity with substantial business interest in ownership and/or operation in any of the asset categories of generation, transmission or distribution.

(b) Federal/State Sector – This Sector includes any U.S. federal entity that owns and/or operates electric facilities and/or provides balancing authority services, in any of the asset categories of generation, transmission, or distribution; or any entity that is owned by or subject to the governmental authority of a state and that is engaged in the generation, delivery, and/or sale of electric power to end-use customers primarily within the political boundaries of the state.

(c) Cooperative Sector – This Sector includes any non-governmental entity that is incorporated under the laws of the state in which it operates, is owned by and provides electric service to end-use customers at cost, and is governed by a board of directors that is elected by the membership of the entity; and any non-governmental entity owned by and which provides generation and/or transmission service to such entities.

(d) Municipal Sector – This Sector includes any entity owned by or subject to the governmental authority of a municipality, that is

engaged in the generation, delivery, and/or sale of electric power to end-use customers primarily within the political boundaries of the municipality; and any entity, whose members are municipalities, formed under state law for the purpose of generating or purchasing electricity for sale at wholesale to their members.

(e) Marketer Sector– This Sector includes any entity that is engaged in the activity of buying and selling of wholesale electric power in the SERC Region on a physical or financial basis.

(f) Merchant Electricity Generator Sector – This Sector includes any entity that owns or operates an electricity generating facility or provides balancing authority services for such entities. This includes, but is not limited to, small power producers and all other non-utility producers such as exempt wholesale generators who sell electricity at wholesale.

(g) ISO-RTO Sector – This Sector includes any entity that operates a FERC approved ISO or RTO.

The Executive Committee's classification of a Member Company in a particular Sector may only be changed by the Executive Committee.

2.5 **Transfer of Membership.** A Member Company may not give or otherwise transfer its membership, except to a successor that becomes a Member Company in accordance with the terms and conditions of these Bylaws, and provided that the successor continues to meet its predecessor's obligations.

2.6 **Powers.** Notwithstanding any other provisions of these Bylaws, except for the appointment of Directors as provided in Section 4.2 below, Member Companies shall be non-voting members and shall have no power or authority or right to vote with respect to the actions of the Corporation, specifically including, but not limited to, the dissolution or merger of the Corporation.

ARTICLE III - PURPOSES

3.1 **General Purposes.** The purpose of the Corporation is to promote effective and efficient administration of Bulk Power System reliability in the SERC Region, as defined in Section 3.2. In pursuit of this goal, the Corporation shall:

(a) enter into a Delegation Agreement to serve as a Regional Entity pursuant to 16 U.S.C. § 824o or the corresponding provisions of any subsequent U.S. Code revisions;

(b) promote the development of reliability and adequacy arrangements among the systems in the SERC Region;

(c) participate in the establishment of Reliability Standards;

(d) participate in the measurement of performance relative to these Reliability Standards;

(e) promote conformance to and compliance with these Reliability Standards;

(f) develop and exchange information with respect to planning and operating matters relating to the reliability and adequacy of the Bulk Power System;

(g) review as necessary activities in the SERC Region on reliability and adequacy in order to meet Reliability Standards;

(h) provide a mechanism to resolve disputes on reliability issues in a manner that meets the needs of the parties and the SERC Region; and

(i) provide information with respect to matters considered by the Corporation, where appropriate, to the Federal Energy Regulatory Commission ("FERC") and to other federal and state agencies concerned with reliability and adequacy.

3.2 **Geographic Area.** The Corporation accomplishes its purposes in a geographic area (the "SERC Region") that is defined in Exhibit A of the Amended and Restated Delegation Agreement Between North American Electric Reliability Corporation and SERC Reliability Corporation.

3.3 **Other Statutory Functions.** The Corporation may also perform statutory functions outside of the SERC Region, on behalf of NERC or other Regional Entities. The Corporation may undertake such activities pursuant to a contract that is approved by the Executive Committee.

ARTICLE IV - BOARD OF DIRECTORS

4.1 **General Powers**. The affairs of the Corporation shall be managed by its Board of Directors except as otherwise provided in these Bylaws.

4.2 **Composition and Eligibility**. The Board of Directors shall be comprised of no fewer than three (3) Directors and no more than two (2) Customer Advisors.

Each Director shall be the principal officer or other authorized employee from a Member Company or a company that controls, is controlled by, or is under common control with such Member Company (an "affiliated entity"). Each Member Company, together with any affiliated entities, may appoint one (1) Director to the Board of Directors. For clarification purposes only, each Member Company and all of such Member Company's affiliated entities (including any affiliated entities which may be a separate Member Company) shall have the right to appoint only one (1) Director to serve on behalf of such Member Company and all of such Member Company's affiliated entities. Each Director shall serve until otherwise replaced by the applicable Member Company, together with any affiliated entities. Each Member Company, together with any affiliated entities, may designate one (1) alternate Director, who shall be a principal officer or other authorized employee from the Director's Member Company or an affiliated entity, to serve in the place of the Member Company's Director at any meeting of the Board of Directors (an "Alternate Director"). Directors may not otherwise use proxy votes. Any vacancy occurring among the Directors or Alternate Directors shall be filled by the applicable Member Company, together with any affiliated entities.

Each Customer Advisor shall be a person who is (i) employed by an entity that receives service at retail and does not otherwise sell, purchase, or transmit power over the Bulk Power System or own, operate or maintain, control or operate facilities or systems that are part of the Bulk Power System; (ii) a state public utility commission representative; or (iii) any other customer advocate. Should the Board of Directors not include two (2) Customer Advisors, the Board of Directors may elect additional Customer Advisors to fill such vacancies. The term of these Customer Advisors shall be for a two (2) year period.

The Chair of FERC and the chair or president of any State Utility Commission in a state in which electric service is provided by a Member Company of the Corporation shall be invited to designate an observer to attend meetings of the Board.

4.3 **Regular Meetings of the Board**. Unless otherwise determined by the Chair, a regular meeting of the Board of Directors shall be held without other notice than these Bylaws on the fourth Wednesday in the months of April and October in each year. Notwithstanding the foregoing, the Chair may elect to hold a regular semi-annual meeting of the Board of Directors on another date provided that the Board receives at least ten (10) days advance notice. If the day fixed for the meeting shall be a legal holiday in the State of North Carolina, the meeting shall be held on the next succeeding business day. The Board of Directors may designate any place as the place of meeting for any meeting. The Board of Directors may provide by resolution the time and place for the holding of additional regular meetings of the Board without other notice than the resolution. Directors or any committee designated by the Board of Directors may participate in such Board or committee meetings by means of a telephone conference, webcast or any other communication by means of which all persons participating in the

meeting can hear each other at the same time, and participation by such means shall constitute presence in person at such meeting.

4.4 **Special Meetings of the Board**. Special meetings of the Board of Directors may be called at the request of the Chair, or by Directors holding twenty percent (20%) or more of the Individual Votes. The Chair may fix any place as the place for holding any special meeting of the Board.

4.5 **Notice of Special Meetings**. Notice of any special meeting of the Board of Directors shall be given at least two (2) days prior to the special meeting by written notice delivered personally, or sent by mail or electronic mail to each Director at the address as shown by the records of the Corporation. If mailed, such notice shall be deemed to be delivered when deposited in the United States mail in a sealed envelope so addressed, with postage prepaid. If sent by electronic mail, such notice shall be deemed to be delivered when sent via electronic mail. Any Director may waive notice of any meeting. The attendance of a Director at any meeting shall constitute a waiver of notice of such meeting, except where a Director attends a meeting for the express purpose of objecting to the transaction of any business because the meeting is not lawfully called or convened. Neither the business to be transacted at, nor the purpose of, any special meeting of the Board need be specified in the notice or waiver of notice of such meeting, unless specifically required by law or by these Bylaws.

4.6 **Election of Board Officers and Executive Committee**. Biennially, at the April meeting, the Board of Directors shall elect Board Officers from among the Directors for the positions of Chair, Vice Chair, and Secretary-Treasurer, each for a term of two (2) years beginning on July 1st after the election. No Director may serve in more than one (1) Board Officer position at the same time. The Chair shall conduct all meetings and shall be responsible for the preparation of the agenda. In the Chair's absence, the Vice Chair shall serve as acting Chair. In the event that a Board Officer cannot complete his or her term, the Board of Directors may hold a special election to elect a replacement Board Officer for the remainder of the unexpired term.

At the same time, the Board shall also approve representatives to the Executive Committee nominated by the Sectors to serve for a period of two (2) years. Each Sector may also elect alternates to the Executive Committee, and, if a Sector has more than one (1) representative on the Executive Committee, such Sector shall designate the priority of succession by such alternates.

4.7 **Agenda**. As far in advance of each regular and special meeting as practical, an agenda shall be distributed to each Director and Customer Advisor.

4.8 **Voting Definitions**.

(a) "Adjusted Weighted Vote" shall mean the number of votes of each Director determined in the manner set forth in Section 4.9 hereof.

(b) "Simple Majority" shall require the presence of a quorum and the (i) concurrence of Directors whose combined Individual Votes are greater than fifty percent (50%) of the total Individual Votes of all Directors present at the meeting and entitled to vote on the issue (the “Individual Vote Test”), (ii) concurrence of Directors whose combined Adjusted Weighted Votes are greater than fifty percent (50%) of the total Adjusted Weighted Vote of all Directors at the meeting and entitled to vote on the issue (the “Adjusted Weighted Vote Test”), and (iii) for at least one of the Individual Vote Test or the Adjusted Weighted Vote Test, on an individual Sector basis, the positive vote shall outweigh the negative vote for at least three Sectors.

(c) "Supermajority" shall require the presence of a quorum and the concurrence of (i) Directors whose combined Individual Votes equal or exceed two-thirds (2/3) of the total Individual Votes of all Directors present at the meeting and entitled to vote on the issue, provided that a quorum is present, and (ii) Directors whose combined Adjusted Weighted Votes are greater than two-thirds (2/3) of the total Adjusted Weighted Vote of all Directors present at the meeting and entitled to vote on the issue.

(d) "Individual Vote" shall mean a single vote accorded to each Director.

(e) "Given Year" shall mean the applicable fiscal year for which the Adjusted Weighted Votes are calculated.

(f) "Reporting Year" shall mean the fiscal year immediately preceding the Given Year.

(g) "Previous Year" shall mean the fiscal year immediately preceding the Reporting Year.

4.9 **Determination of Adjusted Weighted Vote**. The Directors’ Adjusted Weighted Votes for a Given Year shall be determined by the following formula:

V = 10(1/N) + 30(B/C) + 30(D/E) + 30(F/G)

V = % of Adjusted Weighted Vote

N = total number of Member Companies

B = Member Company’s Previous Year internal peak demand

C = total of factor B for all Member Companies

D = Member Company's owned generating capacity as of January 1 of the Reporting Year

E = total of factor D for all Member Companies

F = Member Company's sum of circuit miles of transmission times the respective operating voltage for facilities of 69 kV and above as of December 31 of the Previous Year

G = total of factor F for all Member Companies

4.10 **Voting; Manner of Acting; Voting Rights; Quorum; Proxies**.

(a) Except as otherwise provided in these Bylaws, all actions by the Board of Directors require approval by a Simple Majority vote.

(b) A motion shall be deemed to have passed if it passes either:

(i) the Individual Vote Test; or
(ii) the Adjusted Weighted Vote Test;

and, for purposes of the failed test (any test that is not satisfied), on an individual Sector basis, the positive votes outweigh the negative votes in every Sector but one.

(c) Directors holding two-thirds (2/3) of the Individual Votes shall constitute a quorum for action by the Board. If Directors holding less than two-thirds (2/3) of the Individual Votes are present at the meeting, a majority of the Directors present may adjourn the meeting from time to time without further notice.

(d) The intent of Section 4.8(b)(iii) and Section 4.10(b) is to ensure that no two Sectors should be able to control any decision and that a single Sector should not be able to veto any matter, respectively (other than amendments to these Bylaws). In the event that either of the foregoing shall nevertheless occur, the Member Companies shall promptly revise the provisions of these Bylaws so that no two Sectors shall be able to control any decision and no single Sector shall be able to veto any matter.

4.11 **Compensation**. Directors shall not receive any compensation from the Corporation for their services to the Corporation.

4.12 **Informal Action by Directors**. Any action required by law to be taken at a meeting of Directors, or any action which may be taken at a meeting of Directors, may

be taken without a meeting if all of the Directors consent in writing to the action so taken.

4.13 **Duties**. The Board of Directors shall have the exclusive responsibility to:

(a) Authorize distributions;

(b) Recommend to members or approve dissolution, merger or the sale, pledge or transfer of substantially all of the Corporation's assets;

(c) Fill vacancies on any of the Board's committees;

(d) Adopt, amend, or repeal the Articles of Incorporation or Bylaws;

(e) Form or dissolve committees of the Board as it deems necessary to carry out the business of the Corporation; and

(f) Resolve any disputes regarding the Member Companies and the Corporation, if those issues cannot be resolved by the standing committees or subcommittees of the Corporation and are not otherwise subject to NERC's dispute provisions for non-compliance with Reliability Standards.

ARTICLE V - CORPORATE OFFICERS

5.1 **Corporate Officers**. The Board of Directors shall appoint a President & Chief Executive Officer, Vice President, Secretary, and Treasurer of the Corporation. Two (2) or more of such offices may be held by the same person, except for the offices of President & Chief Executive Officer and Secretary. The Board of Directors may appoint such other officers and assistant officers as it deems necessary.

5.2 **President & Chief Executive Officer**. The President shall be the Chief Executive Officer of the Corporation and shall manage the operations of the Corporation to the end that its purposes shall be accomplished. The Board Officers shall determine the compensation and benefits for the President & Chief Executive Officer (President). The President shall:

(a) Attend all Board of Directors meetings of the Corporation and NERC Stakeholder and Board of Trustees, meetings, as appropriate;

(b) Assist and coordinate the preparation of testimony and reports;

(c) Coordinate subregional activities and interregional affairs, to include data collection;

(d) Install and maintain an adequate system of accounts and records;

(e) Arrange for meetings as directed;

(f) Assist the Corporation Committee Chairs as appropriate;

(g) Manage the business affairs of the Corporation, including the Corporation staff;

(h) Maintain minutes of all the Corporation-related meetings; and

(i) Provide other assistance to the Corporation and NERC, as appropriate.

5.3 **Vice President.** The Vice President shall perform such duties and exercise such powers as may be assigned to him or her from time to time by the Board of Directors, the Executive Committee, or the President. In the absence of the President, or in the case of the President's inability to act, the Vice President shall perform the duties and exercise the powers of the President, but subject to the control of the Board of Directors and the Executive Committee. The Board Officers shall determine the compensation and benefits of the Vice President.

5.4 **Secretary.** The Secretary shall be custodian of the records and of the seal of the Corporation and in general shall perform all duties incident to the office of Secretary and such other duties as may, from time to time, be assigned to him or her by the Board of Directors, the Executive Committee, or the President.

5.5 **Treasurer.** The Treasurer shall have charge and custody of, and be responsible for, all funds and securities of the Corporation and deposit all such funds in the name of the Corporation in such banks, trust companies, or other depositaries as shall be selected in accordance with the provisions of these Bylaws; and in general, perform all of the duties incident to the office of Treasurer and such other duties as from time to time may be assigned to him or her by the Board of Directors, the Executive Committee, or the President.

ARTICLE VI - EXECUTIVE COMMITTEE

6.1 **Executive Committee Representatives**. The Executive Committee shall be comprised of twelve (12) Sector representatives from the Board of Directors, consisting of:

(a) The Investor-Owned Utility Sector shall have three (3) representatives;

(b) The Federal/State Sector shall have two (2) representatives;

(c) The Cooperative Sector shall have two (2) representatives;

(d) The Municipal Sector shall have two (2) representatives;

(e) The Marketer Sector shall have one (1) representative;

(f) The Merchant Electricity Generator Sector shall have one (1) representative; and

(g) The ISO-RTO Sector shall have one (1) representative.

It is the desire of the Board of Directors that the Cooperative and Municipal sectors have representation from both transmission dependent and transmission owning Members. Each Sector shall be responsible for nominating their representative(s) and alternates from among the Directors. The Chair of the Board shall serve as Chair of the Executive Committee and shall conduct all meetings and shall be responsible for the preparation of the agenda. In the event that a representative on the Executive Committee is unable to complete a term, the Sector's alternate shall replace such representative.

6.2 **Ex Officio Representatives**. The Chair, Vice Chair, and Secretary-Treasurer of the Board of Directors shall also be ex officio representatives on the Executive Committee, but shall not have voting rights unless such Board Officer is also elected by a Sector to the Executive Committee pursuant to Section 6.1 above.

6.3 **Authority of Executive Committee**. Except as limited by Section 55A-8-25 of the North Carolina Nonprofit Corporation Act and Section 4.13 of these Bylaws, the Executive Committee is empowered to make all such decisions and take such actions as are deemed to be necessary for the operation of the Corporation.

6.4 **Action.** Each voting representative on the Executive Committee shall have one vote. The presence of three-quarters (3/4) of the voting representatives on the Executive Committee shall constitute a quorum. The positive vote of two-thirds

(2/3) of Executive Committee voting representatives present and voting is necessary to pass a particular action.

ARTICLE VII - OTHER COMMITTEES

7.1 **Designation by Board**. The Board of Directors, by resolution adopted by a Simple Majority vote, may designate Board committees and standing committees, as shall be necessary to address the purposes of the Corporation. Each Board committee shall have at least two Directors among its members.

7.2 **Rules for Governance**. Each committee shall adopt rules for its own governance that are not inconsistent with these Bylaws, rules adopted by the Board of Directors, applicable NERC or FERC rules or regulations, or applicable state or federal laws. Each committee shall maintain its rules for governance in a written scope document that is approved by the Board of Directors.

7.3 **Ad-Hoc Support Committees**. The Board or its committees may, from time to time, appoint ad-hoc committees to research and/or advise it on compliance or technical issues or matters, among other things. Such ad-hoc committees may be formed on an as-needed basis and may vary in makeup depending on the needs of the Board or its committees.

ARTICLE VIII - MISCELLANEOUS

8.1 **Conflicts of Interest.** All Directors, Alternate Directors, Customer Advisors, and Board committee representatives shall comply with the Corporation's Standards of Conduct policy that prohibits conflicts of interest, as such conflicts could cast doubt on the ability of such persons to act with total objectivity with regard to the overall interests of the Corporation.

8.2 **Contracts**. The Board of Directors may authorize any officer or agent of the Corporation, in addition to the officers so authorized by these Bylaws, to enter into any contract or execute and deliver any instrument in the name of and on behalf of the Corporation, and such authority may be general or confined to specific instances.

8.3 **Checks, Drafts, etc**. All checks, drafts, or orders for the payment of money, notes or other evidences of indebtedness issued in the name of the Corporation, shall be signed by an authorized officer or agent of the Corporation and in such manner as shall from time to time be determined by resolution of the Executive Committee. In the absence of such determination by the Executive Committee, such

instruments shall be signed by the Board's Secretary-Treasurer, the Corporation's President, or the Corporation's Finance Director, as stipulated by the Executive Committee. The Corporation's Finance Director may arrange audits of financial records, sign appropriate documents, and perform such duties normally performed by the Board's Secretary-Treasurer, except duties assigned to the Corporation's President.

8.4 **Deposits**. All funds of the Corporation shall be deposited from time to time to the credit of the Corporation in such banks, trust companies, or other depositories as the Corporation's President may select.

8.5 **Books and Records**. The Corporation shall keep correct and complete books and records of account and shall also keep minutes of the proceedings of the Board of Directors and committees having any of the authority of the Board of Directors, and shall keep at its registered or principal office a record giving the names and addresses of the Directors. All books and records of the Corporation may be inspected by any Director, or agent or attorney representing any Director, for any proper purpose at any reasonable time.

8.6 **Seal**. The corporate seal shall be in circular form and shall have inscribed thereon the name of the Corporation, the words "Corporate Seal", and such other word or words, if any, as may be determined by the Board of Directors to be inscribed thereon.

8.7 **Fiscal Year.** The fiscal year of the Corporation shall begin on the first day of January and end on the last day of December in each year.

ARTICLE IX - EXPENSES

9.1 **Allocation of Specific Expenses.** The expenses of Directors and Board Officers shall be borne by that person's regular employer.

9.2 **Statutory Functions.** The Corporation anticipates that as a general rule all of its expenses shall be incurred in the furtherance of statutory activities pursuant to Section 215 of the Federal Power Act, and that all such expenses shall be funded by NERC, subject to FERC approval.

9.3 **Non-Statutory Functions.** Notwithstanding Section 9.2, the Board of Directors may from time to time authorize the Corporation to participate in non-statutory activities (i.e., activities not described in Section 215 of the Federal Power Act). In the event that the Corporation proposes to engage in non-statutory activities, such activities shall be identified in the Corporation's annual business plan that is submitted to NERC and, if approved by NERC, shall be submitted to FERC for approval in advance of engaging in such non-statutory activities. The expenses incurred by the Corporation for

any such approved non-statutory activities shall be allocated by the Board of Directors to the beneficiaries of such activities on a basis proposed in the business plan submitted for NERC and FERC approval.

ARTICLE X - DISPUTE RESOLUTION PROCESS

10.1 **Dispute Resolution.** All disputes regarding non-compliance with Reliability Standards shall be handled in accordance with the NERC Rules of Procedure. The organizational units of the Corporation shall deal with all other disputes within the framework of their respective organizations. For such other disputes, Member Companies of the Corporation are encouraged to utilize the appropriate Dispute Resolution Process within the Corporation prior to seeking resolution at NERC, FERC, or with legal counsel.

ARTICLE XI - DISSOLUTION

11.1 **Dissolution**. The Corporation may be voluntarily dissolved upon unanimous consent of its Member Companies, and in accordance with Section 55A-14-02 of the North Carolina Nonprofit Corporation Act, as amended from time to time.

11.2 **Distribution of Assets**. Upon dissolution of the Corporation as provided in Section 11.1, the residual assets, after payment of all just obligations, shall be distributed exclusively to organizations which are exempt from federal income tax under Section 501(c)(6) of the Internal Revenue Code of 1986, or corresponding provisions of any subsequent federal tax laws, as the Board of Directors shall determine.

ARTICLE XII - WAIVER OF NOTICE

12.1 **Waiver.** Whenever any notice is required to be given under the provisions of the North Carolina Nonprofit Corporation Act or under the provisions of the articles of incorporation or the Bylaws of the Corporation, a waiver thereof in writing signed by the person or persons entitled to such notice, whether before or after the time stated therein, shall be deemed equivalent to the giving of such notice.

ARTICLE XIII - INDEMNIFICATION

13.1 **Indemnification of Directors, Alternate Directors, Customer Advisors, Committee Members, Officers, Employees and Agents**. Every person who is, or has served as, a Director, Alternate Director, Customer Advisor, committee member, Officer, employee, or agent of the Corporation shall be indemnified by the Corporation in the manner and to the extent authorized by the North Carolina Nonprofit Corporation Act. The foregoing rights of indemnification shall be without prejudice to any other rights to which any such Director, Alternate Director, Customer Advisor, committee member, Officer, employee, or agent may be entitled as a matter of law.

ARTICLE XIV - AMENDMENT OF THE BYLAWS AND ARTICLES OF INCORPORATION

14.1 **Amendment of the Bylaws and Articles of Incorporation**. After a request by twenty percent (20%) of the Board of Directors or an affirmative vote of the Executive Committee, a proposal to amend the Bylaws or the Articles of Incorporation shall be put before the Board of Directors at any regular or special meeting for a vote. Copies of the proposed amendments shall be distributed to the Board of Directors at least thirty (30) days before the meeting at which they are to be considered. An amendment to the Bylaws or the Articles of Incorporation shall be adopted after being approved by a Supermajority vote of the Board of Directors, provided that a quorum is present.

ATTACHMENT 3

AMENDED EXHIBIT B OF THE DELEGATION AGREEMENT

BETWEEN

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

AND

SERC RELIABILITY CORPORATION

REDLINED VERSION

AMENDED AND RESTATED

BYLAWS

OF

SERC RELIABILITY CORPORATION

A North Carolina Nonprofit Corporation

Approved by the Board of Directors on October 23, 2013

TABLE OF CONTENTS

ARTICLE I - OFFICES 1
1.1 **Principal Office** 1
1.2 **Other Offices** 1

ARTICLE II - MEMBERSHIP 1
2.1 **General** 1
2.2 **Eligibility** 1
2.3 **Termination** 2
2.4 **Sectors** 2
2.5 **Transfer of Membership** 3
2.6 **Powers** 3

ARTICLE III - PURPOSES 3
3.1 **General Purposes** 3
3.2 **Geographic Area** 4
3.3 **Other Statutory Functions** 4

ARTICLE IV - BOARD OF DIRECTORS 4
4.1 **General Powers** 4
4.2 **Composition and Eligibility** 5
4.3 **Regular Meetings of the Board** 5
4.4 **Special Meetings of the Board** ..... ~~5~~6
4.5 **Notice of Special Meetings** 6
4.6 **Election of Board Officers and Executive Committee** 6
4.7 **Agenda** 6
4.8 **Voting Definitions** 6
4.9 **Determination of Adjusted Weighted Vote** 7
4.10 **Voting; Manner of Acting; Voting Rights; Quorum; Proxies** 8
4.11 **Compensation** 8
4.12 **Informal Action by Directors** 8
4.13 **Duties** 9

ARTICLE V - CORPORATE OFFICERS 9
5.1 **Corporate Officers** 9
5.2 **President & Chief Executive Officer** 9
5.3 **Vice President** 10
5.4 **Secretary** 10
5.5 **Treasurer** 10

ARTICLE VI - EXECUTIVE COMMITTEE 11
6.1 **Executive Committee Representatives** 11
6.2 **Ex Officio Representatives** 11
6.3 **Authority of Executive Committee** 11
6.4 **Action** 11

ARTICLE VII - OTHER COMMITTEES 12
7.1 **Designation by Board** 12
7.2 **Rules for Governance** 12
7.3 **Ad-Hoc Support Committees** 12

ARTICLE VIII - MISCELLANEOUS 12
8.1 **Conflicts of Interest** 12
8.2 **Contracts** 12
8.3 **Checks, Drafts, etc.** 12
8.4 **Deposits** 13
8.5 **Books and Records** 13
8.6 **Seal** 13
8.7 **Fiscal Year** 13

ARTICLE IX - EXPENSES 13
9.1 **Allocation of Specific Expenses** 13
9.2 **Statutory Functions** 13
9.3 **Non-Statutory Functions** 13

ARTICLE X - DISPUTE RESOLUTION PROCESS 14
10.1 **Dispute Resolution** 14

ARTICLE XI - DISSOLUTION 14
11.1 **Dissolution** 14
11.2 **Distribution of Assets** 14

ARTICLE XII - WAIVER OF NOTICE 14
12.1 **Waiver** 14

ARTICLE XIII - INDEMNIFICATION ..... ~~14~~15
13.1 **Indemnification of Directors, Committee Members, Officers, Employees and Agents** ..... ~~14~~15

ARTICLE XIV – AMENDMENT OF THE BYLAWS AND ARTICLES OF INCORPORATION 15
14.1 **Amendment of the Bylaws and Articles of Incorporation** 15

AMENDED AND RESTATED

BYLAWS

OF

SERC RELIABILITY CORPORATION
[Hereinafter referred to as the "Corporation"]

A North Carolina Nonprofit Corporation

ARTICLE I - OFFICES

1.1 **Principal Office**. The principal office of the Corporation shall be located in the City of Charlotte, Mecklenburg County, North Carolina. The Board of Directors may by resolution change the location of this office from time to time.

1.2 **Other Offices**. The Corporation may have other offices at such place or places as the Board of Directors may from time to time appoint or the business of the Corporation may require.

ARTICLE II - MEMBERSHIP

2.1 **General**. The Corporation shall be a membership corporation. Entities that meet the eligibility requirements and apply for membership in the Corporation shall hereinafter be referred to individually as a "Member Company" and collectively as "Member Companies".

2.2 **Eligibility**. Membership in the Corporation is open to any entity in the SERC Region (defined in Section 3.2 below) that is a user, owner or operator of the Bulk Power System and is subject to the jurisdiction of the Federal Energy Regulatory Commission for the purpose of complying with Reliability Standards established under Section 215 of the Federal Power Act and all amendments thereto. Membership in the Corporation is voluntary; however, membership is predicated on mandatory acceptance of the responsibility to promote, support, and comply with Reliability Standards of the Corporation and the North American Electric Reliability Corporation ("NERC"), and to assist the Corporation in its compliance with the terms and provisions of a Delegation Agreement (a "Delegation Agreement") with NERC, by which NERC delegates authority to propose and enforce Reliability Standards, pursuant to 16 U.S.C. § 824o or the corresponding provisions of any subsequent U.S. Code revisions. For purposes of

these Bylaws, the terms “Bulk Power System”, “Reliability Standards” and “Regional Entity” shall be as defined in 16 U.S.C. § 824o or the corresponding provisions of any subsequent U.S. Code revisions.

2.3 **Termination**. A Member Company may terminate its membership in the Corporation by giving the Board of Directors at least thirty (30) days written notice of its intent to terminate such membership (such Member Companies shall hereinafter be referred to as "Terminated Member Companies"). Terminated Member Companies shall nevertheless continue to be liable for any and all obligations incurred prior to the end of the calendar year in which such notice is given, including, but not limited to, the obligation to pay a pro rata share of any Corporation expense. In addition to termination of membership by the Member Company, the Board of Directors, following notice to the Member Company, may terminate the membership of a Member Company if in the judgment of the Board of Directors that Member Company has violated its obligations and responsibilities to the Corporation. The termination of the membership of a Member Company by the Board of Directors shall require a Supermajority vote, as defined in these Bylaws.

2.4 **Sectors.** Each Member Company shall be classified by the Executive Committee in one of the following seven (7) Sectors (each a “Sector”, and collectively, the “Sectors”):

(a) Investor-Owned Utility Sector – This Sector includes any investor-owned entity with substantial business interest in ownership and/or operation in any of the asset categories of generation, transmission or distribution.

(b) Federal/State Sector – This Sector includes any U.S. federal entity that owns and/or operates electric facilities and/or provides balancing authority services, in any of the asset categories of generation, transmission, or distribution; or any entity that is owned by or subject to the governmental authority of a state and that is engaged in the generation, delivery, and/or sale of electric power to end-use customers primarily within the political boundaries of the state.

(c) Cooperative Sector – This Sector includes any non-governmental entity that is incorporated under the laws of the state in which it operates, is owned by and provides electric service to end-use customers at cost, and is governed by a board of directors that is elected by the membership of the entity; and any non-governmental entity owned by and which provides generation and/or transmission service to such entities.

(d) Municipal Sector – This Sector includes any entity owned by or subject to the governmental authority of a municipality, that is

engaged in the generation, delivery, and/or sale of electric power to end-use customers primarily within the political boundaries of the municipality; and any entity, whose members are municipalities, formed under state law for the purpose of generating or purchasing electricity for sale at wholesale to their members.

(e) Marketer Sector– This Sector includes any entity that is engaged in the activity of buying and selling of wholesale electric power in the SERC Region on a physical or financial basis.

(f) Merchant Electricity Generator Sector – This Sector includes any entity that owns or operates an electricity generating facility or provides balancing authority services for such entities. This includes, but is not limited to, small power producers and all other non-utility producers such as exempt wholesale generators who sell electricity at wholesale.

(g) ISO-RTO Sector – This Sector includes any entity that operates a FERC approved ISO or RTO.

The Executive Committee's classification of a Member Company in a particular Sector may only be changed by the Executive Committee.

2.5 **Transfer of Membership.** A Member Company may not give or otherwise transfer its membership, except to a successor that becomes a Member Company in accordance with the terms and conditions of these Bylaws, and provided that the successor continues to meet its predecessor's obligations.

2.6 **Powers.** Notwithstanding any other provisions of these Bylaws, except for the appointment of Directors as provided in Section 4.2 below, Member Companies shall be non-voting members and shall have no power or authority or right to vote with respect to the actions of the Corporation, specifically including, but not limited to, the dissolution or merger of the Corporation.

ARTICLE III - PURPOSES

3.1 **General Purposes.** The purpose of the Corporation is to promote effective and efficient administration of Bulk Power System reliability in the SERC Region, as defined in Section 3.2. In pursuit of this goal, the Corporation shall:

(a) enter into a Delegation Agreement to serve as a Regional Entity pursuant to 16 U.S.C. § 824o or the corresponding provisions of any subsequent U.S. Code revisions;

(b) promote the development of reliability and adequacy arrangements among the systems in the SERC Region;

(c) participate in the establishment of Reliability Standards;

(d) participate in the measurement of performance relative to these Reliability Standards;

(e) promote conformance to and compliance with these Reliability Standards;

(f) develop and exchange information with respect to planning and operating matters relating to the reliability and adequacy of the Bulk Power System;

(g) review as necessary activities in the SERC Region on reliability and adequacy in order to meet Reliability Standards;

(h) provide a mechanism to resolve disputes on reliability issues in a manner that meets the needs of the parties and the SERC Region; and

(i) provide information with respect to matters considered by the Corporation, where appropriate, to the Federal Energy Regulatory Commission ("FERC") and to other federal and state agencies concerned with reliability and adequacy.

3.2 **Geographic Area.** The Corporation accomplishes its purposes in a geographic area (the "SERC Region") that is defined in Exhibit A of the Amended and Restated Delegation Agreement Between North American Electric Reliability Corporation and SERC Reliability Corporation.

3.3 **Other Statutory Functions.** The Corporation may also perform statutory functions outside of the SERC Region, on behalf of NERC or other Regional Entities. The Corporation may undertake such activities pursuant to a contract that is approved by the Executive Committee.

ARTICLE IV - BOARD OF DIRECTORS

4.1 **General Powers**. The affairs of the Corporation shall be managed by its Board of Directors except as otherwise provided in these Bylaws.

4.2 **Composition and Eligibility**. The Board of Directors shall be comprised of no fewer than three (3) Directors and no more than two (2) Customer Advisors.

Each Director shall be the principal officer or other authorized employee from a Member Company or a company that controls, is controlled by, or is under common control with such Member Company (an "affiliated entity"). Each Member Company, together with any affiliated entities, may appoint one (1) Director to the Board of Directors. For clarification purposes only, each Member Company and all of such Member Company's affiliated entities (including any affiliated entities which may be a separate Member Company) shall have the right to appoint only one (1) Director to serve on behalf of such Member Company and all of such Member Company's affiliated entities. Each Director shall serve until otherwise replaced by the applicable Member Company, together with any affiliated entities. Each Member Company, together with any affiliated entities, may designate one (1) alternate Director, who shall be a principal officer or other authorized employee from the Director's Member Company or an affiliated entity, to serve in the place of the Member Company's Director at any meeting of the Board of Directors (an "Alternate Director"). Directors may not otherwise use proxy votes. Any vacancy occurring among the Directors or Alternate Directors shall be filled by the applicable Member Company, together with any affiliated entities.

Each Customer Advisor shall be a person who is (i) employed by an entity that receives service at retail and does not otherwise sell, purchase, or transmit power over the Bulk Power System or own, operate or maintain, control or operate facilities or systems that are part of the Bulk Power System; (ii) a state public utility commission representative; or (iii) any other customer advocate. Should the Board of Directors not include two (2) Customer Advisors, the Board of Directors may elect additional Customer Advisors to fill such vacancies. The term of these Customer Advisors shall be for a two (2) year period.

The Chair of FERC and the chair or president of any State Utility Commission in a state in which electric service is provided by a Member Company of the Corporation shall be invited to designate an observer to attend meetings of the Board.

4.3 **Regular Meetings of the Board**. Unless otherwise determined by the Chair, a regular meeting of the Board of Directors shall be held without other notice than these Bylaws on the fourth Wednesday in the months of April and October in each year. Notwithstanding the foregoing, the Chair may elect to hold a regular semi-annual meeting of the Board of Directors on another date provided that the Board receives at least ten (10) days advance notice. If the day fixed for the meeting shall be a legal holiday in the State of North Carolina, the meeting shall be held on the next succeeding business day. The Board of Directors may designate any place as the place of meeting for any meeting. The Board of Directors may provide by resolution the time and place for the holding of additional regular meetings of the Board without other notice than the resolution. Directors or any committee designated by the Board of Directors may participate in such Board or committee meetings by means of a telephone conference, webcast or any other communication by means of which all persons participating in the

meeting can hear each other at the same time, and participation by such means shall constitute presence in person at such meeting.

4.4 **Special Meetings of the Board**. Special meetings of the Board of Directors may be called at the request of the Chair, or by Directors holding twenty percent (20%) or more of the Individual Votes. The Chair may fix any place as the place for holding any special meeting of the Board.

4.5 **Notice of Special Meetings**. Notice of any special meeting of the Board of Directors shall be given at least two (2) days prior to the special meeting by written notice delivered personally, or sent by mail or electronic mail to each Director at the address as shown by the records of the Corporation. If mailed, such notice shall be deemed to be delivered when deposited in the United States mail in a sealed envelope so addressed, with postage prepaid. If sent by electronic mail, such notice shall be deemed to be delivered when sent via electronic mail. Any Director may waive notice of any meeting. The attendance of a Director at any meeting shall constitute a waiver of notice of such meeting, except where a Director attends a meeting for the express purpose of objecting to the transaction of any business because the meeting is not lawfully called or convened. Neither the business to be transacted at, nor the purpose of, any special meeting of the Board need be specified in the notice or waiver of notice of such meeting, unless specifically required by law or by these Bylaws.

4.6 **Election of Board Officers and Executive Committee**. Biennially, at the April meeting, the Board of Directors shall elect Board Officers from among the Directors for the positions of Chair, Vice Chair, and Secretary-Treasurer, each for a term of two (2) years beginning on July 1st after the election. No Director may serve in more than one (1) Board Officer position at the same time. The Chair shall conduct all meetings and shall be responsible for the preparation of the agenda. In the Chair's absence, the Vice Chair shall serve as acting Chair. In the event that a Board Officer cannot complete his or her term, the Board of Directors may hold a special election to elect a replacement Board Officer for the remainder of the unexpired term.

At the same time, the Board shall also approve representatives to the Executive Committee nominated by the Sectors to serve for a period of two (2) years. Each Sector may also elect alternates to the Executive Committee, and, if a Sector has more than one (1) representative on the Executive Committee, such Sector shall designate the priority of succession by such alternates.

4.7 **Agenda**. As far in advance of each regular and special meeting as practical, an agenda shall be distributed to each Director and Customer Advisor.

4.8 **Voting Definitions**.

(a) "Adjusted Weighted Vote" shall mean the number of votes of each Director determined in the manner set forth in Section 4.9 hereof.

(b) "Simple Majority" shall require the presence of a quorum and the (i) concurrence of Directors whose combined Individual Votes are greater than fifty percent (50%) of the total Individual Votes of all Directors present at the meeting and entitled to vote on the issue (the "Individual Vote Test"), (ii) concurrence of Directors whose combined Adjusted Weighted Votes are greater than fifty percent (50%) of the total Adjusted Weighted Vote of all Directors at the meeting and entitled to vote on the issue (the "Adjusted Weighted Vote Test"), and (iii) for at least one of the Individual Vote Test or the Adjusted Weighted Vote Test, on an individual Sector basis, the positive vote shall outweigh the negative vote for at least three Sectors.

(c) "Supermajority" shall require the presence of a quorum and the concurrence of (i) Directors whose combined Individual Votes equal or exceed two-thirds (2/3) of the total Individual Votes of all Directors present at the meeting and entitled to vote on the issue, provided that a quorum is present, and (ii) Directors whose combined Adjusted Weighted Votes are greater than two-thirds (2/3) of the total Adjusted Weighted Vote of all Directors present at the meeting and entitled to vote on the issue.

(d) "Individual Vote" shall mean a single vote accorded to each Director.

(e) "Given Year" shall mean the applicable fiscal year for which the Adjusted Weighted Votes are calculated.

(f) "Reporting Year" shall mean the fiscal year immediately preceding the Given Year.

(g) "Previous Year" shall mean the fiscal year immediately preceding the Reporting Year.

4.9 **Determination of Adjusted Weighted Vote**. The Directors' Adjusted Weighted Votes for a Given Year shall be determined by the following formula:

V = 10(1/N) + 30(B/C) + 30(D/E) + 30(F/G)

V = % of Adjusted Weighted Vote

N = total number of Member Companies

B = Member Company's Previous Year internal peak demand

C = total of factor B for all Member Companies

D = Member Company's owned generating capacity as of January 1 of the Reporting Year

E = total of factor D for all Member Companies

F = Member Company's sum of circuit miles of transmission times the respective operating voltage for facilities of 69 kV and above as of December 31 of the Previous Year

G = total of factor F for all Member Companies

4.10 **Voting; Manner of Acting; Voting Rights; Quorum; Proxies**.

(a) Except as otherwise provided in these Bylaws, all actions by the Board of Directors require approval by a Simple Majority vote.

(b) A motion shall be deemed to have passed if it passes either:

(i) the Individual Vote Test; or
(ii) the Adjusted Weighted Vote Test;

and, for purposes of the failed test (any test that is not satisfied), on an individual Sector basis, the positive votes outweigh the negative votes in every Sector but one.

(c) Directors holding two-thirds (2/3) of the Individual Votes shall constitute a quorum for action by the Board. If Directors holding less than two-thirds (2/3) of the Individual Votes are present at the meeting, a majority of the Directors present may adjourn the meeting from time to time without further notice.

(d) The intent of Section 4.8(b)(iii) and Section 4.10(b) is to ensure that no two Sectors should be able to control any decision and that a single Sector should not be able to veto any matter, respectively (other than amendments to these Bylaws). In the event that either of the foregoing shall nevertheless occur, the Member Companies shall promptly revise the provisions of these Bylaws so that no two Sectors shall be able to control any decision and no single Sector shall be able to veto any matter.

4.11 **Compensation**. Directors shall not receive any compensation from the Corporation for their services to the Corporation.

4.12 **Informal Action by Directors**. Any action required by law to be taken at a meeting of Directors, or any action which may be taken at a meeting of Directors, may

be taken without a meeting if all of the Directors consent in writing to the action so taken.

4.13 **Duties**. The Board of Directors shall have the exclusive responsibility to:

(a) Authorize distributions;

(b) Recommend to members or approve dissolution, merger or the sale, pledge or transfer of substantially all of the ~~c~~Corporation's assets;

(c) Fill vacancies on any of the Board's committees;

(d) Adopt, amend, or repeal the Articles of Incorporation or Bylaws;

(e) Form or dissolve committees of the Board as it deems necessary to carry out the business of the Corporation; and

(f) Resolve any disputes regarding the Member Companies and the Corporation, if those issues cannot be resolved by the standing committees or subcommittees of the Corporation and are not otherwise subject to NERC's dispute provisions for non-compliance with Reliability Standards.

ARTICLE V - CORPORATE OFFICERS

5.1 **Corporate Officers**. The Board of Directors shall appoint a President & Chief Executive Officer, Vice President, Secretary, and Treasurer of the Corporation. Two (2) or more of such offices may be held by the same person, except for the offices of President & Chief Executive Officer and Secretary. The Board of Directors may appoint such other officers and assistant officers as it deems necessary.

5.2 **President & Chief Executive Officer**. The President shall be the Chief Executive Officer of the Corporation and shall manage the operations of the Corporation to the end that its purposes shall be accomplished. The Board Officers shall determine the compensation and benefits for the President & Chief Executive Officer (President). The President shall:

(a) Attend all Board of Directors meetings of the Corporation and NERC Stakeholder and Board of Trustees, meetings, as appropriate;

(b) Assist and coordinate the preparation of testimony and reports;

(c) Coordinate subregional activities and interregional affairs, to include data collection;

(d) Install and maintain an adequate system of accounts and records;

(e) Arrange for meetings as directed;

(f) Assist the Corporation Committee Chairs as appropriate;

(g) Manage the business affairs of the Corporation, including the Corporation staff;

(h) Maintain minutes of all the Corporation-related meetings; and

(i) Provide other assistance to the Corporation and NERC, as appropriate.

5.3 **Vice President.** The Vice President shall perform such duties and exercise such powers as may be assigned to him or her from time to time by the Board of Directors, the Executive Committee, or the President. In the absence of the President, or in the case of the President's inability to act, the Vice President shall perform the duties and exercise the powers of the President, but subject to the control of the Board of Directors and the Executive Committee. The Board Officers shall determine the compensation and benefits of the Vice President.

5.4 **Secretary.** The Secretary shall be custodian of the records and of the seal of the Corporation and in general shall perform all duties incident to the office of Secretary and such other duties as may, from time to time, be assigned to him or her by the Board of Directors, the Executive Committee, or the President.

5.5 **Treasurer.** The Treasurer shall have charge and custody of, and be responsible for, all funds and securities of the Corporation and deposit all such funds in the name of the Corporation in such banks, trust companies, or other depositaries as shall be selected in accordance with the provisions of these Bylaws; and in general, perform all of the duties incident to the office of Treasurer and such other duties as from time to time may be assigned to him or her by the Board of Directors, the Executive Committee, or the President.

ARTICLE VI - EXECUTIVE COMMITTEE

6.1 **Executive Committee Representatives**. The Executive Committee shall be comprised of twelve (12) Sector representatives from the Board of Directors, consisting of:

(a) The Investor-Owned Utility Sector shall have three (3) representatives;

(b) The Federal/State Sector shall have two (2) representatives;

(c) The Cooperative Sector shall have two (2) representatives;

(d) The Municipal Sector shall have two (2) representatives;

(e) The Marketer Sector shall have one (1) representative;

(f) The Merchant Electricity Generator Sector shall have one (1) representative; and

(g) The ISO-RTO Sector shall have one (1) representative.

It is the desire of the Board of Directors that the Cooperative and Municipal sectors have representation from both transmission dependent and transmission owning Members. Each Sector shall be responsible for nominating their representative(s) and alternates from among the Directors. The Chair of the Board shall serve as Chair of the Executive Committee and shall conduct all meetings and shall be responsible for the preparation of the agenda. In the event that a representative on the Executive Committee is unable to complete a term, the Sector's alternate shall replace such representative.

6.2 **Ex Officio Representatives**. The Chair, Vice Chair, and Secretary-Treasurer of the Board of Directors shall also be ex officio representatives on the Executive Committee, but shall not have voting rights unless such Board Officer is also elected by a Sector to the Executive Committee pursuant to Section 6.1 above.

6.3 **Authority of Executive Committee**. Except as limited by Section 55A-8-25 of the North Carolina Nonprofit Corporation Act and Section 4.13 of these Bylaws, the Executive Committee is empowered to make all such decisions and take such actions as are deemed to be necessary for the operation of the Corporation.

6.4 **Action.** Each voting representative on the Executive Committee shall have one vote. The presence of three-quarters (3/4) of the voting representatives on the Executive Committee shall constitute a quorum. The positive vote of two-thirds

(2/3) of Executive Committee voting representatives present and voting is necessary to pass a particular action.

ARTICLE VII - OTHER COMMITTEES

7.1 **Designation by Board**. The Board of Directors, by resolution adopted by a Simple Majority vote, may designate Board committees and standing committees, as shall be necessary to address the purposes of the Corporation. Each Board committee shall have at least two Directors among its members.

7.2 **Rules for Governance**. Each committee shall adopt rules for its own governance that are not inconsistent with these Bylaws, rules adopted by the Board of Directors, applicable NERC or FERC rules or regulations, or applicable state or federal laws. Each committee shall maintain its rules for governance in a written scope document that is approved by the Board of Directors.

7.3 **Ad-Hoc Support Committees**. The Board or its committees may, from time to time, appoint ad-hoc committees to research and/or advise it on compliance or technical issues or matters, among other things. Such ad-hoc committees may be formed on an as-needed basis and may vary in makeup depending on the needs of the Board or its committees.

ARTICLE VIII - MISCELLANEOUS

8.1 **Conflicts of Interest.** All Directors, Alternate Directors, Customer Advisors, and Board committee representatives shall comply with the Corporation's Standards of Conduct policy that prohibits conflicts of interest, as such conflicts could cast doubt on the ability of such persons to act with total objectivity with regard to the overall interests of the Corporation.

8.2 **Contracts**. The Board of Directors may authorize any officer or agent of the Corporation, in addition to the officers so authorized by these Bylaws, to enter into any contract or execute and deliver any instrument in the name of and on behalf of the Corporation, and such authority may be general or confined to specific instances.

8.3 **Checks, Drafts, etc**. All checks, drafts, or orders for the payment of money, notes or other evidences of indebtedness issued in the name of the Corporation, shall be signed by an authorized officer or agent of the Corporation and in such manner as shall from time to time be determined by resolution of the Executive Committee. In the absence of such determination by the Executive Committee, such

instruments shall be signed by the Board's Secretary-Treasurer, the Corporation's President, or the Corporation's Finance Director, as stipulated by the Executive Committee. The Corporation's Finance Director may arrange audits of financial records, sign appropriate documents, and perform such duties normally performed by the Board's Secretary-Treasurer, except duties assigned to the Corporation's President.

8.4 **Deposits**. All funds of the Corporation shall be deposited from time to time to the credit of the Corporation in such banks, trust companies, or other depositories as the Corporation's President may select.

8.5 **Books and Records**. The Corporation shall keep correct and complete books and records of account and shall also keep minutes of the proceedings of the Board of Directors and committees having any of the authority of the Board of Directors, and shall keep at its registered or principal office a record giving the names and addresses of the Directors. All books and records of the Corporation may be inspected by any Director, or agent or attorney representing any Director, for any proper purpose at any reasonable time.

8.6 **Seal**. The corporate seal shall be in circular form and shall have inscribed thereon the name of the Corporation, the words "Corporate Seal", and such other word or words, if any, as may be determined by the Board of Directors to be inscribed thereon.

8.7 **Fiscal Year.** The fiscal year of the Corporation shall begin on the first day of January and end on the last day of December in each year.

ARTICLE IX - EXPENSES

9.1 **Allocation of Specific Expenses.** The expenses of Directors and Board Officers shall be borne by that person's regular employer.

9.2 **Statutory Functions.** The Corporation anticipates that as a general rule all of its expenses shall be incurred in the furtherance of statutory activities pursuant to Section 215 of the Federal Power Act, and that all such expenses shall be funded by NERC, subject to FERC approval.

9.3 **Non-Statutory Functions.** Notwithstanding Section 9.2, the Board of Directors may from time to time authorize the Corporation to participate in non-statutory activities (i.e., activities not described in Section 215 of the Federal Power Act). In the event that the Corporation proposes to engage in non-statutory activities, such activities shall be identified in the Corporation's annual business plan that is submitted to NERC and, if approved by NERC, shall be submitted to FERC for approval in advance of engaging in such non-statutory activities. The expenses incurred by the Corporation for

any such approved non-statutory activities shall be allocated by the Board of Directors to the beneficiaries of such activities on a basis proposed in the business plan submitted for NERC and FERC approval.

ARTICLE X - DISPUTE RESOLUTION PROCESS

10.1 **Dispute Resolution.** All disputes regarding non-compliance with Reliability Standards shall be handled in accordance with the NERC Rules of Procedure. The organizational units of the Corporation shall deal with all other disputes within the framework of their respective organizations. For such other disputes, Member Companies of the Corporation are encouraged to utilize the appropriate Dispute Resolution Process within the Corporation prior to seeking resolution at NERC, FERC, or with legal counsel.

ARTICLE XI - DISSOLUTION

11.1 **Dissolution**. The Corporation may be voluntarily dissolved upon unanimous consent of its Member Companies, and in accordance with Section 55A-14-02 of the North Carolina Nonprofit Corporation Act, as amended from time to time.

11.2 **Distribution of Assets**. Upon dissolution of the Corporation as provided in Section 11.1, the residual assets, after payment of all just obligations, shall be distributed exclusively to organizations which are exempt from federal income tax under ~~Section 501(c)(3)~~Section 501(c)(6) of the Internal Revenue Code of 1986, or corresponding provisions of any subsequent federal tax laws, as the Board of Directors shall determine, ~~or to federal, state, or local governments to be used exclusively for public purposes.~~

ARTICLE XII - WAIVER OF NOTICE

12.1 **Waiver.** Whenever any notice is required to be given under the provisions of the North Carolina Nonprofit Corporation Act or under the provisions of the articles of incorporation or the Bylaws of the Corporation, a waiver thereof in writing signed by the person or persons entitled to such notice, whether before or after the time stated therein, shall be deemed equivalent to the giving of such notice.

ARTICLE XIII - INDEMNIFICATION

13.1 **Indemnification of Directors, Alternate Directors, Customer Advisors, Committee Members, Officers, Employees and Agents**. Every person who is, or has served as, a Director, Alternate Director, Customer Advisor, committee member, Officer, ~~Director by virtue of serving as an Alternate Director,~~ employee, or agent of the Corporation shall be indemnified by the Corporation in the manner and to the extent authorized by the North Carolina Nonprofit Corporation Act. The foregoing rights of indemnification shall be without prejudice to any other rights to which any such Director, Alternate Director, Customer Advisor, committee member, Officer, ~~Alternate Director,~~ employee, or agent may be entitled as a matter of law.

ARTICLE XIV - AMENDMENT OF THE BYLAWS AND ARTICLES OF INCORPORATION

14.1 **Amendment of the Bylaws and Articles of Incorporation**. After a request by twenty percent (20%) of the Board of Directors or an affirmative vote of the Executive Committee, a proposal to amend the Bylaws or the Articles of Incorporation shall be put before the Board of Directors at any regular or special meeting for a vote. Copies of the proposed amendments shall be distributed to the Board of Directors at least thirty (30) days before the meeting at which they are to be considered. An amendment to the Bylaws or the Articles of Incorporation shall be adopted after being approved by a Supermajority vote of the Board of Directors, provided that a quorum is present.

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 6th day of June, 2014.

/s/ Thomas DeVita
Thomas DeVita

Counsel for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Generator Relay Loadability and	**)**	**Docket Nos. RM13-19-000**
Revised Transmission Relay Loadability	**)**	**RM14-3-000**
Reliability Standards	**)**	

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

On March 20, 2014, the Federal Energy Regulatory Commission ("FERC" or the "Commission") issued a Notice of Proposed Rulemaking ("NOPR")[1] proposing to approve proposed Reliability Standards PRC-025-1[2] (Generator Relay Loadability) and PRC-023-3[3] (Transmission Relay Loadability) submitted by the North American Electric Reliability Corporation ("NERC"). NERC supports the Commission's proposal to approve the proposed Reliability Standards as filed. NERC agrees with the Commission that the proposed Reliability Standards will serve to enhance reliability by imposing mandatory requirements governing generator relay loadability, thereby reducing the likelihood of premature or unnecessary tripping of generators during system disturbances. NERC looks forward to the Commission's final rule on these proposed Reliability Standards and respectfully requests that the Commission maintain its proposal to approve the proposed PRC-025-1 and PRC-023-3 Reliability Standards.

---

1 *Generator Relay Loadability and Revised Transmission Relay Loadability Reliability Standards,* 146 FERC ¶ 61,189 (2014) ("NOPR").

2 NERC Sept. 30, 2013 *Petition for Approval of PRC-025-1*, Docket No. RM13-19-000. The purpose of proposed Reliability Standard PRC-025-1 is to set load-responsive protective relays associated with generation Facilities at a level to prevent unnecessary tripping of generators during a system disturbance for conditions that do not pose a risk of damage to the associated equipment.

3 NERC Dec. 17, 2013 *Supplemental Information to Petition for Approval of PRC-025-1*, Docket No. RM14-3-000. The purpose of proposed Reliability Standard PRC-023-3 is to ensure protective relay settings: do not limit transmission loadability; do not interfere with a system operators' ability to take remedial action to protect system reliability; and are set to reliably detect all fault conditions and protect the electrical network from these faults.

Notices and communications with respect to this filing may be addressed to:[4]

Charles A. Berardesco*
Senior Vice President and General Counsel
Holly A. Hawkins*
Associate General Counsel
William H. Edwards*
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
william.edwards@nerc.net

Mark G. Lauby*
Vice President and Director of Standards
Steven Noess*
Associate Director of Standards Development
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595 – facsimile
mark.lauby@nerc.net
steven.noess@nerc.net

Respectfully submitted,

/s/ William H. Edwards

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Associate General Counsel
William H. Edwards
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
william.edwards@nerc.net

April 21, 2014

Counsel for North American Electric Reliability Corporation

[4] Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of 18 C.F.R. § 385.203(b) (2014) to permit the inclusion of more than two people on the service list.

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in the proceeding. Dated at Washington, D.C. this 21st day of April, 2014.

/s/ William H. Edwards
William H. Edwards
Counsel for North American Electric Reliability Corporation

SCHIFF HARDIN LLP
A Limited Liability Partnership

Owen E. MacBride
(312) 258-5680
Email: omacbride@schiffhardin.com

233 SOUTH WACKER DRIVE
SUITE 6600
CHICAGO, ILLINOIS 60606

Tel.: 312.258.5500
Fax: 312.258.5700

www.schiffhardin.com

May 30, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

Re: North American Electric Reliability Corporation
Docket No. RR14-_-000
Report of Comparisons of Budgeted to Actual Costs for 2013 for NERC and the Regional Entities

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby submits the "North American Electric Reliability Corporation's Report of Comparisons of Budgeted to Actual Costs for 2013 for NERC and the Regional Entities."

This filing consists of: (1) this transmittal letter, (2) the narrative text of the filing, which follows this transmittal letter, and (3) Attachments 1 through 10. The Table of Contents to the narrative text list the 10 attachments.

Please contact the undersigned if you have any questions concerning this filing.

Respectfully submitted,

/s/ Owen E. MacBride
Owen E. MacBride

Attorney for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
Before the
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)** **)** **)**	**Docket No. RR14-__-000**

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION'S REPORT OF COMPARISONS OF BUDGETED TO ACTUAL COSTS FOR 2013 FOR NERC AND THE REGIONAL ENTITIES

Gerald W. Cauley
President and Chief Executive Officer
Michael Walker
Senior Vice President and Chief Financial and Administrative Officer
North American Electric Reliability Corporation
3353 Peachtree Road
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-9765 – facsimile

Owen E. MacBride
Schiff Hardin LLP
233 South Wacker Drive, Suite 6600
Chicago, IL 60606
(312) 258-5680
(312) 258-5700 – facsimile
omacbride@schiffhardin.com

Charles A. Berardesco
Senior Vice President and General Counsel
Rebecca J. Michael
Associate General Counsel for Regulatory and Corporate Matters
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
rebecca.michael@nerc.net

May 30, 2014

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	NOTICES AND COMMUNICATIONS	2
III.	COMPARISONS OF ACTUAL COSTS TO BUDGETS FOR THE YEAR ENDED DECEMBER 31, 2013	3
IV.	METRICS CONCERNING ADMINISTRATIVE COSTS IN 2013 NERC AND REGIONAL ENTITY BUDGETS AND ACTUAL COSTS	10
V.	CONCLUSION	19

ATTACHMENTS:

Attachment 1: North American Electric Reliability Corporation – 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements

Attachment 2: Florida Reliability Coordinating Council, Inc. – 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements

Attachment 3: Midwest Reliability Organization – 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements

Attachment 4: Northeast Power Coordinating Council, Inc. – 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements

Attachment 5: ReliabilityFirst Corporation – 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements

Attachment 6: SERC Reliability Corporation – 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements

Attachment 7: Southwest Power Pool Regional Entity – 2013 Actual Cost-to-Budget Comparison; Audited Financial Statements of Southwest Power Pool, Inc.

Attachment 8: Texas Reliability Entity, Inc. – 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements

Attachment 9: Western Electricity Coordinating Council – 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements

Attachment 10: Metrics Concerning Administrative Costs in 2013 NERC and Regional Entity Budgets and Actual Costs

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") respectfully submits this filing to provide comparisons of actual to budgeted costs for the year 2013 for NERC and the eight Regional Entities.[1] The Commission originally directed NERC to file, each year, comparisons of actual to budgeted costs for the preceding year, in an order issued October 18, 2007 concerning the 2008 business plans and budgets of NERC and the Regional Entities.[2] As described in §III below, in several subsequent orders, the Commission has clarified and expanded upon the information to be included in the annual actual-to-budget cost comparisons.

The following information is provided in this filing:

- A comparison of the actual funding received and costs incurred by NERC and each Regional Entity for statutory and (where applicable) non-statutory activities for the year ended December 31, 2013, to the budgets of NERC and each Regional Entity for that year, with explanations of significant actual cost-to-budget variances.
- Audited financial statements of NERC and each Regional Entity for the year ended December 31, 2013.
- Metrics concerning NERC and Regional Entity administrative costs in their 2013 budgets and actual results.[3]

This filing includes the following attachments:

Attachment 1: 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements for NERC.

---

[1] The eight Regional Entities are the Florida Reliability Coordinating Council, Inc. ("FRCC"), Midwest Reliability Organization ("MRO"), Northeast Power Coordinating Council, Inc. ("NPCC"), ReliabilityFirst Corporation ("ReliabilityFirst"), SERC Reliability Corporation ("SERC"), Southwest Power Pool, Inc. Regional Entity ("SPP RE"), Texas Reliability Entity, Inc. ("Texas RE"), and Western Electricity Coordinating Council ("WECC").

[2] *North American Electric Reliability Corporation, Order Conditionally Accepting 2008 Business Plan and Budget of the North American Electric Reliability Corporation and Ordering Compliance Filings*, 121 FERC ¶ 61,057 (2007) ("*2008 ERO Budget Order*").

[3] The metrics information is provided in response to P 39 of the Commission's Order issued June 19, 2008. *North American Electric Reliability Corporation, Order Conditionally Accepting Compliance Filing*, 123 FERC ¶61,282 (2008) ("*June 19, 2008 Budget Compliance Order*").

Attachment 2: 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements for FRCC.

Attachment 3: 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements for MRO.

Attachment 4: 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements for NPCC.

Attachment 5: 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements for ReliabilityFirst.

Attachment 6: 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements for SERC.

Attachment 7: 2013 Actual Cost-to-Budget Comparison for SPP RE and 2012 Audited Financial Statements for Southwest Power Pool, Inc.

Attachment 8: 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements for Texas RE.

Attachment 9: 2013 Actual Cost-to-Budget Comparison and Audited Financial Statements for WECC.

Attachment 10: Metrics Concerning Administrative Costs in 2013 NERC and Regional Entity Budgets and Actual Costs

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to:

Gerald W. Cauley
President and Chief Executive Officer
Michael Walker
Senior Vice President and Chief Financial
and Administrative Officer
North American Electric Reliability Corporation
3353 Peachtree Road
North Tower, Suite 600
Atlanta, GA 30326
(404) 446-2560
(404) 446-9765 – facsimile

*Owen E. MacBride
Schiff Hardin LLP
233 South Wacker Drive, Suite 6600
Chicago, IL 60606
(312) 258-5680
(312) 258-5700 – facsimile
omacbride@schiffhardin.com

*Charles A. Berardesco
Senior Vice President and General Counsel
*Rebecca J. Michael, Associate General Counsel
for Regulatory and Corporate Matters
North American Electric Reliability
Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
rebecca.michael@nerc.net

*Persons to be included on the Commission's official service list. NERC requests waiver of the limitation to two persons on the service list in order to include a third person.

III. COMPARISONS OF ACTUAL COSTS TO BUDGETS FOR THE YEAR ENDED DECEMBER 31, 2013

As noted above, in the *2008 ERO Budget Order*, the Commission directed NERC to make annual filings comparing the NERC and Regional Entity budgets to actual costs incurred in the preceding year, "in sufficient detail and with sufficient explanations for the Commission to determine, by program area, the reasons for deviations from the budget and the impacts of those deviations."[4] In the *June 19, 2008 Budget Compliance Order*, which addressed NERC's April 1, 2008 compliance filing to the *2008 ERO Budget Order*, the Commission provided additional direction concerning the presentation of the annual filings comparing NERC's and the Regional Entities' actual to budgeted expenditures:

> 37. To promote consistency and transparency, the Commission directs the use of certain practices and formats in future true-up filings. In particular, Regional Entities must provide a cover letter discussing major areas of actual cost-to-budget variances for all of the Regional Entity's statutory programs in the aggregate. Regional Entities should also follow NERC's template for the presentation of actual costs and budgeted costs on a program-by-program and line-item basis. Significant variances must be explained on a line-item basis with enough particularized information to clearly support each such variance. Regional Entities should refrain from using generic, program area summaries to support significant variances. The cause for each such variance should therefore be clear on its face. Further, each Regional Entity must provide an explanation of the allocation methods it used to allocate indirect costs to the direct statutory program or functional areas, as well as any allocation between any statutory and non-statutory activities.
>
> 38. Cash reserves are meant to handle expenses which exceed the amount budgeted, as well as unforeseen events that could occur at any time. However, in the future, the Commission expects NERC and the Regional Entities to justify the use of cash reserves as variances in the April true-up. Cash reserves should not become a means to fund expected projects outside of the budget approval process. The Commission expects that as NERC and the Regional Entities develop experience in planning and functioning under their budgets the amounts and number of variance will decrease. In addition, the Commission expects that with experience, the explanations for the variances will improve.

In addition, although the following directive in the *2008 ERO Budget Order* was

[4] *2008 ERO Budget Order* at P 23.

expressly applicable to NERC's compliance filing comparing actual expenses to budgets for the year ended December 31, 2007 for NERC and the Regional Entities, NERC has treated the directive as intended to apply to the annual filings comparing actual expenses to budgets for future years as well:

> 66. . . . [T]he Commission reminds NERC and the Regional Entities that, to the extent funding identified as statutory is used to fund non-statutory activities, those funds must be reimbursed (e.g., to load serving entities or to statutory expenditures). NERC is directed to inform the Commission in the . . . compliance filing the extent to which this has occurred and document that the funds have been or will be reimbursed.

The comparisons of 2012 actual-to-budget funding and expenditures for NERC and the Regional Entities are provided in **Attachments 1 through 9**, as follows:

- **Attachment 1:** NERC
- **Attachment 2:** FRCC
- **Attachment 3:** MRO
- **Attachment 4:** NPCC
- **Attachment 5:** ReliabilityFirst
- **Attachment 6:** SERC
- **Attachment 7:** SPP RE
- **Attachment 8:** Texas RE
- **Attachment 9:** WECC

Each Attachment also includes the respective entity's audited financial report for the year ended December 31, 2013, as prepared by its independent public accounting firm.

The comparisons provided in **Attachments 1** through **9** conform to the Commission's directives as quoted above:

- Each comparison contains a cover letter identifying overall actual-to-budget variances in Funding and total Expenses and in major Expense categories, and discussing reasons for major areas of actual cost-to-budget variances.
- Each comparison contains a summary table, prepared using a NERC-supplied template, showing the entity's 2013 budget, 2013 actual amounts, and the variance,

for major line-item categories of Funding and Expenses.

- For those entities that engaged in both statutory and non-statutory activities in 2013, the comparisons include separate summary tables for statutory programs and non-statutory activities, prepared using the NERC-supplied template, showing the entity's 2013 budget, 2013 actual amounts, and the variance, for major line-item categories of Funding and Expenses.[5]
- The comparisons include individual tables, also prepared using a NERC-supplied template, showing 2013 budget, 2013 actual amounts, and the variance, for major line-item categories of Funding and Expenses, for each of the statutory programs[6] (direct costs) and the overhead functions[7] (indirect costs). These tables also provide explanations for significant line-item actual-to-budget variances.[8]

The Attachments also address (generally in the cover letter) (i) where applicable, whether any statutory funds were used in 2013 for non-statutory activities (neither NERC nor any Regional Entity reports using statutory funds for non-statutory activities during 2013); (ii) the impact of the entity's 2013 results on its working cash reserve for statutory programs (*e.g.*, whether working cash reserves were used to fund expenditures during 2013)[9]; (iii) how indirect

[5] FRCC, NPCC, Texas RE and WECC had non-statutory activities in 2013 and each has provided summary tables for statutory and non-statutory activities. NERC, MRO, ReliabilityFirst, SERC and SPP RE did not have non-statutory activities in 2013 (although SPP RE's parent organization, Southwest Power Pool, Inc. had non-statutory activities).

[6] Reliability Standards, Compliance Operations, Enforcement and Organization Registration, Reliability Assessment and Performance Analysis, Training, Education and Operator Certification, and Situation Awareness and Infrastructure Security (including Critical Infrastructure Protection). NERC and SERC have each provided separate tables for (i) Compliance Operations and Organization Registration and (ii) Compliance Enforcement. In addition, NERC has also provided separate tables for Event Analysis and Investigations and for Critical Infrastructure Protection and ES-ISAC (Electricity Sector Information Sharing and Analysis Center).

[7] Committees and Member Forums, General and Administrative, Legal and Regulatory, Information Technology, Human Resources, and Accounting and Finance. Some of the Regional Entities report budget and actual expenditure information for some or all of the overhead functions on a combined basis, in order to protect the confidentiality of compensation information for departments that have a limited number of staff members.

[8] Generally, explanations have been provided for line-item variances that are greater than +/- 10% of the budgeted amount and greater than $10,000 over or under the budgeted amount.

[9] The summary comparison tables for total entity and (where applicable) statutory and non-statutory activities show the "Change in Working Capital" (or in "Operating Reserves") for the 2013 Actual Funding and Expenditures. A positive "Change in Working Capital" means the entity's total Actual Funding exceeded its total Actual Expenditures for the year 2013; therefore, it was not necessary for the entity to use a portion of its cash reserves balance at December 31, 2012 to fund 2013 expenditures.

costs were allocated to the direct statutory programs or functions; and (iv) where applicable, whether, and if so how, costs were allocated between statutory programs and non-statutory activities in 2013.

As it did in its actual cost-to-budget comparisons filed with the Commission for 2011 and 2012,[10] NERC has provided additional information in its 2013 report in **Attachment 1** on (1) actual cost to budget variances for Consultants and Contracts expense, and (2) a detailed analysis and comparison of the major sources of changes in its working capital and operating reserves for 2013, as budgeted and per actual results. The analysis of working capital and operating reserves includes a breakdown of the changes in working capital and operating reserves due to 2013 budgeted operations and to differences in actual funding or expenditures from amounts budgeted, including unbudgeted or above-budget expenditures funded from the Known Contingency Reserve or the Unknown Contingency Reserve. This additional information is also responsive to recommendations adopted in the approved Settlement Agreement for the Commission's financial performance audit of NERC.[11] The table on page 4 of **Attachment 1** shows the actual cost to budget variances for Consultants and Contracts expense for 2013 by NERC program area, and is followed by a detailed narrative discussion of the reasons for actual cost-to-budget variances for Consultants and Contracts expense in each program area (pages 4-5). The analysis of changes in working capital and operating reserves is provided on pages 8-9 of **Attachment 1**, including the

[10] *See* Attachment 1 to *North American Electric Reliability Corporation's Report of Comparisons of Budgeted to Actual Costs for 2011 for NERC and the Regional Entities*, filed May 30, 2012 in Docket No. RR12-11-000 ("*2011 True-Up Filing*"); and Attachment 1 to *North American Electric Reliability Corporation's Report of Comparisons of Budgeted to Actual Costs for 2012 for NERC and the Regional Entities*, filed May 30, 2013 in Docket No. RR13-6-000 ("*2012 True-Up Filing*")

[11] *See North American Electric Reliability Corporation, Order Approving Settlement Agreement*, 142 FERC ¶ 61,054 (2013), Attachment (Settlement Agreement) at §II(8)(a), specifying that NERC will "[i]ncrease the granularity of the NERC budget filings by identifying proposed budgeted expenditures, at a minimum, by the major activities to be undertaken by each program area" (Audit Staff Recommendation 4). NERC also agreed with Audit Staff Recommendation 5 to "[i]ncrease the granularity of the NERC true-up filings in line with the budget filings."

table on page 9 which shows the major sources of generation and additions to operating reserves in 2013 and the major expenditures of operating reserves in 2013.

In addition, in its 2013 report, NERC has also provided (1) details relating to Miscellaneous Expense, reporting actual expenses for employee rewards and recognition, community responsibility activities and charitable contributions (*see* page 6 of **Attachment 1**); and (2) an actual cost-to budget comparison of 2013 Board of Trustees expenses, detailed by Meetings and Travel Expense (Quarterly Board Meetings and Trustee Travel expense) and Professional Services (Independent Trustee Fees and Trustee Search Fees). The information relating to Board of Trustees expenses is provided on page 7 of **Attachment 1**.

Because the NERC and Regional Entity reports in each Attachment identify and discuss major areas of actual-to-budget variances, and the individual tables for each direct statutory program and each indirect cost function contain specific explanations of significant variances on a line-item basis, a detailed, entity-by-entity discussion of the actual-to-budget variances experienced in 2013 by NERC and individual Regional Entities is not provided here. However, the list below describes several recurring drivers of actual-to-budget variances experienced by NERC and the Regional Entities in 2013, as identified by NERC's review of the comparisons.

- A number of entities[12] experienced under-budget variances in Salary Expense and related Personnel Expenses (Payroll Taxes, Employee Benefits and Savings & Retirement), in one or more program areas, due to being unable to fill budgeted positions, due to filling budgeted positions later in the year than was assumed in the budget, or due to employees in existing positions leaving the entity, resulting in a vacant position for a portion of the year. Additionally, having fewer personnel on staff than budgeted tended to reduce Meetings and/or Travel Expense below the budgeted amounts.[13]

[12] The term "entities" is used in this discussion to include NERC as well as Regional Entities.

[13] In the development of their annual budgets, NERC and some of the Regional Entities have begun to address this "vacant position" variance issue by including an "attrition factor" or "labor float factor" into their budget calculations. The attrition factor recognizes that, as in any organization, a portion of the

- In some instances, due to the difficulty in filling budgeted positions, the entity may have found it necessary (i) to pay higher compensation than budgeted to fill a new or vacant position, and/or (ii) to incur costs for temporary staffing services while budgeted positions were vacant.
- In order to address unfilled positions or emergent needs in particular program areas, some entities transferred one or more employees from one program area to another during 2013, or had shared FTEs who spent a greater portion of their time working in one program area and a lesser portion of time in another program area than was reflected in the budget. This resulted in actual cost-to-budget variances in Personnel Expenses and related Meeting and Travel expenses for the program areas involved in such transfers, although not necessarily for the entity as a whole.
- The inability to fill budgeted positions as planned, or the departure of existing employees, also resulted in some instances in higher-than budgeted Consultants & Contracts expense, due to either or both the need to use consultants or contractors to perform work that would have been done by employees, or the need to make greater use than budgeted of personnel recruiting services and search firms.
- Generally, NERC and the Regional Entities allocate Indirect Expenses to the direct statutory programs on the basis of numbers of FTEs in each statutory program. Therefore, due to differences in actual versus budgeted FTEs during the year in individual statutory programs, some entities experienced variances from budget in the amounts of Indirect Expenses allocated to the individual direct statutory programs.
- Some entities experienced higher or lower Employee Benefits expenses than budgeted due to actual renewal rates from services providers for their health and medical benefits programs being different than projected at the time of budget preparation.
- Some entities experienced lower than budgeted Employee Benefits expenses due to decisions by employees not to participate in the entity's medical benefits program. In some cases employees elected to stay on the health and medical programs of previous employers or of their spouse's employer.
- Some entities experienced either higher or lower costs than budgeted for Retirement costs due to greater or lesser participation by employees in the entity's retirement plan than was assumed in the budget.
- A number of entities realized lower than budgeted actual costs for Meetings and Travel due to (i) continuing efforts to make greater use of teleconferencing, Webinars and other virtual meeting capabilities rather than in-person meetings; (ii) holding several meetings in the same hotel or other outside facility, thereby obtaining lower charges; and/or (ii) scheduling meetings at NERC or Regional Entity facilities or the facilities of stakeholders (*e.g.* at the offices of Regional Entity members) rather than in rented, third-party meeting spaces.

---

budgeted positions will be vacant during a part of the year due to delays in filling new or vacant positions and unexpected/unbudgeted departures of existing employees.

- In particular with respect to Meetings and Travel expense, several entities which moved to new offices with larger meeting spaces, or expanded existing offices, in 2013 or in recent prior years have been able to reduce Meetings and Travel expense by holding more meetings in the entity's office rather than in outside facilities.
- Some entities incurred lower than budgeted costs for Conference Calls due to entering into a new contract for teleconferencing services with the existing provider, or entering into a contract with a new provider of these services, at lower costs, during the course of the year.
- Several entities were able to spend less on Consultants and Contracts and/or Professional Services than budgeted, as a result of having work budgeted to be performed by contractors and consultants handled by internal staff of the entity. As some entities have increased their staffing over time, they have seen less need to use outside services, due to increased in-house staff capabilities.
- Some entities experienced lower than budgeted Consultants and Contracts expense due to timing delays or deferrals in planned projects.
- Some entities experienced variances in Office Rent or Office Costs due to new or changed office lease terms (including as a result of moving to a new office or taking additional space in the existing office facility), or due to implementing changes in the manner in which the entity accounted for Office Rent or Office Costs, as compared to the terms or accounting reflected in the budget.
- In addition, some entities which moved to new offices or expanded existing offices to accommodate increased staffing, incurred additional costs for capital expenditures (Furniture & Fixtures CapEx, Equipment CapEx, Computer & Software CapEx, and/or Leasehold Improvements) associated with the move to the new office or expansion of the existing office.
- Some actual cost-to-budget variances within program areas are due to the entity budgeting certain costs entirely in one program area but then recording the actual costs in the program area responsible for incurring the cost (*e.g.*, budgeting all outside legal services in Legal and Regulatory but recording actual outside legal expenses in the program area(s) whose activities necessitate the services).
- Some entities budget Professional Services expense for one or two contested compliance hearing per year (*e.g.*, for outside counsel to handle the hearing or for hearing officer services); if no contested hearings occur during the year, an under-budget variance in Professional Services expenses results.
- For some entities, Information Technology projects or Fixed Asset purchases (*e.g.*, office furniture purchases) that were included in the 2013 budget were either (i) completed, or at least initiated, in late 2012, (ii) not carried out in 2013 (*i.e.*, delayed/deferred to 2014), or (iii) initiated later in 2013 than assumed in the budget and therefore not completed in 2013. This resulted in reduced actual IT costs, Capital Expenditures, and/or Consultants and Contracts expense (where the project was to require the use of consulting services or outside contracts). In other cases, projects that were planned and budgeted for execution and completion in 2012 were not fully

completed in 2012 or were delayed or deferred into 2013, resulting in unbudgeted expenditures in 2013.

- Some entities budgeted certain expenditures as expenses (*e.g.*, as Office Costs), but then determined that the expenditure(s) needed to be capitalized (*i.e.*, recorded as Fixed Asset additions, such as Computer & Software Capital Expenditures or Equipment Capital Expenditures) based on the entity's capitalization policy. The determination to capitalize rather than expense these expenditures also resulted in additional Depreciation expense.
- Some entities experienced higher or lower Funding from Workshop attendance fees, or other programs conducted for industry participants, due to higher or lower attendance at workshops or other programs than projected in the budget, holding more or fewer Workshops than assumed in the budget, making a determination not to charge fees (or charging lower fees) for some programs for which fees had been budgeted, or a combination of these factors.

In addition to the above-described causes of actual-to-budget variances that were experienced by more than one entity, NERC and the Regional Entities experienced other above- or below-budget variances in actual Funding, Expenses and Fixed Asset Additions in individual line items due to particular events and circumstances impacting the particular entity. These variances are identified in the individual actual cost-to-budget comparisons presented in **Attachments 1** through **9**.

NERC and the Regional Entities are taking the actual cost-to-budget comparisons for 2013, as well as year-to-date actual cost-to-budget comparisons for 2014, into account in developing their business plans and budgets for 2015, which are to be submitted to the NERC Board for approval, and then filed with the Commission for approval, in August 2014. In addition, the Regional Entities' working capital and operating reserve policies are being reviewed as part of the 2015 business plan and budget review process.

IV. METRICS CONCERNING ADMINISTRATIVE COSTS IN 2014 NERC AND REGIONAL ENTITY BUDGETS AND ACTUAL COSTS

In the *June 19, 2008 Budget Compliance Order*, the Commission directed NERC to develop additional metrics analyzing its administrative expenses and those of the Regional

Entities, and to present these metrics in future annual actual cost-to-budget filings and Business Plan and Budget filings:

> 39. Our analysis of the Regional Entities' true-up statements indicates that many Regional Entities spent a significant percentage of their 2007 budgets on various administrative functions to support their statutory functions.[13] The amounts spent on administrative functions vary widely among the Regional Entities. . . We recognize that 2007 is the first year that these Regional Entities have prepared a budget for statutory functions and that there are some startup costs that will be unique to 2007. The Commission anticipates, however, that such effects will diminish as NERC and the Regional Entities gain experience preparing their budgets. To promote better transparency, the Commission directs NERC to develop additional metrics to identify, in a uniform manner, information detailing its total expenses for administrative functions as well as the expenses for administrative functions for each Regional Entity. For example, one of the matrices should be the percentage spent by the Regional Entity on administrative functions as a portion of its total approved budgeted funding similar to the information provided in the table attached to this order. These new metrics should be designed to enhance the Commission's ability to compare information provided by the Regional Entities on administrative costs and to understand the reasons for any significant differences in amounts budgeted by different Regional Entities for the same function. The Commission therefore directs NERC to develop these additional metrics for use in the true-up filings for NERC's 2008 and 2009 budgets and for use in NERC's subsequent business plans and budgets beginning with NERC's 2010 Business Plan and Budget.
>
> [13] The Commission considered the amount each Regional Entity spent on administrative functions as a percentage of its total budgeted funding. The administrative functions included in staff's analysis are: Committees and Member Forums, General and Administration, Legal and Regulatory, Information Technology, Human Resources, and Accounting and Finance. A table of administrative expenses spent by each Regional Entity as a percentage of its budgeted funding is included as Attachment A to this order.

The administrative functions cited in footnote 13 of the *June 19, 2008 Budget Compliance Order* (Committees and Member Forums, General and Administration, Legal and Regulatory, Information Technology, Human Resources and Accounting and Finance) are the functions that NERC and the Regional Entities refer to as "indirect costs" in their business plans and budgets and reports of actual expenses. It is appropriate to analyze these indirect costs in the aggregate (as the Commission did in P 39 and footnote 13 of the *June 19, 2008 Budget Compliance Order*),

rather than by individual function, due to certain necessary inconsistencies among the Regional Entities in budgeting and recording these costs. For example, as noted earlier, some of the Regional Entities budget and record all Salary expense for Legal and Regulatory, Human Resources and/or Accounting and Finance under General and Administrative, because they have only one or two employees in each of these functions, and therefore reporting the budgeted and actual Salary expense for these individual functional categories could reveal salary information of individual employees.[14] As stated earlier, the actual cost-to-budget comparisons for 2013, as well as year-to-date actual cost-to-budget comparisons for 2014, are being taken into account in developing the NERC and Regional Entity business plans and budgets for 2015.

Attachment 10 provides the following three sets of metrics comparisons for NERC and the Regional Entities for their 2013 budgets and 2013 actual costs. In addition, **Attachment 10** provides a comparison of these metrics values for 2011, 2012 and 2013 actual results.

- Statutory indirect expenditures as a percent of total statutory expenditures,[15] and statutory direct expenditures per dollar of statutory indirect expenditures (top row of tables on **Attachment 10**).[16]
- Statutory indirect full-time equivalent employees ("FTE") as a percent of total statutory FTE, and ratio of statutory direct FTE to statutory indirect FTE (middle row of tables on **Attachment 10**).
- Total statutory expenditures per total FTE, statutory direct expenditures per direct FTE, statutory indirect expenditures per indirect FTE, and statutory indirect expenditures per total FTE (bottom row of tables on **Attachment 10**).

These are the same metrics that NERC provided in its previous annual filings comparing

[14] In addition, in some instances NERC or a Regional Entity has budgeted all of its projected costs for indirect functions such as General and Administrative, Legal and Regulatory or Information Technology in the indirect program, but has recorded some or all of the actual costs incurred for the function in the statutory program in which work was performed (*e.g.*, recording Professional Services expenses budgeted in Legal and Regulatory in the direct program for which outside legal services were performed).

[15] This is the metric shown in Attachment A to the *June 19, 2008 Budget Compliance Order*.

[16] The term "expenditures" is used in this discussion to mean expenses plus capital expenditures (fixed asset additions net of depreciation).

actual-to-budget costs for NERC and the Regional Entities for 2008, 2009, 2010, 2011 and 2012.[17] In the *June 29, 2009 Budget Compliance Order*, the Commission indicated that these metrics were acceptable.[18]

In reviewing indirect expenditures, it is important to take into consideration that NERC's indirect expenses support more than NERC's internal operations. NERC's indirect expenditures also include support of software applications that interface with Regional Entities. Costs for outside audit resources in connection with Regional Entity oversight, as well as Compliance and Certification Committee oversight of NERC's compliance with its Rules of Procedure, are also included in indirect expenses. In addition, expenses incurred in NERC's legal and executive (General and Administrative) operations, as well as those of the Regional Entities, directly support the activities of the standards, compliance and enforcement, and other statutory program areas. NERC's legal department, as well as those of the Regional Entities, devotes considerable resources to supporting standards development, compliance enforcement and registration matters.

The following subsections provide discussion and analysis of the metrics provided in **Attachment 10**.

Statutory indirect expenditures as a percent of total statutory expenditures, and statutory direct expenditures per dollar of statutory indirect expenditures

The data and metrics in the top row of tables on **Attachment 10** measure the portions of

[17] *Additional Compliance Filing of the North American Electric Reliability Corporation in Response to October 18, 2007 Order – Comparisons of Budgeted to Actual Costs for 2008 for NERC and the Regional Entities*, filed April 1, 2009 in Docket No. RR07-16-005; *North American Electric Reliability Corporation's Report of Comparisons of Budgeted to Actual Costs for 2009 for NERC and the Regional Entities*, filed June 1, 2010 in Docket No. RR08-6-000; *North American Electric Reliability Corporation's Report of Comparisons of Budgeted to Actual Costs for 2010 for NERC and the Regional Entities*, filed May 31, 2011 in Docket No. RR11-4-000; *2011 True-Up Filing; 2012 True-Up Filing.*

[18] *North American Electric Reliability Corporation, Order Conditionally Accepting Compliance Filing*, 127 FERC ¶ 61,307 (2009) ("*June 29, 2009 Budget Compliance Order*"), at PP 13-14.

the total statutory expenditures of NERC and each Regional Entity, and the Electric Reliability Organization ("ERO") in the aggregate, that are being expended on statutory direct functions and on statutory indirect functions. Based on 2013 actual data, statutory indirect expenditures averaged 33.61% of total statutory expenditures for NERC and the Regional Entities, and the average statutory direct expenditure per dollar of statutory indirect expenditure was $1.98.[19] The actual average statutory indirect expenditure percentage was almost equal, and the actual average statutory direct expenditure per dollar of indirect expenditure was equal, to the averages based on the NERC and Regional Entity budgets (33.51% and 1.98, respectively). Further, the 2011 and 2012 actual results are not significantly different from the 2013 actual results for these metrics. The 2013 actual average statutory indirect expenditure percentage was 33.61% while the 2011 and 2012 actual average statutory indirect expenditure percentages were 31.06% and 30.35%, respectively. The three-year average for this metric for 2011, 2012 and 2013 combined was 31.72%. The 2013 actual average statutory direct expenditure per dollar of indirect expenditure was $1.98 while the 2011 and 2012 statutory direct expenditure per dollar of statutory indirect expenditure was $2.22 and $2.29, respectively. The three-year average for 2011, 2012 and 2013 combined for this metric was $2.15.

Looking at the 2013 values of these metrics for the individual entities compared to the 2013 averages, the percentages of actual statutory indirect expenditures to total statutory expenditures for NERC and SPP RE were noticeably higher than the overall weighted and

[19] These figures are essentially weighted averages, *i.e.*, they are calculated using the sums of the total statutory expenditures, total statutory direct expenditures, and total statutory indirect expenditures, for NERC and the eight Regional Entities. Since NERC's and WECC's expenditures are substantially larger than those of the other Regional Entities, the NERC and WECC results significantly influence the weighted averages. (The significance of the WECC data to the averages is further magnified due to the amount of U.S. Department of Energy grant funds and related expenditures included in WECC's 2013 budget and actual results.) The arithmetic averages for these two metrics are 34.53% for statutory indirect expenditures as a percent of total statutory expenditures, and $2.57 for statutory direct expenditures per dollar of statutory indirect expenditures.

arithmetic averages, and their 2013 ratios of actual statutory direct expenditures to statutory indirect expenditures were noticeably lower than the overall weighted and arithmetic averages.

For NERC, its total actual direct statutory expenditures were approximately $337,600 less than budgeted while its total statutory indirect expenditures exceeded budget by approximately $766,300, resulting in its percentage of statutory indirect expenditures to total statutory expenditures rising from 43.06% in its budget to 44.13% actual. NERC's lower-than budgeted direct statutory expenditures was primarily due to: (1) lower than budgeted Personnel Expenses, which were collectively under budget $581,200, due to unfilled positions in the Compliance Enforcement, Situation Awareness and Training, Education, and Operator Certification departments; (2) lower than budgeted Meetings, Travel and Conferencing expenses, which were collectively $620,600 under budget, due primarily to management initiatives to lower these expenses; and (3) higher than budgeted Fixed Asset expenditures due to the capitalization (rather than expensing) of the Enterprise Bulk Electric System Exceptions application and the standards balloting software application.

SPP RE's actual 2013 indirect expense amount was in fact lower than budgeted (by approximately $337,500, or about 6%), but SPP RE's 2012 statutory direct expenditures were also lower than budgeted (by approximately $1,500,000, or about 25%), with the result that SPP RE's percentage of statutory indirect expenditures to total statutory expenditures increased from 47.33% as budgeted to 52.81% actual, and its ratio of statutory direct expenditures to statutory indirect expenditures fell from $1.11 as budgeted to $0.89 actual. In other words, the principal reason for SPP RE's actual percentage of statutory indirect expenditures to total statutory expenditures being higher than budgeted for 2013 was that SPP RE's actual direct statutory

expenditures were much lower than budgeted, not that its actual indirect expenses were higher than budgeted.

As shown by the data provided on the second page of **Attachment 10**, comparisons of the actual 2013 results for this first set of metrics to the actual results for 2012 and 2011 for these metrics show that, over this three-year period, NERC and the Regional Entities, in the aggregate, spent about the same portion of their total statutory expenditures on statutory indirect costs. Further, with only limited exceptions, each entity's annual values for these metrics were fairly consistent over the three-year period. This three-year view indicates that as their organizations and programs mature, with seven years of ERO and delegated function activities, each entity is reaching a steady state in terms of the portions of its total resources that are expended on statutory direct program costs and statutory indirect costs.

Statutory indirect FTE as a percent of total statutory FTE, and ratio of statutory direct FTE to statutory indirect FTE

On average for NERC and the Regional Entities, 2013 actual statutory indirect FTEs were 24.28% of total statutory FTEs, and on average NERC and the Regional Entities had 3.12 statutory direct FTEs per statutory indirect FTE in 2013. The 2013 actual value for statutory indirect FTEs as a percent of total statutory FTEs was slightly lower than the 2012 value for this metric of 24.65% and slightly higher than the 2011 value for this metric of 23.42%; while the 2013 actual value for the number of statutory direct FTEs per statutory indirect FTE was slightly higher than the 2012 value for this metric of 3.06, and lower than the 2011 value for this metric of 3.27. Overall, however, the annual averages for this metric were fairly consistent across the three-year period 2011-2013.

In 2013, the actual percentage of statutory indirect FTEs to statutory total FTEs was less than 25% for each entity in the ERO except NERC (for which the percentage was 30.84%) and

SERC (26.94%); and NERC and each Regional Entity had at least 2.24 statutory direct FTE per statutory indirect FTE. Among the Regional Entities, FRCC, MRO, Texas RE and WECC each had a lower actual percentage of statutory indirect FTEs to statutory total FTEs in 2013 than in 2012 and 2011. NPCC and SERC each experienced higher actual percentages of statutory indirect FTEs to statutory total FTEs in 2013 than in 2012 and 2011. NERC's actual percentage of statutory indirect FTEs to statutory total FTEs in 2013 was approximately equal to its value for this metric in 2012 and was somewhat higher than its value for this metric in 2011. ReliabilityFirst's actual percentage of statutory indirect FTEs to statutory total FTEs in 2013 was lower than its value for this metric in 2012 and higher than its value for this metric in 2011.

Similarly, FRCC, MRO, Texas RE and WECC each had a higher actual ratio of statutory direct FTEs per statutory indirect FTE in 2013 than in 2012 and 2011, while NPCC and SERC each had lower actual ratios of statutory direct FTEs per statutory indirect FTE in 2013 than in 2012 and 2011. NERC's actual ratio of statutory direct FTEs per statutory indirect FTE in 2013 was equal to its 2012 value, and lower than its 2011 value, for this metric. ReliabilityFirst's actual ratio of statutory direct FTEs per statutory indirect FTE in 2013 was higher than its value for this metric in 2012 and lower than its value for this metric in 2011.

The three-year average percentage of actual statutory indirect FTEs to total statutory FTEs was 24.14%. The three-year average actual ratio of statutory direct FTEs per statutory indirect FTE was 3.14. As noted above in the discussion of the first set of metrics, comparisons of the actual 2013 results for this second set of metrics to the actual results for 2012 and 2011 for these metrics show that, over this three-year period, NERC and the Regional Entities, in the aggregate, had about the same percentage of indirect FTEs to total statutory FTEs and about the same ratio of statutory direct FTEs per statutory indirect FTEs for each of the three years (*i.e.*,

the highest annual average value for each metric was within 7% or less of the lowest annual average value for the metric).

Total statutory expenditures per total FTE, statutory direct expenditures per direct FTE, statutory indirect expenditures per indirect FTE, and statutory indirect expenditures per total FTE

The bottom row of metrics in the tables in **Attachment 10** shows the (i) total statutory expenditures per total FTE (total statutory expenditures divided by total number of statutory FTE), (ii) statutory direct expenditures per direct FTE, (iii) statutory indirect expenditures per indirect FTE, and (iv) statutory indirect expenditures per total FTE (statutory indirect expenditures divided by total number of FTE), for NERC and each Regional Entity. For NERC and the eight Regional Entities, in the aggregate:

- The actual average total statutory expenditures per statutory FTE were approximately 7.6% higher than budgeted ($273,210 actual versus $253,971 budgeted).
- The actual average statutory direct expenditures per statutory direct FTE were also approximately 7.6% higher than budgeted ($239,565 actual versus $222,630 budgeted).
- The actual average statutory indirect expenditures per statutory indirect FTE were 7.3% higher than budgeted ($378,131 actual verses $352,402 budgeted).
- The actual average statutory indirect expenditures per total statutory FTE were higher than budgeted by 7.9% ($91,815 actual versus $85,109).

Overall, for NERC and the Regional Entities in the aggregate, the actual 2013 value for each of the first three metrics was lower than the actual values for 2012 and 2011, with only one exception:

- The actual average total statutory expenditures per statutory FTE were $273,210 in 2013, as compared to $278,306 in 2012 and as compared to $291,503 in 2011. The three-year average value for this metric was $281,007.
- The actual average statutory direct expenditures per statutory direct FTE were $239,565 in 2013 as compared to $257,242 in 2012 and as compared to $262,409 in 2011. The three-year average value for this metric was $253,072.

- The actual average statutory indirect expenditures per statutory indirect FTE were $378,131 in 2013 as compared to $342,707 in 2012 and as compared to $386,650 in 2011. The three-year average value for this metric was $369,163.

This latter comparison shows that from 2011 to 2013, the ERO's FTE staffing (both direct function and indirect function personnel) grew faster than statutory expenditures grew, indicating an increase in the efficiency of use of the ERO's personnel.

A final, overall observation on the entire set of metrics data presented in **Attachment 10** (similar to the observation stated earlier based on the first set of metrics), is that, after seven years of ERO operations, as their organizations and programs mature, with only limited exceptions, each of the nine entities appears to be reaching a steady state in terms of the portions of its total statutory expenditures and personnel resources that are being devoted to statutory direct program activities and to statutory indirect activities. While some differences remain in the individual metrics values among the entities, these differences (*i.e.* each entity's metrics values) can be seen as becoming ingrained in their organizational and program structures.

V. CONCLUSION

The North American Electric Reliability Corporation respectfully requests that the Commission accept this filing and Attachments as compliant with the Commission's requirements for annual presentation of comparisons of actual-to-budgeted funding and costs for NERC and the Regional Entities for the year ended December 31, 2013.

Respectfully submitted,

Gerry W. Cauley
President and Chief Executive Officer
Michael Walker
Senior Vice President and Chief Financial and Administrative Officer
North American Electric Reliability Corporation
3353 Peachtree Road
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-9765 – facsimile

/s/ Owen E. MacBride
Owen E. MacBride
Schiff Hardin LLP
233 South Wacker Drive, Suite 6600
Chicago, IL 60606
(312) 258-5680
(312) 258-5700 – facsimile
omacbride@schiffhardin.com

Charles A. Berardesco
Senior Vice President and General Counsel
Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
rebecca.michael@nerc.net

ATTACHMENT 1

2013 ACTUAL COST-TO-BUDGET COMPARISON

AND

2013 AUDITED FINANCIAL REPORT

FOR

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

North American Electric Reliability Corporation 2013 Audited Results – Actual to Budget Variance Analysis

For the year ending December 31, 2013, NERC was approximately on budget with a minor over budget variance of $428.6k (0.8%) for total expenses and fixed asset (capital) purchases, inclusive of expenditures of reserves. While there were some significant variances within the expense categories, as further explained below, this minor overall budget variance was primarily due to: (1) higher personnel expenses resulting from the addition of senior personnel, higher than budgeted expenses for temporary office services needed to support NERC's ongoing operations during times of staff vacancies, higher incentive compensation based upon year-end performance results, higher payroll tax expense due to a higher maximum salary limit subject to taxes, and the accrued expense for unused paid time off, which were partially offset by lower than budgeted benefits and retirement costs; and (2) higher than budgeted expenditures of fixed assets due to capitalization of the development costs of the Enterprise Bulk Electric System Exception (BES) software application and furniture and leasehold improvement costs required for the approved increase in lease space for the Atlanta offices. These over budget expenses were offset to a degree by lower travel expenses due to having fewer FTEs on staff, fewer telecommuters, various management initiatives to reduce overall travel expenses, and lower than budgeted consultant and contract expense. Consultant and contract expenses were under budget primarily due to the reclassification of expenses related to development of the BES software application which were partially budgeted under consulting and contract expenses, but were recorded in fixed assets as capitalized software, resulting in the over budget variance in fixed asset additions . All uses of operating reserves received necessary corporate authorizations and are further explained beginning on page 8 under the heading Operating Reserve Analysis.

2013 ACTUAL VERSUS BUDGET BY CATEGORY

	2013 Actual	2013 Budget	2013 Variance Over(Under)	%
TOTAL FUNDING	**52,349,031**	**52,252,656**	**96,375**	**0.2%**
BUDGET - EXPENSES and FIXED ASSETS				
PERSONNEL EXPENSES	32,113,505	31,298,403	815,101	2.6%
MEETINGS, TRAVEL and CONFERENCE CALLS	3,414,306	4,098,310	(684,005)	-16.7%
CONSULTANTS and CONTRACTS	8,293,693	8,816,254	(522,561)	-5.9%
RENT	2,722,106	2,756,840	(34,734)	-1.3%
OFFICE COSTS, PROFESSIONAL SERVICES and MISCELLANEOUS	5,461,481	5,494,346	(32,865)	-0.6%
Other Non-Operating Expenses	203,164	50,000	153,164	306.3%
FIXED ASSET PURCHASES (excludes the credit for depreciation)	2,506,631	1,772,100	734,531	41.4%
TOTAL BUDGET	**54,714,886**	**54,286,253**	**428,631**	**0.8%**
Change in Working Capital and Operating Reserves	**(2,365,855)**	**(2,033,597)**	**(332,256)**	
FTEs	**174.75**	**186.25**	**(11.50)**	**-6.2%**

The following is an explanation the major factors influencing actual to budget performance for 2013:

- **Funding –** Over budget variance is the net effect of over-budget variances in services and software and testing fees and under-budget variances in workshop fees and Interest. Testing fees were over budget primary due to more system operator certification tests taken and more certificate renewals than expected. Services and software were over budget primarily due to licensing of GADS data which was not planned for 2013. Workshop fees were under budget primarily due to elimination of a NASPI workshop and the elimination of fees for a compliance auditor workshop that was held at a Regional Office instead of a hotel. Interest was under-budget primarily due to extremely low rates of return on invested funds.
- **Staff Vacancies and Attrition**- The company ended the year 11.5 FTEs under budget. Staff attrition for 2013 was 19%, down from 26% in 2012.
- **Personnel Expenses** were $815.1k (2.6%) over budget
    - Salaries expense, which is comprised of base salaries, at risk performance compensation, employment agency fees, temporary office services, and accrued vacation, or paid time off expense, was over budget $1.4M (5.9%).
        - Base salaries were over budget $245.5k, primarily due to the addition of senior personnel.
        - At risk performance compensation was $847.7k over budget primarily due to the fact that the budget was not established taking into account historic results. Similar

to previous budgets, the 2013 budget for at risk performance compensation was based on a hypothetical threshold payout level of 70 percent, with the final payout level dependent upon actual performance results, as well as the availability of funding for any payout amounts in excess of budget.[1] At risk performance compensation is subject to finalization and approval of corporate and departmental performance measures and year end performance reviews of personnel, as well as the receipt of management, Corporate Governance and Human Resources Committee and Board of Trustee approvals in accordance with the company's compensation governance policies. Commencing with the 2015 budget, management is proposing to budget at risk performance compensation based on historic results. This should avoid large variances in actual to budgeted expense for this item and more closely track projected actual year end results throughout the year.

  - Temporary office services expenses were approximately $226.9k over budget due to the increased use of temporary staffing to support NERC's ongoing operations during times of staff vacancies.
  - The accrual for earned but unused vacation, or paid time off expense, was increased at year end and resulted in $89.2k in expense that was not budgeted.

- Payroll taxes were $68.0k (4.7%) over budget due to a higher maximum taxable earnings cap than the assumption in the budget.
- Benefits expense, which is comprised of education and training, health and life, workers compensation, and relocation was $212.6k (6.9%) under budget, primarily due to having fewer FTEs on staff than budgeted and due to lower than budgeted renewal costs associated with NERC's health plans. In the 2013 budget, NERC assumed the cost of health plans would increase 10% over 2012, but actual renewal rates, effective April 1, 2013, increased 9%.
- Retirement expenses were $449.6k (16.6%) under budget primarily due to having fewer FTEs on staff, later eligibility dates due to timing of hiring and due to forfeiture of unvested funds related to personnel attrition.

- **Meetings, Travel, Conferencing and Webinar** expenses were under budget $684.0k (16.7%), primarily due to lower travel costs, as explained above. Travel costs, which were $736.5k lower than budget, were slightly offset by higher than budgeted meetings expense. Meetings expense, which includes the cost of rented space and catering for meetings and workshops held in hotels and the cost of catering for meetings held in NERC or Regional Entity offices, was over budget $63.7k

[1] Over the past several years the incentive compensation budget has been based upon a threshold percentage achievement of corporate goals and per employee maximum incentive compensation eligibility. Projected incentive compensation expense was then accrued during the year based upon historic results. Beginning in 2015, the budget will be based on the three year historic average of the actual total company wide incentive compensation payment amount to actual salary expense. This methodology should more closely track actual results and avoid large variances between budgeted and actual incentive compensation expenses.

primarily due to meetings related to the standards reform initiative, Geo-Magnetic Disturbance initiatives and the Reliability Issues Steering Committee, which were not specifically budgeted.

- **Consultants and Contracts** expenses were $522.6k (5.9%) under budget due primarily, as noted above, to the reclassification of expenses related to development of the Enterprise BES software application, which was partially budgeted under consulting and contract expenses in Information Technology, but recorded in fixed assets as capitalized software in the Reliability Assessments and Performance Analysis program. The following table summarizes the over and under budget variances for consultants and contracts by Program area.

CONSULTANTS and CONTRACTS	Actual	Budget	Over(Under)
STANDARDS	310,600	150,000	160,600
COMPLIANCE OPERATIONS	17,282	-	17,282
RELIABILITY ASSESSMENTS and PERFORMANCE ANALYSIS	757,899	685,000	72,899
RELIABILITY RISK MANAGEMENT*	2,764,411	2,863,180	(98,769)
CRITICAL INFRASTRUCTURE DEPARTMENT**	683,667	785,000	(101,333)
TRAINING, EDUCATION and OPERATOR CERTIFICATION	604,214	848,574	(244,360)
POLICY and EXTERNAL AFFAIRS	39,223	150,000	(110,777)
LEGAL and REGULATORY	3,000	-	3,000
INFORMATION TECHNOLOGY	2,039,258	2,721,000	(681,742)
HUMAN RESOURCES	501,367	288,500	212,867
FINANCE and ACCOUNTING	572,770	325,000	247,770
TOTAL CONTRACTS and CONSULTANTS	**8,293,693**	**8,816,254**	**(522,561)**

*Includes Event Analysis and Situation Awareness Departments

**Includes Critical Infrastructure and ES-ISAC

- The over budget variance in the Reliability Standards Program was related to the NERC standards reform initiative which utilized outside expert consulting resources to review existing standards. These costs were funded from Unknown Contingency operating reserves.
- Compliance Operations – Over budget $17.3k for outside consulting assistance in connection with the reliability assurance initiative. These costs were funded from the Unknown Contingency operating reserves.
- Reliability Assessments and Performance Analysis – Over budget $72.9k primarily related to change orders in connection with improvements to the GADS and TADS databases and to evaluate the development of a web-based replacement for pcGAR. These costs were funded from the Unknown Contingency operating reserves.
- Critical Infrastructure Department – Under budget $101.3k due to lower than budget expenses related to cyber risk preparedness assessments and outside contract and consulting support for deployment of the secure communications portal within the ES-ISAC.

- Reliability Risk Management – Collectively under budget $98.8k for events analysis and situation awareness. The use of subject matter experts to support event analysis was not required, resulting in an under budget variance of $98.0k. Situation Awareness was $0.8k under budget due to lower than budgeted costs for additional industry user licensing fees for SAFNR, which were incurred in 2012 but budgeted in 2013, and due to lower than budgeted costs for the current secure alerts system, the replacement of which is included in NERC's 2014 budget. The under budget expenses related to SAFNR and the alerts system were offset by higher than budgeted network communication expenses for NERCnet.
- Training, Education and Operator Certification –$244.4k under budget due to lower than budgeted expenses for consulting and contract support for (1) system operator exam development, (2) web-based course development and, (3) course review in the continuing education program.
- Policy and External Affairs – Under budget $110.8k due to reductions in external contract support and assumption of greater responsibilities by NERC staff.
- Information Technology – Under expense budget $681.7k primarily due to: (1) the reclassification of expenses related to development of the BES Enterprise software application which was partially budgeted ($500k) as consulting and contract expense, but recorded in fixed assets as capitalized software and required expenditure of operating reserves as reflected in the operating reserve analysis; (2) the decision to delay expenditure of $250k for data warehouse design as the company continues to evaluate its requirements in connection with long term IT infrastructure and application planning; and (3) the decision to delay expenditure of $150k for disaster recovery to permit funding of other higher priority projects which required additional funding. The reduction in expense associated with these projects was offset by costs for development of the Event Information Data System (EIDS), which had been recorded in fixed assets during the course of 2013, but were reclassed as consulting and contract expense prior to finalizing the 2013 audited financial report and as described in the company's March 31, 2014 unaudited variance report which has been filed with the Commission. The total EIDS development cost incurred in 2013 was $638.8k and was funded through a combination of budgeted funds and Known Contingency Operating Reserves.
- Human Resources - $212.9k over budget at year end, due primarily to higher than budgeted costs associated with staff and board compensation studies.
- Finance and Accounting - $247.8k over budget to fund additional outside auditor support in connection with various risk management and internal control initiatives and for costs associated with the evaluation and implementation of upgrades to the company's accounting system.

- **Rent** - $34.7k, 1.3%, under budget due to lower than budgeted straight-line rent expense as a result of the refund of an excess tenant improvement associated with the expansion of the Atlanta office.

- **Office Costs, Professional Services and Miscellaneous**
    - Office Costs were $48.2k, 1.5%, over budget primarily due to higher than budgeted, (1) communication expenses (i.e. internet and cellular services), (2) equipment costs to support employee communications, and (3) equipment repair and service contracts related to NERC's leased offices in Atlanta and Washington, DC. These higher than budgeted expenses were offset by lower than budgeted costs related to copying, use taxes and merchant card fees.
    - Professional Services were $74.0k, 3.2%, under budget due lower than budgeted use of outside counsel. The under budget variance for outside counsel expenses was offset by an increase in outside services expenses related to the implementation of a new travel and expense management system which will improve efficiency and internal controls.
    - Miscellaneous expenses, which were $7.0k, 32.6%, under budget, consist of employee rewards and recognition expenses, costs associated with community responsibility activities, and charitable contributions. The total combined cost of year end employee recognition events in both Atlanta and DC was $13.4k.
- **Depreciation** was $366.1k, 23.2%, over budget due primarily to: (1) development costs of the Enterprise BES software application, which were partially budgeted as contract and consultant expense but recorded in fixed Assets as capitalized software; and (2) higher than budgeted amortization of leasehold improvements in NERC's Atlanta and Washington, DC offices.
- **Other Non-Operating Expenses**, were over budget $153.2k, 306.3%, due primarily to recording as an expense the loss on retirement or disposal of certain fixed assets, principally assets in the situation room in Princeton which was closed in 2013, and the expense of moving certain of the assets to other NERC locations.
- **Fixed Asset Purchases**, excluding a credit for depreciation, were $734.5k, 41.5%, over budget primarily due to, (1) capitalization of the development costs of the Enterprise BES software application, as previously noted, and (2) furniture and leasehold improvement costs required for the approved increase in lease space for the Atlanta offices. As described in 2013 quarterly variance reports, the costs associated with the increase in lease space required for the Atlanta office was not fully known and was estimated at the time the budget was developed, but were within the range of projected expenditures at the time the lease amendment and associated improvements were authorized by the board and committee. Total costs also include the use of operating reserve funding for the standards balloting software (SBS) application and the Enterprise BES software application which are further detailed in the Operating Reserve Analysis and received necessary corporate authorizations in accordance with NERC's Working Capital and Operating Reserve Policy.
- **Allocation of Indirect Expenses and Fixed Assets by Program** – Total direct expenses of the administrative programs were $24.4M, which was 1.3M, 5.8% over budget. Direct expenses were over budget primarily due to higher personnel expenses as a result of having more FTEs on staff than budgeted, the addition of senior staff, higher incentive compensation than budgeted, and an

increase in accrued, unused paid time off. The actual and budgeted allocations of indirect expenses by FTE were $202.0k and $172.9k, respectively, for an increase per FTE of $29.1k. Total fixed assets, net of depreciation for the administrative programs were ($272.1k), which was $569.9k, 191.4%, under budget. Total fixed assets was under budget primarily due to lower than budgeted purchases of capitalized computers and software in the Information Technology department as explained in more detail in the variance report for Informaton Technology that follows on page 21. Collectively, the total budget for administrative programs was $766.3k, 3.3% over budget. The actual and budgeted allocations of fixed assets net of depreciation by FTE were ($2.3k) and $2.2k, respectively for a decrease of $4.4k per FTE. The variances in indirect expenses and the allocation of fixed assets reflected in the variance reports by department are the result of the change in costs per FTE and the difference in actual versus budgeted FTE by department.

Use of Statutory Funds for Non-Statutory Activities

NERC does not have non-statutory activities and therefore did not use statutory funds for non-statutory activities.

Board of Trustees Expenses

The following table provides actual and budgeted expenses of the Board of Trustees. The amounts reflected in this table are included in the totals by expense category in the tables presented above. Trustee expenses were under budget $20.8k, 1.5%, primarily due to lower than budgeted trustee compensation, which was due to a reduction in the total number of independent trustees from eleven to ten, offset by an increase in trustee compensation as approved by the Board on August 15, 2013. Trustee travel expenses were over budget primarily due to 2012 travel expense that was recorded and reimbursed in 2013.

Board of Trustee Expenses	2013 Actual	2013 Budget	Variance Over (Under)	%
Meetings and Travel Expenses				
Quarterly Board Meetings	243,984	234,000	9,984	4.3%
Trustee Travel	166,481	155,000	11,481	7.4%
Total Board of Trustees Meetings and Travel Expenses	**410,465**	**389,000**	**21,465**	**5.5%**
Professional Services				
Independent Trustee Fees	931,250	980,000	(48,750)	-5.0%
Trustee Search Fees	6,495	-	6,495	
Total Board of Trustee Professional Services Expenses	**937,745**	**980,000**	**(42,255)**	**-4.3%**
Total Board of Trustee Expenses	**1,348,210**	**1,369,000**	**(20,790)**	**-1.5%**

Operating Reserve Analysis

As detailed by the table on page 9, the use of "Known Contingency Reserves" included: (1) $209.0k for the development of the BES Enterprise software application, of which $50.1k in non-capitalized costs was recorded in contracts and consultants and $772.2k was recorded as capitalized software[2]; (2) $206.3k for EIDS[3]; (3) consulting support for the Reliability Assurance Initiative and risk management audits, collectively $158.2k; and (4) implementation of additional back office accounting and expense management systems, together with consulting support, related to implementation of the FERC Audit recommendations, $92.7k. The use of "Unknown Contingency Reserves" included: (1) the Standards Overview Project, $160.6k; (2) GADS and TADS upgrades and maintenance and development of a web-based replacement application for pcGAR, collectively $253.7k; (3) a total of $164.2k in costs in excess of the tenant improvement allowance associated with an increase in lease space for the Atlanta office, of which $49.6k was recorded as operating expenses and $114.6k of which was recorded in fixed assets[4]; and (4) $5.1k development of the SBS application, which was not specifically budgeted but was available from reserves due to under runs in the IT capital budget which were transferred to reserves[5].

The working capital and operating reserve analysis reflects that NERC's 2013 approved budget included a reduction in assessments associated with the return of $2,033,600 in excess working capital and operating reserves, which would be funded from $1,686,310 from Unknown Contingency Reserves and $347,290 from the System Operator Reserves. The actual reduction in excess working capital and operating reserves was $2,193,106, of which $2,106,494 came from Known and Unknown Contingency Reserves[6] and $86,613 came from the System Operator Reserves. The lower than budgeted reduction in System Operator reserves, ($86,613 compared to the budgeted reduction of $347,290) was due primarily to (1) higher than budgeted funding from testing fees and certificate renewals, and (2) lower than budgeted Contract and Consultant expenses related to exam development.

[2] The total amount budgeted in contracts and consultants was $613.3k.

[3] The total cost of EIDS in 2013 was $638.8k. The total amount budgeted in contracts and consultants and fixed assets was $432.5k

[4] As previously reported, the total cost of construction, furniture, equipment, leasehold improvements, and operating expenses was $915,162. The tenant improvement allowance was $751,007. The difference between these two figures of $164,155 represents the total cash outlay by NERC for the build out of the additional leased space.

[5] Total 2013 development costs of SBS was $250.1, $245k of which was funded from the IT capital budget.

[6] The $2,365,855 reduction in excess working capital and operating reserves from budgeted operations and the use of known and unknown contingencies was offset by the $172,749 adjustment to reserves related to the excess tenant improvement allowance associated with expansion of NERC's Atlanta office.

OPERATING RESERVE ANALYSIS

	2013 Actual	2013 Budget	Generation (Use) of Reserves	2013 Generation (Use) of Reserves in Excess of Budget: Known Contingency Reserves	Unknown Contingency Reserves[1]	System Operator Reserves
Beginning Working Capital and Operating Reserves						
Balance as of 12/31/12 - per audit	8,305,675	5,440,748	2,864,927			
Less: Adjustment for future liabilities	(3,665,375)		(3,665,375)			
Available Working Capital and Operating Reserves	**4,640,300**	**5,440,748**	**(800,448)**	**1,000,000**	**2,036,821**	**1,603,479**
(1) Generation (Use) of Operating Reserves from Budgeted Operations						
Funding	52,262,956	52,252,656	10,300		10,300	
Personnel	(32,113,505)	(31,298,405)	(815,101)		(815,101)	
Meetings, Travel and Conference Calls	(3,414,306)	(4,098,310)	684,005		684,005	
Contracts and Consultants	(6,504,577)	(7,417,968)	913,391		913,391	
Operating Expenses (excl. contracts, consultants & depreciation)	(8,057,549)	(8,214,186)	156,638		243,250	(86,613)
Non-Operating Expenses	(103,456)	(50,000)	(53,456)		(53,456)	
Fixed Assets (excluding depreciation)	(1,336,565)	(1,444,600)	108,035		108,035	
Total Operating Reserves Generated(Used) from Budgeted Operations	**732,999**	**(270,814)**	**1,003,812**	**-**	**1,090,425**	**(86,613)**
(2) Additions to Operating Reserves						
Services and Software Fees not budgeted	86,075	-	86,075		86,075	
Total Additions to Operating Reserves	86,075	-	86,075	-	86,075	-
(3) Expenditures of Operating Reserves						
Contracts and Consultants						
NERC Standards Overview Project	(310,600)	(150,000)	(160,600)		(160,600)	
GADS and TADS Change Management and Consulting	(269,479)	(80,000)	(189,479)		(189,479)	
pcGAR web-based application development	(64,225)	-	(64,225)		(64,225)	
BES - non-capitalized costs	(50,150)	(613,286)	563,136	563,136		
EIDS	(638,755)	(350,000)	(288,755)	(288,755)		
Reliability Assurance Initiative and Other Auditing	(363,232)	(205,000)	(158,232)	(158,232)		
Systems review and implementation (FERC Audit)	(92,675)		(92,675)	(92,675)		
Subtotal	(1,789,116)	(1,398,286)	(390,830)	23,474	(414,304)	-
Operating Expenses						
Travel and invoice system implementation	(76,452)	(37,000)	(39,452)	(39,452)		
Atlanta Office Expansion	(49,587)		(49,587)		(49,587)	
Subtotal	(126,039)	(37,000)	(89,039)	(39,452)	(49,587)	-
Other Non-Operating Expenses						
Disposal of assets	(99,708)		(99,708)		(99,708)	
Subtotal	(99,708)	-	(99,708)	-	(99,708)	-
Fixed Assets						
SAS Software Upgrade	(33,190)	-	(33,190)		(33,190)	
Atlanta Office Expansion - net in excess of TIA	(114,568)	-	(114,568)		(114,568)	
ERO Applications - BES Exceptions - Capitalized Costs	(772,177)	-	(772,177)	(772,177)		
ERO Applications - EIDS		(82,500)	82,500	82,500		
Standards Balloting Software	(250,131)	(245,000)	(5,131)		(5,131)	
Subtotal	(1,170,066)	(327,500)	(842,566)	(689,677)	(152,889)	-
Total Expenditure of Operating Reserves	(3,184,929)	(1,762,786)	(1,422,143)	(705,655)	(716,488)	-
(4) Net Expenditure of Operating Reserves	**(3,098,855)**	**(1,762,786)**	**(1,336,069)**	**(705,655)**	**(630,414)**	**-**
Total Generation (Use) of Operating Reserves	**(2,365,855)**	**(2,033,600)**	**(332,256)**	**(705,655)**	**460,011**	**(86,613)**
				2013 Reserve Balance		
TOTAL Operating Reserves						
Beginning Balance 1/1/2013	4,640,300	5,440,748	(800,448)	1,000,000	2,036,821	1,603,479
Generation (Use) from Budgeted Operations	732,999	(270,814)	1,003,812	-	819,612	(86,613)
Generation (Use) - Known and Unknown Contingency Reserve	(3,098,855)	(1,762,786)	(1,336,069)	(705,655)	(2,393,200)	
Other adjustments to reserves[2]	172,749		172,749		172,749	
Balance 12/31/13	**2,447,194**	**3,407,148**	**(959,955)**	**294,345**	**635,982**	**1,516,866**

[1]The use of Unknown Contingency Reserves includes the $1,686,310 budgeted reduction in reserves. The 2013 budget also included a $347,290 planned reduction in the System Operator Reserves, for a total budgeted reduction in reserves of $2,033,600.

[2]Represents transactions recorded only on the Statement of Financial Position (balance sheet) and do not impact the Statement of Activities (income statement), including true-up of current versus non-current deferred rent obligation. The increase to reserves in 2013 was due to excess tenant improvement allowance received as part of NERC's expansion in the Atlanta office.

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Statement of Activities and Fixed Assets
(Audited)
For the period ended 12/31/2013

		2013 Actual	2013 Budget	2013 Variance Over(Under)	%
	Funding				
	Assessments	47,604,156	47,604,156	0	
	Penalties	2,512,500	2,512,500	(0)	
	Testing	1,822,154	1,680,000	142,154	
	Services & Software	86,075	-	86,075	
	Workshop Fees	320,725	436,000	(115,275)	
	Interest	3,197	20,000	(16,803)	
	Miscellaneous	224	-	224	
A	**Total Funding**	52,349,031	52,252,656	96,375	0.2%
	Expenses				
	Personnel Expenses				
	Salaries	25,465,466	24,056,166	1,409,301	
	Payroll Taxes	1,527,728	1,459,710	68,018	
	Employee Benefits	2,867,337	3,079,941	(212,604)	
	Savings & Retirement	2,252,973	2,702,588	(449,615)	
	Total Personnel Expenses	32,113,505	31,298,405	815,101	2.6%
	Meeting Expenses				
	Meetings	1,105,734	1,042,000	63,734	
	Travel	2,001,968	2,738,500	(736,532)	
	Conference Calls	306,603	317,810	(11,207)	
	Total Meeting Expenses	3,414,306	4,098,310	(684,005)	-16.7%
	Operating Expenses				
	Consultants and Contracts	8,293,693	8,816,254	(522,561)	
	Rent & Improvements	2,722,106	2,756,840	(34,734)	
	Office Costs	3,229,693	3,181,515	48,178	
	Professional Services	2,217,307	2,291,331	(74,024)	
	Miscellaneous	14,482	21,500	(7,018)	
	Depreciation	1,945,946	1,579,801	366,145	
	Total Operating Expenses	18,423,226	18,647,242	(224,015)	-1.2%
	Other Non-Operating Expenses	203,164	50,000	153,164	306.3%
	Indirect Expenses	-	-	-	
B	**Total Expenses**	54,154,201	54,093,957	60,245	0.1%
=A-B	**Net Change in Assets**	**(1,805,170)**	**(1,841,301)**	**36,130**	**-2.0%**
	Fixed Assets				
	Depreciation	(1,945,946)	(1,579,801)	(366,145)	
	Computer & Software CapEx	1,536,218	1,556,100	(19,882)	
	Furniture & Fixtures CapEx	354,745	-	354,745	
	Equipment CapEx	540,478	216,000	324,478	
	Leasehold Improvements	75,189	-	75,189	
	Allocation of Fixed Assets	-	-	-	
C	**Incr(Dec) in Fixed Assets**	**560,685**	**192,299**	**368,386**	**191.6%**
=B+C	**Total Budget (Expenses plus Incr(Dec) in Fixed Assets)**	**54,714,886**	**54,286,256**	**428,631**	**0.8%**
=A-B-C	**Change in Operating Reserves (Total Funding less Total Budget)**	**(2,365,855)**	**(2,033,600)**	**(332,256)**	**16.3%**
	FTE's	174.75	186.25	(11.50)	-6.2%

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

STANDARDS	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Funding					
Assessments	9,156,330	9,156,330	-	0.0%	
Penalties	510,788	510,788	-	0.0%	
Testing		-	-		
Services & Software		-	-		
Workshop Fees	99,250	104,000	(4,750)	-4.6%	
Interest	688	3,970	(3,282)	-82.7%	
Miscellaneous	48		48		
Total Funding	9,767,104	9,775,088	(7,984)	-0.1%	
Expenses					
Personnel Expenses					
Salaries	3,428,381	3,335,519	92,862	2.8%	Lower than budgeted salaries due to fewer FTEs was offset by higher than budgeted incentive compensation as explained in the cover letter, and costs related to temporary office services which was budgeted in HR.
Payroll Taxes	215,109	213,052	2,057	1.0%	
Employee Benefits	371,555	350,484	21,071	6.0%	Relocation and education benefits budgeted in HR, offset by lower than budgeted health benefits.
Savings & Retirement	328,236	362,334	(34,098)	-9.4%	Under budget due to timing of hiring and later eligibility in the plan
Total Personnel Expenses	4,343,281	4,261,389	81,892	1.9%	
Meeting Expenses					
Meetings	224,755	164,000	60,755	37.0%	Standards/Compliance workshop expense $30k higher than budgeted, but largely offset by workshop fees; and meetings of standards drafting teams $30k higher than budgeted
Travel	352,082	372,500	(20,418)	-5.5%	Due to having fewer telecommuters and management initiatives to lower overall corporate travel
Conference Calls	117,670	108,500	9,170	8.5%	
Total Meeting Expenses	694,507	645,000	49,507	7.7%	
Operating Expenses					
Consultants and Contracts	310,600	150,000	160,600	107.1%	Higher than budget due to costs of standards overview project.
Rent & Improvements		-	-		
Office Costs	78,654	77,850	804	1.0%	
Professional Services	-	-	-		
Miscellaneous	500	500	(0)	0.0%	
Depreciation	2,324	-	2,324		
Total Operating Expenses	392,078	228,350	163,728	71.7%	
Other Non-Operating Expenses	-	-	-	0.0%	
Indirect Expenses	5,252,332	4,581,241	671,091	14.6%	
Total Expenses	10,682,199	9,715,980	966,219	9.9%	
Net Change in Assets	(915,094)	59,108	(974,203)		
Fixed Assets					
Depreciation	(2,324)	-	(2,324)		
Computer & Software CapEx	252,330	-	252,330		$245k -Funded SBS from IT capital budget that was released to reserves and laptop purchase, also budgeted in IT
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Allocation of Fixed Assets	(58,544)	59,108	(117,652)		
Incr(Dec) in Fixed Assets	191,462	59,108	132,354	223.9%	
Total Budget	10,873,661	9,775,088	1,098,573	11.2%	
Change in Working Capital	(1,106,556)	0	(1,106,556)		
FTE's	26.00	26.50	(0.50)	-1.9%	Due to staff vacancies

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

COMPLIANCE OPERATIONS , ORGANIZATION REGISTRATION, and INVESTIGATIONS	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Funding					
Assessments	8,422,798	8,422,798	-	0.0%	
Penalties	462,601	462,601	-	0.0%	
Testing		-	-		
Services & Software		-	-		
Workshop Fees		40,000	(40,000)	-100.0%	Compliance auditor workshop held at Regional Office so no fees were charged
Interest	599	3,595	(2,996)	-83.3%	
Miscellaneous	42	-	42		
Total Funding	8,886,040	8,928,994	(42,954)	-0.5%	
Expenses					
Personnel Expenses					
Salaries	3,263,844	3,202,041	61,803	1.9%	
Payroll Taxes	200,837	202,103	(1,266)	-0.6%	
Employee Benefits	382,147	325,580	56,567	17.4%	Primarily due to education, training, relocation and other employee benefits which were budgeted in HR but recorded in the employee's home department.
Savings & Retirement	299,376	368,031	(68,655)	-18.7%	Due to fewer FTEs and timing of hiring which impacts eligibility
Total Personnel Expenses	4,146,204	4,097,755	48,449	1.2%	
Meeting Expenses					
Meetings	79,986	80,000	(14)	0.0%	
Travel	294,303	440,500	(146,197)	-33.2%	Due to having fewer FTEs on staff, fewer telecommuters, and various management initiatives to reduce overall travel expenses
Conference Calls	12,077	34,235	(22,158)	-64.7%	The budget for conference calls was based upon historical usage, which was lower in 2013 than prior years. Also, $12.1k for conference calls related to the Operating Committee were recorded in the Events Analysis department because the employee liason to the committee transferred to that department in 2013.
Total Meeting Expenses	386,366	554,735	(168,369)	-30.4%	
Operating Expenses					
Consultants and Contracts	17,282	-	17,282		
Rent & Improvements	-	-	-		
Office Costs	57,358	73,424	(16,066)	-21.9%	Telephone, office supplies, and dues were under budget $18k; offset by $2k office costs that were over budget.
Professional Services	7,529	-	7,529		Meeting and interview transcripts that was not budgeted
Miscellaneous	-	500	(500)	-100.0%	
Depreciation	64,869	60,630	4,239	7.0%	
Total Operating Expenses	147,038	134,554	12,484	9.3%	
Other Non-Operating Expenses	4,017	-	4,017		Loss from disposal of assets
Indirect Expenses	4,571,549	4,149,048	422,501	10.2%	
Total Expenses	9,255,174	8,936,092	319,082	3.6%	
Net Change in Assets	(369,134)	(7,098)	(362,036)		
Fixed Assets					
Depreciation	(64,869)	(60,630)	(4,239)	7.0%	
Computer & Software CapEx			-		
Furniture & Fixtures CapEx			-		
Equipment CapEx			-		
Leasehold Improvements			-		
Allocation of Fixed Assets	(50,956)	53,532	(104,488)		
Incr(Dec) in Fixed Assets	(115,825)	(7,098)	(108,727)	1531.8%	
Total Budget	9,139,348	8,928,994	210,355	2.4%	
Change in Working Capital	(253,309)	0	(253,309)		
FTE's	22.63	24.00	(1.37)	-5.7%	Due to staff vacancies and transfer of 1 position to another department

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

COMPLIANCE ENFORCEMENT	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Funding					
Assessments	6,317,083	6,317,083	-	0.0%	
Penalties	404,775	404,775	-	0.0%	
Testing		-	-		
Services & Software		-	-		
Workshop Fees		-	-		
Interest	413	3,146	(2,733)	-86.9%	
Miscellaneous	29	-	29		
Total Funding	6,722,300	6,725,004	(2,704)	0.0%	
Expenses		-			
Personnel Expenses		-			
Salaries	1,854,459	2,152,370	(297,910)	-13.8%	Due to open positions and transfers to other departments, all personnel costs are under budget.
Payroll Taxes	115,289	140,794	(25,505)	-18.1%	
Employee Benefits	199,134	274,882	(75,748)	-27.6%	
Savings & Retirement	188,524	247,200	(58,676)	-23.7%	
Total Personnel Expenses	2,357,406	2,815,246	(457,839)	-16.3%	
Meeting Expenses					
Meetings	4,704	5,000	(296)	-5.9%	
Travel	42,477	186,000	(143,523)	-77.2%	Due to open positions and transfers to other departments and management initiatives to reduce costs
Conference Calls	3,950	-	3,950		
Total Meeting Expenses	51,131	191,000	(139,869)	-73.2%	
Operating Expenses		-			
Consultants and Contracts		-	-		
Rent & Improvements		-	-		
Office Costs	26,116	41,000	(14,884)	-36.3%	Primarily due to lower telecommunications costs due to having fewer FTEs on staff
Professional Services		-	-		
Miscellaneous	-	500	(500)	-100.0%	
Depreciation	2,724	-	2,724		
Total Operating Expenses	28,840	41,500	(12,660)	-30.5%	
Other Non-Operating Expenses		-	-		
Indirect Expenses	3,155,439	3,630,417	(474,978)	-13.08%	
Total Expenses	5,592,816	6,678,163	(1,085,347)	-16.3%	
Net Change in Assets	1,129,484	46,841	1,082,643		
Fixed Assets					
Depreciation	(2,724)	-	(2,724)		
Computer & Software CapEx	2,199		2,199		Laptop purchase budgeted in IT
Furniture & Fixtures CapEx			-		
Equipment CapEx			-		
Leasehold Improvements			-		
Allocation of Fixed Assets	(35,172)	46,841	(82,013)		
Incr(Dec) in Fixed Assets	(35,697)	46,841	(82,538)	-176.2%	
Total Budget	5,557,119	6,725,004	(1,167,885)	-17.4%	
Change in Working Capital	1,165,181	0	1,165,181		
FTE's	15.62	21.00	(5.38)	-25.6%	Due to staff vacancies and transfers to other departments

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

RELIABILITY ASSESSMENTS and PERFORMANCE ANALYSIS	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Funding					
Assessments	7,358,220	7,358,220	-	0.0%	
Penalties	361,407	361,407	-	0.0%	
Testing		-	-		
Services & Software	82,500	-	82,500		The 2013 budget did not include anticipated funding from licensing GADS software to third parties because there were no plans to actively pursue this source of funding. The funding received is reflected in the Operating Reserve Analysis as an addition to the Unknown Contingence Reserve.
Workshop Fees	16,900	40,000	(23,100)	-57.8%	The budget was for a GADS workshop that was not offered in 2013. The funding received was for a modeling workshop that was not planned.
Interest	445	2,809	(2,364)	-84.2%	
Miscellaneous	31	-	31		
Total Funding	7,819,503	7,762,436	57,067	0.7%	
Expenses					
Personnel Expenses			-		
Salaries	2,395,766	2,429,590	(33,823)	-1.4%	
Payroll Taxes	149,180	150,215	(1,036)	-0.7%	
Employee Benefits	263,635	262,761	874	0.3%	
Savings & Retirement	210,672	269,736	(59,064)	-21.9%	Due to fewer FTEs and timing of hiring which impacts eligibility in the plan
Total Personnel Expenses	3,019,253	3,112,303	(93,050)	-3.0%	
Meeting Expenses					
Meetings	114,636	78,000	36,636	47.0%	Additional GMD and RISC meetings that were not budgeted
Travel	309,465	410,000	(100,535)	-24.5%	Due to having fewer telecommuters and management initiatives to lower overall corporate travel
Conference Calls	28,384	31,950	(3,566)	-11.2%	
Total Meeting Expenses	452,485	519,950	(67,465)	-13.0%	
Operating Expenses					
Consultants and Contracts	757,899	685,000	72,899	10.6%	Primarily related to change orders in connection with improvements to the GADS and TADS databases and to evaluate the development of a web-based replacement for pcGAR.
Rent & Improvements		-	-		
Office Costs	122,082	161,416	(39,334)	-24.4%	Telecommunications under budget $11.1k primarily due to fewer FTEs on staff; Maintenance & service agreements $20.65k under budget due to lower cost of software used in modeling and asset tracking
Professional Services	-	-	-		
Miscellaneous	258	500	(242)	-48.5%	
Depreciation	154,643	37,450	117,193	312.9%	The BES database was partially budgeted as Contract and Consultinig expense in IT, but was recorded as capitalized software. Depreciation began in July when the asset was put into production.
Total Operating Expenses	1,034,882	884,366	150,516	17.0%	
Other Non-Operating Expenses		-	-		
Indirect Expenses	3,397,854	3,241,444	156,410	4.8%	
Total Expenses	7,904,473	7,758,064	146,411	1.9%	
Net Change in Assets	(84,970)	4,372	(89,344)	-2043.7%	
Fixed Assets					
Depreciation	(154,643)	(37,450)	(117,193)	312.9%	Depreciation of the BES database which was not budgeted - See above
Computer & Software CapEx	810,517	-	810,517		$772.2k for development of BES exception database which was partially budgeted as an expense; $31k for SAS Software; and laptop purchase budgeted in IT
Furniture & Fixtures CapEx			-		
Equipment CapEx			-		
Leasehold Improvements			-		
Allocation of Fixed Assets	(37,874)	41,822	(79,696)		
Incr(Dec) in Fixed Assets	618,000	4,372	613,628		
Total Budget	8,522,473	7,762,436	760,038	9.8%	
Change in Working Capital	(702,970)	(0)	(702,970)		
FTE's	16.82	18.75	(1.93)	-10.3%	Due to staff vacancies

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

TRAINING, EDUCATION and OPERATOR CERTIFICATION	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Funding					
Assessments	1,449,793	1,449,793	0	0.0%	
Penalties	93,484	93,484	-	0.0%	
Testing	1,822,154	1,680,000	142,154	8.5%	
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	182	1,199	(1,017)	-84.8%	
Miscellaneous	13	-	13		
Total Funding	3,365,625	3,224,476	141,149	4.4%	
Expenses	-	-			
Personnel Expenses	-	-			
Salaries	648,971	837,645	(188,674)	-22.5%	Due to staff vacancies and lower than budget average salaries due to evaluation of future requirments for open positions
Payroll Taxes	55,655	54,087	1,568	2.9%	
Employee Benefits	111,634	112,396	(762)	-0.7%	
Savings & Retirement	57,056	94,203	(37,147)	-39.4%	Due to fewer FTEs and timing of hiring that impacts eligibility in the plan
Total Personnel Expenses	873,315	1,098,331	(225,015)	-20.5%	
Meeting Expenses			-		
Meetings	53,277	30,000	23,277	77.6%	The Personnel Certification Governance Committee (PCGC) held quarterly meetings at hotels which in prior years had been held via conference call
Travel	45,692	70,000	(24,308)	-34.7%	Less travel than budgeted due to management initiative to lower total corporate travel expense.
Conference Calls	33,257	27,000	6,257	23.2%	The Training department increased training opportunities for NERC employees through the use of webinars.
Total Meeting Expenses	132,226	127,000	5,226	4.1%	
Operating Expenses	-	-	-		
Consultants and Contracts	604,214	848,574	(244,360)	-28.8%	Under budget primarily due to lower than budgeted expenses for consulting and contract support for (1) system operator exam development, (2) web-based course development and, (3) course review in the continuing education program
Rent & Improvements	-	-	-		
Office Costs	85,908	96,500	(10,592)	-11.0%	$3.4k due to lower telecommunications costs; $3k due to lower merchant credit card fees; $2.7k lower dues and subscription expenses
Professional Services	-	-	-		
Miscellaneous	80	500	(420)	-84.0%	
Depreciation	480	-	480		
Total Operating Expenses	690,682	945,574	(254,892)	-27.0%	
Other Non-Operating Expenses	-	-	-		
Indirect Expenses	1,387,828	1,383,016	4,812	0.3%	
Total Expenses	3,084,051	3,553,921	(469,870)	-13.2%	
Net Change in Assets	281,574	(329,445)	611,019	-185.5%	
Fixed Assets					
Depreciation	(480)	-	(480)		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	9,595	-	9,595		Equipment purchased for producing training materials that can be saved and posted on NERC's website and internal intranet for future use
Leasehold Improvements	-	-	-		
Allocation of Fixed Assets	(15,469)	17,844	(33,313)		
Incr(Dec) in Fixed Assets	(6,354)	17,844	(24,198)	-135.6%	
Total Budget	3,077,697	3,571,765	(494,068)	-13.8%	
Change in Working Capital	287,928	(347,289)	635,217	-182.9%	
FTE's	6.87	8.00	(1.13)	-14.1%	Due to staff vacancies

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

EVENT ANALYSIS	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Funding					
Assessments	3,501,894	3,501,894	-		
Penalties	183,113	183,113	-		
Testing		-	-		
Services & Software		-	-		
Workshop Fees	43,650	52,000	(8,350)	-16.1%	Fees collected for Human Performance Workshop less than budgeted. The cost of the workshop, recorded as Meetings Expense, was under budget $5k.
Interest	269	1,423	(1,154)	-81.1%	
Miscellaneous	19	-	19		
Total Funding	3,728,945	3,738,430	(9,485)	-0.3%	
Expenses					
Personnel Expenses					
Salaries	1,612,923	1,340,677	272,246	20.3%	FTEs were over budget 7% due to transfer of staff from another department. Personnel expenses are 18% higher because the 2013 budget for personnel expenses included a 3% reduction in salaries, payroll taxes and retirement costs to budget for attrition and timing of new hires, but the 3% reduction was not applied to budgeted FTEs. Salaries expense was also higher due to higher than budgeted incentive compensation. Higher salaries expense also contributed to higher retirement expenses.
Payroll Taxes	94,740	82,107	12,633	15.4%	
Employee Benefits	129,757	125,336	4,421	3.5%	
Savings & Retirement	168,223	153,189	15,034	9.8%	
Total Personnel Expenses	2,005,644	1,701,309	304,335	17.9%	
Meeting Expenses					
Meetings	76,184	62,000	14,184	22.9%	Meetings of the Operating Committee were budgeted in another department resulting in an over budget variance of $19.2k; offset by $5k under budget cost of the Human Performance workshop as noted above.
Travel	132,958	155,000	(22,042)	-14.2%	Primarily due to management initiatives to reduce overal travel expense.
Conference Calls	12,519	-	12,519		Conference calls were collectively budgeted in Compliance Operations due to the lack of historical data to support an allocation to Event Analysis
Total Meeting Expenses	221,662	217,000	4,662	2.1%	
Operating Expenses					
Consultants and Contracts	22,050	120,000	(97,950)	-81.6%	The use of subject matter experts to support event analysis was not required
Rent & Improvements		-	-		
Office Costs	32,606	36,100	(3,494)	-9.7%	
Professional Services	-	-	-		
Miscellaneous	909	500	409	81.8%	
Depreciation	842	-	842		
Total Operating Expenses	56,407	156,600	(100,193)	-64.0%	
Other Non-Operating Expenses					
Indirect Expenses	2,054,470	1,642,332	412,138	25.1%	
Total Expenses	4,338,183	3,717,240	620,941	16.7%	
Net Change in Assets	(609,238)	21,190	(630,426)		
Fixed Assets					
Depreciation	(842)	-	(842)		
Computer & Software CapEx	-		-		
Furniture & Fixtures CapEx			-		
Equipment CapEx	-		-		
Leasehold Improvements			-		
			-		
Allocation of Fixed Assets	(22,900)	21,190	(44,090)		
Incr(Dec) in Fixed Assets	(23,742)	21,190	(44,932)	-212.0%	
Total Budget	4,314,441	3,738,430	576,009	15.4%	
Change in Working Capital	(585,495)	(0)	(585,495)		
FTE's	10.17	9.50	0.67	7.1%	Staff transfer from another department

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

SITUATION AWARENESS	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Funding					
Assessments	5,093,049	5,093,049	-	0.0%	
Penalties	125,288	125,288	-	0.0%	
Testing		-	-		
Services & Software	3,575	-	3,575		FIST Royalties and TSIN fees not budgeted due to unpredictability
Workshop Fees	88,405	105,000	(16,595)	-15.8%	NASPI workshop fees lower than budgeted due to elimination of 1 of 3 planned workshops
Interest	131	974	(843)	-86.6%	
Miscellaneous	9		9		
Total Funding	5,310,457	5,324,311	(13,854)	-0.3%	
Expenses					
Personnel Expenses					
Salaries	662,124	856,927	(194,802)	-22.7%	Lower salaries and payroll tax expense due to having fewer FTE's on staff than budgeted
Payroll Taxes	43,913	56,925	(13,011)	-22.9%	
Employee Benefits	106,891	87,659	19,232	21.9%	Medical and Dental $8.7k under budget due to fewer FTEs; offset by $24k in costs for education and relocation benefits that were budgeted in HR
Savings & Retirement	50,303	98,496	(48,194)	-48.9%	Due to fewer FTEs and timing of hiring that impacts eligibility in the plan
Total Personnel Expenses	863,231	1,100,007	(236,775)	-21.5%	
Meeting Expenses					
Meetings	107,491	198,000	(90,509)	-45.7%	Budget included three NASPI workshops but only two were held and the department held all other meetings in NERC's offices rather than hotels
Travel	29,235	72,500	(43,265)	-59.7%	Due to open positions and management initiatives to lower overall travel costs
Conference Calls	2,544	24,175	(21,631)	-89.5%	The budget for conference calls was based upon historical usage. In prior years, the Situation Awareness and Critical Infrastructure (CID) departments were combined. This under budget variance is offset by the over budget variance in CID.
Total Meeting Expenses	139,270	294,675	(155,405)	-52.7%	
Operating Expenses					
Consultants and Contracts	2,742,361	2,743,180	(819)	0.0%	
Rent & Improvements		-	-		
Office Costs	40,145	47,750	(7,605)	-15.9%	Primarily due to lower telecommunications costs due to having fewer FTEs on staff.
Professional Services	-	-	-		
Miscellaneous	-	500	(500)	-100.0%	
Depreciation	4,645	7,395	(2,750)	-37.2%	
Total Operating Expenses	2,787,151	2,798,825	(11,674)	-0.4%	
Other Non-Operating Expenses	56,346	-	56,346		Primarily due to loss on disposal of assets in the situation room in the Princeton office which was closed in 2013
Indirect Expenses	997,943	1,123,701	(125,758)	-11.2%	
Total Expenses	4,843,942	5,317,208	(473,266)	-8.9%	
Net Change in Assets	466,515	7,103	459,412	6467.5%	
Fixed Assets					
Depreciation	(4,645)	(7,395)	2,750	-37.2%	
Computer & Software CapEx	2,155		2,155		Laptop purchase budgeted in IT
Furniture & Fixtures CapEx			-		
Equipment CapEx			-		
Leasehold Improvements			-		
			-		
Allocation of Fixed Assets	(11,123)	14,498	(25,621)		
Incr(Dec) in Fixed Assets	(13,613)	7,103	(20,716)	-291.7%	
Total Budget	4,830,328	5,324,311	(493,982)	-9.3%	
Change in Working Capital	480,128	0	480,128		
FTE's	4.94	6.50	(1.56)	-24.0%	Due to staff vacancies

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

CRITICAL INFASTRUCTURE and ES-ISAC	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Funding					
Assessments	7,991,299	7,991,299	-	0.0%	
Penalties	371,044	371,044	-	0.0%	
Testing		-	-		
Services & Software		-	-		
Workshop Fees	72,520	95,000	(22,480)	-23.7%	Lower than budgeted fees collected for the Grid Security Conference. As noted below under Meetings, the expense of the conference was under budget $34k.
Interest	471	2,884	(2,413)	-83.7%	
Miscellaneous	33	-	33		
Total Funding	8,435,367	8,460,227	(24,860)	-0.3%	
Expenses					
Personnel Expenses					
Salaries	2,838,325	2,853,871	(15,546)	-0.5%	
Payroll Taxes	165,139	172,586	(7,447)	-4.3%	
Employee Benefits	294,135	250,885	43,250	17.2%	Education, training, relocation and parking/mass transit benefits budgeted in HR and collectively $54.59k over budget; offset by medical, life, and other benefits $11.40k under budget
Savings & Retirement	288,819	312,315	(23,496)	-7.5%	Due to fewer FTEs and timing of hiring which affects eligibility in the plan
Total Personnel Expenses	3,586,418	3,589,657	(3,239)	-0.1%	
Meeting Expenses					
Meetings	120,648	145,000	(24,352)	-16.8%	The cost of CIPC meetings was $10k over budgeted, offset by $34k Grid Security Conference that was under budget
Travel	278,628	420,000	(141,372)	-33.7%	Fewer FTEs on staff than budgeted and lower costs due to management initiatives to lower total corporate travel expense
Conference Calls	40,831	24,000	16,831	70.1%	The budget for conference calls was based upon historical usage. In prior years, the Situation Awareness and Critical Infrastructure (CID) departments were combined. This over budget variance is offset by the over budget variance in Situation Awareness.
Total Meeting Expenses	440,107	589,000	(148,893)	-25.3%	
Operating Expenses					
Consultants and Contracts	683,667	785,000	(101,333)	-12.9%	Lower than budgeted expenses related to cyber risk preparedness assessments and outside contract and consulting support for deployment of the secure communications portal within the ES-ISAC
Rent & Improvements		-	-		
Office Costs	128,724	125,250	3,474	2.8%	
Professional Services	-	-	-		
Miscellaneous	-	500	(500)		
Depreciation	16,602	-	16,602		Depreciation of capitalized software supporting the ES-ISAC that was purchased after the 2013 budget was developed.
Total Operating Expenses	828,993	910,750	(81,757)	-9.0%	
Other Non-Operating Expenses		-	-		
Indirect Expenses	3,597,847	3,327,882	269,965	8.1%	
Total Expenses	8,453,365	8,417,290	36,076	0.4%	
Net Change in Assets	(17,998)	42,937	(60,936)	-141.9%	
Fixed Assets					
Depreciation	(16,602)	-	(16,602)		Depreciation of capitalized software supporting the ES-ISAC that was purchased after the 2013 budget was developed.
Computer & Software CapEx			-		
Furniture & Fixtures CapEx			-		
Equipment CapEx			-		
Leasehold Improvements	3,159		3,159		Improvements specifically related to ES-ISAC
Allocation of Fixed Assets	(40,103)	42,937	(83,040)		
Incr(Dec) in Fixed Assets	(53,546)	42,937	(96,483)	-224.7%	
Total Budget	8,399,819	8,460,227	(60,407)	-0.7%	
Change in Working Capital	35,547	(0)	35,547		
			0		
FTE's	17.81	19.25	(1.44)	-7.5%	Due to staff vacancies

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

GENERAL and ADMINISTRATIVE, including Executive and Policy & External Affairs	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Funding					
Assessments	(1,686,309)	(1,686,309)	-	0.0%	
Penalties	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding	(1,686,309)	(1,686,309)	-	0.0%	
Expenses					
Personnel Expenses					
Salaries	2,477,017	1,342,080	1,134,938	84.6%	Due to transfers from other departments, addition of senior management, higher than budgeted incentive compensation, increase in accrued but unpaid vacation expense and the 3% reduction in the 2013 budgeted expenses to adjust for attrition
Payroll Taxes	113,386	60,640	52,746	87.0%	Due to additional FTEs on staff
Employee Benefits	286,595	156,238	130,357	83.4%	Due to additional FTEs on staff
Savings & Retirement	92,594	175,179	(82,585)	-47.1%	Higher retirement expenses due to having additional FTEs on staff was offset by forfeited unvested benefits
Total Personnel Expenses	2,969,592	1,734,136	1,235,456	71.2%	
Meeting Expenses		-			
Meetings	305,054	260,000	45,054	17.3%	The cost of BOT meetings was approximately $10k over budget; $15k sponsorship of Electric Infrastructure Security Council not budgeted; and $21.1k participation in Canadian Electricity Assoc cross-border forum, also not budgeted
Travel	332,176	322,000	10,176	3.2%	
Conference Calls	28,633	57,500	(28,868)	-50.2%	Conference call expense was budgeted based upon historical average. Decreased usage in 2013 from prior years.
Total Meeting Expenses	665,862	639,500	26,362	4.1%	
Operating Expenses					
Consultants and Contracts	39,223	150,000	(110,777)	-73.9%	Due to reductions in external contract support for Policy & External Affairs department and assumption of greater responsibilities by NERC staff
Rent & Improvements	2,722,106	2,756,840	(34,734)	-1.3%	
Office Costs	392,437	507,000	(114,563)	-22.6%	Office supplies, computer supplies, and equipment maintenance and repair were collectively $75k over budget, offset by under budget variances in all other expenses in this category
Professional Services	1,116,638	1,132,053	(15,415)	-1.4%	
Miscellaneous	1,279	5,500	(4,221)	-76.7%	
Depreciation	489,488	350,526	138,962	39.6%	Primarily due to higher than budgeted amortization of leasehold improvements
Total Operating Expenses	4,761,172	4,901,919	(140,747)	-2.9%	
Other Non-Operating Expenses	66,385	50,000	16,385		Loss from disposal of assets and cost to move remaining useable equipment from Princeton to other NERC offices
Indirect Expenses	(8,463,012)	(7,325,556)	(1,137,456)	15.5%	
Total Expenses	(0)	(0)	0	-59.0%	
Net Change in Assets	(1,686,309)	(1,686,309)	(0)	0.0%	
Fixed Assets					
Depreciation	(489,488)	(350,526)	(138,962)	39.6%	See above
Computer & Software CapEx	2,199	-	2,199		Laptop purchase budgeted in IT
Furniture & Fixtures CapEx	354,745	-	354,745		Furniture for the expansion of the Atlanta office
Equipment CapEx	-	-	-		
Leasehold Improvements	72,030	-	72,030		Expansion of Atlanta office
Allocation of Fixed Assets	60,513	350,526	(290,013)		
Incr(Dec) in Fixed Assets	(0)	-	(0)		
Total Budget	(0)	(0)	0		
Change in Working Capital	(1,686,309)	(1,686,309)	(0)	0.0%	
FTE's	11.21	8.00	3.21	40.1%	Transfers from other department

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

LEGAL and REGULATORY	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Funding					
Assessments			-		
Penalties			-		
Testing			-		
Services & Software			-		
Workshop Fees			-		
Interest			-		
Miscellaneous			-		
Total Funding	-	-	-		
Expenses					
Personnel Expenses					
Salaries	2,536,703	2,325,293	211,410	9%	The budget for salaries, payroll taxes and retirment expenses were reduced by 3% based upon estimated attrition and timing of hiring, but the reduction was not applied to budgeted FTEs. This department was fully staffed in 2013, resulting in the over budget variance for salaries and payroll taxes. Payroll taxes are also higher due to higher maximum salary subject to FICA tax. Retirement expense was under budget due to timing of hiring which affects elibility. Employee benefits was over budget primarily due to education, training and other benefits that were budgeted in HR.
Payroll Taxes	149,302	119,177	30,125	25%	
Employee Benefits	227,659	185,835	41,825	23%	
Savings & Retirement	217,503	261,724	(44,221)	-17%	
Total Personnel Expenses	3,131,168	2,892,029	239,138	8%	
Meeting Expenses					
Meetings	10,572	5,000	5,572	111%	Meetings of the ERO Legal Group were not included in the budget due to being newly formed and lack of historical data
Travel	83,449	144,500	(61,051)	-42%	Less travel due to management initiative to lower overall corporate travel expenses
Conference Calls	10,724	3,200	7,524	235%	Conference call expense was budgeted based upon historical average. Increased usage in 2013 from prior years.
Total Meeting Expenses	104,745	152,700	(47,955)	-31%	
Operating Expenses					
Consultants and Contracts	3,000	-	3,000		Industry survey related to the 5-Yr performance assessment
Rent & Improvements		-	-		
Office Costs	68,053	50,500	17,553	35%	Telephone expense and subscription/publication expense higher than budgeted
Professional Services	735,807	950,000	(214,193)	-23%	All outside counsel fees are budgeted in Legal, but actual fees charged to department managing the engagement. In total, NERC was under budget for outside counsel fees $104.4k.
Miscellaneous	364	500	(136)	-27%	
Depreciation	3,380	-	3,380		
Total Operating Expenses	810,604	1,001,000	(190,396)	-19%	
Other Non-Operating Expenses		-	-		
Indirect Expenses	(4,046,516)	(4,045,729)	(787)	0.02%	
Total Expenses	0	0	(0)	-59%	
Net Change in Assets	(0)	(0)	0	-59%	
Fixed Assets					
Depreciation	(3,380)	-	(3,380)		
Computer & Software CapEx	4,310		4,310		Laptop purchases budgeted in IT
Furniture & Fixtures CapEx			-		
Equipment CapEx			-		
Leasehold Improvements			-		
Allocation of Fixed Assets	(929)		(929)		
Incr(Dec) in Fixed Assets	0	-	0		
Total Budget	0	0	(0)		
Change in Working Capital	(0)	(0)	0		
			0		
FTE's	13.80	14.00	(0.20)		

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

INFORMATION TECHNOLOGY	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Expenses					
Personnel Expenses					
Salaries	1,787,073	1,651,076	135,997	8.2%	Base salaries were under budget due to staff vacancies, but were offset by higher incentive compensation and higher temporary office services that were required as a result of the vacancies
Payroll Taxes	118,892	114,954	3,938	3.4%	
Employee Benefits	226,979	224,184	2,794	1.2%	
Savings & Retirement	166,119	178,464	(12,345)	-6.9%	Due to fewer FTEs and timing of hiring which impacts eligibility
Total Personnel Expenses	2,299,062	2,168,679	130,383	6.0%	
Meeting Expenses					
Meetings	3,371	5,000	(1,629)	-32.6%	
Travel	32,872	62,000	(29,128)	-47.0%	Less travel due to management initiative to lower overall corporate travel expenses
Conference Calls	5,338	4,800	538	11.2%	
Total Meeting Expenses	41,582	71,800	(30,218)	-42.1%	
Operating Expenses					
Consultants and Contracts	2,039,258	2,721,000	(681,742)	-25.1%	Refer to the cover letter, which provides a detailed explanation of this variance.
Rent & Improvements	-	-	-		
Office Costs	2,155,419	1,893,725	261,694	13.8%	Communications expense $202.9k over budget primarily related to delays in closure of the Princeton data center and cancellation of data connection contracts; maintenance and service agreements and non-capitalized software $38.8k over budget due to initiation of enterprise software agreements that will lower annual costs on a long-term basis.
Professional Services	4,706	-	4,706		On-site technical support for employee meetings
Miscellaneous	17	500	(483)	-96.5%	
Depreciation	1,198,919	1,123,002	75,917	6.8%	
Total Operating Expenses	5,398,320	5,738,227	(339,907)	-5.9%	
Other Non-Operating Expenses	76,655	-	76,655		Loss on disposal of assets not fully depreciated
Indirect Expenses	(7,815,620)	(7,978,706)	163,086	-2.0%	
Total Expenses	(0)	(0)	(0)	120.0%	
Net Change in Assets	0	0	0	120.0%	
Fixed Assets					
Depreciation	(1,198,919)	(1,123,002)	(75,917)	6.8%	
Computer & Software CapEx	448,414	1,556,100	(1,107,686)	-71.2%	$245.0k for SBS recorded in Standards; $350.0 less than budgeted for data warehouse hardware; $202.4k for hardware recorded in Equipment CapEx; $132.3k less for laptops (offset by $15k recorded in other departments); $82.5k allocated to EIDS; $95.5k less for replacement servers that were not needed
Furniture & Fixtures CapEx		-	-		
Equipment CapEx	530,883	216,000	314,883	145.8%	$112.4k related to expansion of Atlanta office; $202.4k for hardware budgeted as computer CapEx
Leasehold Improvements		-	-		
Allocation of Fixed Assets	219,622	(649,098)	868,720		
Incr(Dec) in Fixed Assets	0	-	0		
Total Budget	(0)	(0)	(0)		
Change in Working Capital	0	0	0		
FTE's	14.88	16.75	(1.87)	-11.2%	Due to staff vacancies

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

HUMAN RESOURCES	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Funding					
Assessments			-		
Penalties			-		
Testing			-		
Services & Software			-		
Workshop Fees			-		
Interest			-		
Miscellaneous			-		
Total Funding	-	-	-		
Expenses					
Personnel Expenses					
Salaries	531,365	498,723	32,642	6.5%	Over budget due to no attrition, which was budgeted at 3% across all departments and higher incentive compensation than budgeted
Payroll Taxes	26,028	22,610	3,418	15.1%	
Employee Benefits	111,231	573,737	(462,506)	-80.6%	Benefits budgeted in HR but charged to employee's home cost center when utilized include education and training, relocation and parking/mass transit benefits. Collectively, these expenses are $490.49k under budget in HR, but equal to budget for total NERC. Medical benefits are $27.96k over budget due to a higher actual cost than the budgeted average cost per employee.
Savings & Retirement	43,971	41,348	2,623	6.3%	
Total Personnel Expenses	712,595	1,136,418	(423,823)	-37.3%	
Meeting Expenses					
Meetings	1,943	5,000	(3,057)	-61.1%	
Travel	13,829	21,000	(7,171)	-34.1%	Primarily due to management initiatives to reduce overal travel expense.
Conference Calls	1,181	600	581	96.8%	
Total Meeting Expenses	16,952	26,600	(9,648)	-36.3%	
Operating Expenses					
Consultants and Contracts	501,367	288,500	212,867	73.8%	Due primarily to higher than budgeted costs associated with staff and board compensation studies
Rent & Improvements		-	-		
Office Costs	10,142	42,500	(32,358)	-76.1%	Monthly fees for performance management and benefits enrollment services were budgeted in office costs, but actuals are charged to professional fees to more accurately describe the expense. A corresponding over budget variance is reflected for professional services.
Professional Services	61,562	23,278	38,284	164.5%	See comment under office costs
Miscellaneous	10,936	10,500	436	4.2%	
Depreciation	4,833	-	4,833		
Total Operating Expenses	588,840	364,778	224,062	61.4%	
Other Non-Operating Expenses		-	-		
Indirect Expenses	(1,318,387)	(1,527,796)	209,409	-13.7%	
Total Expenses	0	(0)	(0)	36.8%	
Net Change in Assets	(0)	0	0	36.8%	
Fixed Assets					
Depreciation	(4,833)	-	(4,833)		
Computer & Software CapEx	11,600		11,600		Active Strategy software budgeted in IT
Furniture & Fixtures CapEx			-		
Equipment CapEx			-		
Leasehold Improvements			-		
Allocation of Fixed Assets	(6,767)		(6,767)		
Incr(Dec) in Fixed Assets	(0)	-	(0)		
Total Budget	0	(0)	(0)		
Change in Working Capital	(0)	0	0		
FTE's	3.00	3.00	-		

North American Electric Reliability Corp
2013 Statement of Activities and Fixed Asset Budget

FINANCE and ACCOUNTING	2013 Actual	2013 Budget	2013 Variance Over(Under)	%	Comments (Explain variances < +/- 10% and $10,000)
Funding					
Assessments			-		
Penalties			-		
Testing			-		
Services & Software			-		
Workshop Fees			-		
Interest			-		
Miscellaneous			-		
Total Funding	-	-	-		
Expenses					
Personnel Expenses					
Salaries	1,428,514	1,230,355	198,159	16.1%	Salaries and payroll taxes over budget due to the 3% reduction in budgeted expenses to adjust for attrition in all departments and temporary office services, budgeted in HR, utilized during staff leave of absence.
Payroll Taxes	80,258	70,460	9,799	13.9%	
Employee Benefits	155,986	149,964	6,022	4.0%	
Savings & Retirement	141,578	140,368	1,210	0.9%	
Total Personnel Expenses	1,806,336	1,591,146	215,190	13.5%	
Meeting Expenses					
Meetings	3,113	5,000	(1,887)	-37.7%	
Travel	54,803	62,500	(7,697)	-12.3%	
Conference Calls	9,494	1,850	7,644	413.2%	
Total Meeting Expenses	67,410	69,350	(1,940)	-2.8%	
Operating Expenses					
Consultants and Contracts	572,770	325,000	247,770	76.2%	Additional outside auditor support in connection with various risk management and internal control initiatives and costs associated with the evaluation and implementation of upgrades to the company's accounting system
Rent & Improvements		-	-		
Office Costs	32,050	28,500	3,550	12.5%	
Professional Services	291,064	186,000	105,064	56.5%	Primarily due to outside counsel fees which is budgeted in the Legal department. NERC was under budget $104.4k for all outside counsel fees.
Miscellaneous	139	500	(361)	-72.2%	
Depreciation	2,196	798	1,398	175.2%	
Total Operating Expenses	898,219	540,798	357,421	66.1%	
Other Non-Operating Expenses	(240)	-	(240)		
Indirect Expenses	(2,771,726)	(2,201,294)	(570,432)	25.9%	
Total Expenses	(0)	0	0	43.2%	
Net Change in Assets	0	(0)	(0)	43.2%	
Fixed Assets					
Depreciation	(2,196)	(798)	(1,398)	175.2%	
Computer & Software CapEx	2,495		2,495		Additional module to accounting software
Furniture & Fixtures CapEx			-		
Equipment CapEx			-		
Leasehold Improvements			-		
Allocation of Fixed Assets	(299)	798	(1,097)		
Incr(Dec) in Fixed Assets	0	-	0		
Total Budget	(0)	0	0	61.4%	
Change in Working Capital	0	(0)	(0)	61.4%	
FTE's	11.00	11.00	-		

Financial Statements and Report of
Independent Certified Public Accountants

North American Electric Reliability Corporation

December 31, 2013 and 2012

Table of contents

Report of Independent Certified Public Accountants 1

Financial statements:

- Statements of financial position 3
- Statements of activities 4
- Statements of cash flows 5

Notes to financial statements 6

Supplemental schedules of expenses 15

Audit • Tax • Advisory

Grant Thornton LLP
1100 Peachtree Street, NE, Suite 1200
Atlanta, GA 30309-4504

T 404.330.2000
F 404.330.2047
www.GrantThornton.com

Report of Independent Certified Public Accountants

To the Board of Trustees of
North American Electric Reliability Corporation:

We have audited the accompanying financial statements of North American Electric Reliability Corporation (a New Jersey non-profit corporation), which comprise the statements of financial position as of December 31, 2013 and 2012, and the related statements of activities, and cash flows for the years then ended, and the related notes to the financial statements.

Management's responsibility for the financial statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's responsibility

Our responsibility is to express an opinion on these financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

Grant Thornton

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of North American Electric Reliability Corporation as of December 31, 2013 and 2012, and the results of its operations and its cash flows for the years then ended in accordance with accounting principles generally accepted in the United States of America.

Supplementary information

Our audit was conducted for the purpose of forming an opinion on the financial statements as a whole. The supplemental schedules of expenses shown on pages 15-16 are presented for purposes of additional analysis and are not a required part of the financial statements. Such supplementary information is the responsibility of management and was derived from and relates directly to the underlying accounting and other records used to prepare the financial statements. The information has been subjected to the auditing procedures applied in the audit of the financial statements and certain additional procedures. These additional procedures included comparing and reconciling the information directly to the underlying accounting and other records used to prepare the financial statements or to the financial statements themselves, and other additional procedures in accordance with auditing standards generally accepted in the United States of America. In our opinion, the supplementary information is fairly stated, in all material respects, in relation to the financial statements as a whole.

Grant Thornton LLP

Atlanta, Georgia
May 7, 2014

Statements of Financial Position

December 31,	2013	2012
Assets		
Current Assets		
Cash and cash equivalents	**$ 26,182,060**	$ 27,936,696
Accounts receivable, net of allowance for doubtful accounts of $0 and $62,572	**3,353,895**	4,281,602
Prepaid expenses	**869,876**	888,087
Total Current Assets	**30,405,831**	33,106,385
Long-Term Assets		
Property and equipment, net	**5,645,116**	5,220,210
Security deposits	**99,136**	114,903
Cash surrender value of insurance policies	**-**	337,414
457b Plan Assets	**320,660**	118,243
Total Long-Term Assets	**6,064,912**	5,790,770
Total assets	**$ 36,470,743**	$ 38,897,155
Liabilities and net assets		
Current Liabilities		
Accounts payable and accrued expenses	**$ 6,943,283**	$ 5,868,604
Accrued retirement liabilities	**1,788,624**	1,409,548
Deferred revenue	**5,287,044**	5,177,751
Deferred rent - current	**182,421**	123,270
Deferred compensation -current	**20,386**	28,280
Capital lease obligations - current	**47,108**	65,928
Regional assessments collected in advance	**9,427,293**	9,614,829
Total Current Liabilities	**23,696,159**	22,288,210
Long-Term Liabilities		
Deferred rent - non-current	**3,817,478**	3,618,267
Deferred compensation - non-current	**597,514**	711,308
Capital lease obligations- non-current	**-**	47,108
Total Long-Term Liabilities	**4,414,992**	4,376,683
Total liabilities	**28,111,151**	26,664,893
Net assets		
Unrestricted	**7,914,592**	9,719,762
Temporarily restricted	**445,000**	2,512,500
Total net assets	**8,359,592**	12,232,262
Total liabilities and net assets	**$ 36,470,743**	$ 38,897,155

The accompanying notes are an integral part of these financial statements.

Statements of Activities

	For the Year Ended December 31, 2013			For the Year Ended December 31, 2012		
	Unrestricted	Temporarily Restricted	Total	Unrestricted	Temporarily Restricted	Total
Revenues:						
NERC assessments	**$ 47,604,156**	**$ -**	**$ 47,604,156**	$ 50,661,271	$ -	$ 50,661,271
Penalty income	**-**	**445,000**	**445,000**	-	100,000	100,000
Testing / fees	**1,822,154**	**-**	**1,822,154**	2,057,383	-	2,057,383
Services and software	**86,075**	**-**	**86,075**	129,618	-	129,618
Workshops	**320,725**	**-**	**320,725**	470,800	-	470,800
Rental Income	**293,000**	**-**	**293,000**	314,080	-	314,080
Interest	**3,197**	**-**	**3,197**	13,335	-	13,335
(Loss) gain on disposal of fixed assets	**(99,708)**	**-**	**(99,708)**	34	-	34
Miscellaneous revenues	**224**	**-**	**224**	2,081	-	2,081
Net assets (penalties) released from restrictions	**2,512,500**	**(2,512,500)**	**-**	-	-	-
Total revenues	**52,542,323**	**(2,067,500)**	**50,474,823**	53,648,602	100,000	53,748,602
Expenses:						
Salaries	**25,465,466**	**-**	**25,465,466**	23,391,982	-	23,391,982
Employee costs	**4,395,066**	**-**	**4,395,066**	4,096,501	-	4,096,501
Retirement and savings plans	**2,252,973**	**-**	**2,252,973**	1,793,528	-	1,793,528
Travel and meetings	**3,414,306**	**-**	**3,414,306**	3,616,022	-	3,616,022
Services	**10,511,000**	**-**	**10,511,000**	11,819,937	-	11,819,937
Rent	**3,015,106**	**-**	**3,015,106**	2,908,290	-	2,908,290
Office costs	**1,622,635**	**-**	**1,622,635**	1,829,606	-	1,829,606
Computer	**1,607,057**	**-**	**1,607,057**	1,284,025	-	1,284,025
Depreciation and amortization	**1,945,946**	**-**	**1,945,946**	2,144,184	-	2,144,184
Property tax expense	**48,606**	**-**	**48,606**	51,008	-	51,008
Provision for bad debts	**45,610**	**-**	**45,610**	(113,173)	-	(113,173)
Miscellaneous expenses	**20,608**	**-**	**20,608**	25,197	-	25,197
Interest	**3,114**	**-**	**3,114**	6,993	-	6,993
Total expenses	**54,347,493**	**-**	**54,347,493**	52,854,100	**-**	52,854,100
Change in net assets	**(1,805,170)**	**(2,067,500)**	**(3,872,670)**	794,502	100,000	894,502
Net assets, beginning of year	**9,719,762**	**2,512,500**	**12,232,262**	8,925,260	2,412,500	11,337,760
Net assets, end of year	**$ 7,914,592**	**$ 445,000**	**$ 8,359,592**	$ 9,719,762	$2,512,500	$ 12,232,262

The accompanying notes are an integral part of these financial statements.

Statements of Cash Flow

For the Years Ended December 31,	2013	2012
Cash flows from operating activities:		
Change in net assets	**$ (3,872,670)**	$ 894,502
Adjustments to reconcile change in net assets to net cash provided by operating activities:		
Depreciation and amortization	**1,945,946**	2,144,184
Straight-line rent accrual	**258,362**	1,583,373
Loss (gain) on disposal of fixed assets	**99,708**	(34)
Provision for bad debts	**45,610**	(113,173)
Change in value of insurance policies	**337,414**	(55,316)
Increase (decrease) in cash attributable to changes in operating assets and liabilities:		
Accounts receivable	**882,097**	(625,538)
Prepaid expenses	**18,211**	(336,246)
Security deposits	**15,767**	-
Receipt of funds for regional entities	**152,966,084**	115,437,437
Disbursements of funds to regional entities	**(152,966,084)**	(115,437,437)
Accounts payable and accrued expenses	**803,926**	(913,150)
Deferred revenue	**109,293**	2,533,575
Regional assessments collected in advance	**(187,536)**	4,939,801
Deferred compensation	**(324,105)**	26,716
Accrued retirement liabilities	**379,076**	(272,933)
Net cash provided by operating activities	**511,099**	9,805,761
Cash flows from investing activities		
Purchases of property and equipment	**(2,200,782)**	(804,411)
Proceeds from sales of property and equipment	**975**	2,381
Net cash used in investing activities	**(2,199,807)**	(802,030)
Cash flows from financing activities		
Capital lease payments	**(65,928)**	(83,185)
Net cash used in financing activities	(65,928)	(83,185)
Net (decrease) increase in cash and cash equivalents	**(1,754,636)**	8,920,546
Cash and cash equivalents, beginning of year	**27,936,696**	19,016,150
Cash and cash equivalents, end of year	**$ 26,182,060**	$ 27,936,696
Supplemental disclosure of non-cash information:		
Fixed asset purchases within accounts payable	**$ 270,753**	$ -
Capital lease obligation for equipment	**$ -**	$ 93,242
Supplemental disclosure of cash paid:		
Interest	**$ 3,113**	$ 6,993

The accompanying notes are an integral part of these financial statements.

Notes to the Financial Statements

1 Organization and Nature of Business

North American Electric Reliability Corporation (the "Corporation" or "NERC") is an international, independent, not-for-profit organization, whose mission is to ensure the reliability of the bulk power system in North America. NERC relies on the diverse and collective expertise of electricity industry participants, subject to government oversight and audit. The Corporation is certified by the U.S. Federal Energy Regulatory Commission ("FERC") as the Electric Reliability Organization ("ERO") within the United States. In the United States, the Corporation has the authority to levy fines and penalties against any of the individual users, owners and operators of the bulk power system for non-compliance with the reliability standards that govern the bulk power system. The Corporation has also been recognized as the ERO by governmental authorities in Canada.

The Corporation's mission is to enhance the reliability and security of the bulk power system in North America. To achieve that, the Corporation develops and enforces reliability standards; monitors the bulk power system; assesses future adequacy and educates, trains and certifies industry personnel. Entities subject to the Corporation's reliability standards account for virtually all the electricity supplied in the United States of America, Canada and a portion of Baja California, Norte, Mexico.

The Corporation is the successor to North American Electric Reliability Council (the "Council") which was formed in 1968 in the aftermath of the November 1965 blackout that affected the northeastern United States and Ontario, Canada. On October 31, 2006, the Council entered into an agreement and plan of merger with the Corporation, a New Jersey non-profit corporation. At the effective date of the merger, January 1, 2007, the separate corporate existence of the Council ceased, and Corporation became the surviving entity. All of the property, assets, rights, privileges, powers, franchises and immunities of the Council became the property of the Corporation. All debts, liabilities and obligations of the Council were also assumed by the Corporation. The Corporation is organized and operates as a business league under Internal Revenue Code Section 501(c) (6). The activities of the Corporation are directed by an independent board of trustees.

The membership of the Corporation is unique. It is a not-for-profit corporation whose members include users, owners and operators of the bulk power system, eight regional entities, large and small end-use customers, state and provincial governmental authorities and any other interested parties.

Annually, the board of trustees approves an operating budget for the Corporation that includes a provision for working capital and operating reserves, which are recovered through assessments to Load-Serving Entities ("LSE"). The determination of the annual working capital and operating reserve requirements and the authorization of management to access these funds is governed by the Corporation's "Working Capital and Operating Reserve Policy". The Corporation assesses each LSE its proportional share of its annual operating budget based on "net energy for load". During 2013, the assessments to LSEs made up approximately 94% of the total funding for the Corporation. Assessments to U.S. entities were offset in 2013 by $2.5M in penalties received in prior years but were restricted from use until 2013 per the Corporation's policy on the "Accounting, Financial Statement and Budgetary Treatment of Penalties Imposed and Received for Violations of Reliability Standards". The Corporation also generates funding from the collection of fees charged for various services. These services include the maintenance of a certification program for system operators, the development of reports and software programs, and the hosting of workshops to educate the industry on various reliability matters.

The Corporation has entered into separate Delegation Agreements, which have been approved by FERC, with eight Regional Entities: Florida Reliability Coordinating Council ("FRCC"), Midwest Reliability Organization ("MRO"), Northeast Power Coordinating Council ("NPCC"), Reliability First Corporation ("RFC"), SERC Reliability Corporation ("SERC"), Southwest Power Pool Regional Entity ("SPP"), Texas Reliability Entity ("TRE") and Western Electricity Coordinating Council ("WECC"). Through these Delegation Agreements, the Corporation has delegated certain of its ERO responsibilities and functions to the Regional Entities.

The Corporation must annually approve the eight Regional Entities' budgets and submit them along with its budget and schedule of assessments to load serving entities to FERC for final approval of the budgets and the U.S. portion of the assessments. The Corporation has the sole responsibility to invoice, collect and disburse the monies approved in the Regional Entities' budgets. These pass-through amounts are not included as revenue and expense in the statement of activities, see related Note 6.

2 Summary of Significant Accounting Policies

Basis of Accounting and Presentation

The financial statements of the Corporation have been prepared on the accrual basis of accounting in conformity with accounting principles generally accepted in the United States of America. Net assets, revenues, expenses, gains and losses are classified based on the existence or absence of restrictions. The Corporation reports information regarding its financial position and activities according to three classes of net assets: unrestricted net assets, temporarily restricted net assets and permanently restricted net assets. There were no permanently restricted net assets as of December 31, 2013 or 2012. Net assets totaling $445,000 and $2,512,500 were temporarily restricted by FERC as of December 31, 2013 and 2012, respectively, to offset future assessments.

Cash and Cash Equivalents

The Corporation considers all highly liquid investments purchased with original maturities of three months or less to be cash and cash equivalents. The Corporation maintains its cash balances with one bank. The accounts at the bank are insured up to certain limits by the Federal Deposit Insurance Corporation. Balances in these accounts may exceed Federally-insured limits from time to time.

Use of Estimates

The preparation of financial statements in conformity with accounting principles generally accepted in the United States of America requires management to make estimates and assumptions that affect the amounts of assets and liabilities and disclosure of contingent assets and liabilities at the date of the financial statements and the reported amounts of revenues and expenses during the reporting period. Actual results could differ from those estimates.

Revenue Recognition

The Corporation recognizes assessment revenue billed to the LSEs on a pro-rata basis over the calendar year. Fees generated for testing, certifications, services and software, workshops and other services are recognized when the test is taken, service rendered and/or workshops are completed.

Penalty income is derived from FERC's approval of assessment of penalties to registered entities regarding enforcement of NERC's Reliability Standards. The penalty income from a registered entity is recorded following closure of the enforcement matter including exhaustion of appeals and the outcome determined. The funds are temporarily restricted due to FERC's requirement that the funds be used to reduce future NERC assessments.

Deferred Revenue

Deferred revenue represents assessments billed and received in advance of the period in which it is earned. Deferred revenue is recognized as revenue in the period in which it is earned.

Accounts Receivable

Accounts receivable are recorded at the original invoice amount, less an estimated allowance for uncollectible accounts. Credit is generally extended on a short-term basis; thus accounts receivable do not bear interest. Accounts receivable are periodically evaluated for collectability based on past experience and an analysis of current accounts receivable collectability. Changes in the estimated collectability of accounts receivable are recorded in the results of operations for the period in which the estimate is revised. Accounts deemed uncollectible are charged to the allowance in the years they are deemed uncollectible.

Property and Equipment

Purchased property and equipment are capitalized at cost. Donated assets are capitalized at the fair market value of the assets on the date of contribution. The Corporation's minimum capitalization policy is for additions greater than $2,000.

Depreciation and amortization is provided by the straight-line method over the estimated useful lives of the related assets as follows:

	Years
Software development	3 years
Furniture and equipment	3-7 years
Leasehold improvements	Term of lease or estimated useful life of the asset, whichever is shorter

Expenditures for maintenance and repairs are charged to operations as incurred while renewals and betterments are capitalized.

Compensated Absences

Employees of the Corporation are entitled to paid time off depending on length of service. At December 31, 2013 and 2012, the Corporation has recorded accrued compensated absences of $543,126 and $453,950 related to days earned, included with accounts payable and accrued expenses on the statements of financial position.

Income Taxes

The Corporation has received a determination letter from the Internal Revenue Service concluding that it is exempt from Federal income taxes under Section 501(c)(6) of the Internal Revenue Code. The Corporation is subject to income taxes on revenues related to unrelated business activities. The Corporation is subject to a proxy tax related to nondeductible lobbying and political expenses incurred. There was no proxy tax incurred in 2013 or 2012.

The Corporation recognizes the tax benefit from an uncertain tax position only if it is more likely than not that the tax position will be sustained on examination by the taxing authority, based on the technical merits of the position. The Corporation is no longer subject to federal and state tax examinations by the respective taxing authorities for the years prior to 2010. Tax years 2010 through 2013 remain subject to examination by major tax jurisdictions.

Subsequent Events

The Corporation discloses material events that occur after the statement of financial position date but before financial statements are issued. In general, these events are recognized in the financial statements if the condition existed at the date of the statement of financial position, but are not recognized if the condition did not exist at the statement of financial position date. The Corporation discloses non-recognized events if required to keep the financial statements from being misleading. Management evaluated events occurring subsequent to December 31, 2013 through May 7, 2014, the date the financial statements were available for issuance.

On January 13, 2014, the company secured a non-revolving credit facility under the Capital Financing Program that was approved by the Board of Trustees and the Federal Energy Regulatory Commission (FERC) as part of the Corporation's 2014 Business Plan and Budget. The interest rate is floating and equal to LIBOR plus 275 basis points, which yielded a rate of 2.91% at closing. The total size of the non-revolving credit facility is $7.5M, with the total authorized borrowings each year limited to the amount approved by the Board of Trustees and FERC in that year's business plan and budget. The Corporation's line of credit was also amended. See Note 4 below.

In April, 2014, management became aware that the sub-tenant under the Washington, D.C. lease, referenced in Note 8, filed for Chapter 11 bankruptcy, but the full impact of the event is not known at this time.

3 Property and Equipment

Property and equipment consist of the following at December 31:

December 31,	2013	2012
Software development	**$ 2,986,517**	$ 1,599,433
Furniture and equipment	**6,860,119**	7,269,259
Leasehold improvements	**1,100,281**	1,241,799
	10,946,917	10,110,491
Accumulated depreciation and amortization	**(5,301,801)**	(4,890,281)
	$ 5,645,116	$ 5,220,210

Depreciation and amortization expense for the years ended December 31, 2013 and 2012 was $1,945,946 and $2,144,184, respectively.

4 Line of Credit

The Corporation has a line of credit with a bank that expires in June 2014. The line of credit provides for up to $4,000,000 of availability to be used for working capital needs. The line of credit accrues interest at prime plus 0.5% (3.25% at December 31, 2013 and 2012). Total borrowings under the line of credit may not exceed 70% of the qualified accounts receivable. The line of credit is collateralized by all existing and future assets and subject to a filing under the Uniform Commercial Code. As part of the line of credit agreement, the Corporation was required to maintain $400,000 in a non-interest bearing account with the lender. The $400,000 is classified within cash and cash equivalents on the statements of financial position. There were no borrowings outstanding at December 31, 2013 or 2012. At December 31, 2013 and 2012, the available amount under the line of credit was reduced by open letters of credit totaling $140,736 and $101,236 respectively, which represents security deposits for the Corporation's office lease agreements. Pursuant to the line of credit agreement, the Corporation is required to comply with financial covenants primarily related to minimum net asset requirements.

In connection with the non-revolving credit facility secured on January 13, 2014, the line of credit was amended and restated. As part of the amended and restated line of credit not, the Corporation is no longer required to maintain the $400,000 non-interest bearing account with the lender.

5 Penalty Income

The Corporation received $445,000 and $100,000 of penalty income in 2013 and 2012, respectively, which is temporarily restricted. The penalty income will be utilized in accordance with the timing of the receipt of the income and FERC's requirement for the use of penalty income to reduce assessments. NERC transferred $2,512,500 of penalty income from temporarily restricted net assets to unrestricted net assets during 2013. During 2012, NERC did not transfer any penalty income from temporarily restricted net assets to unrestricted net assets.

6 Regional Assessments Collected in Advance

In addition to Corporation assessments billed to LSEs or designees, a regional assessment is also billed by the Corporation on behalf of the regional entities. The regional assessment is based on approved budgets of the eight regional entities and remitted to the regional entities by the Corporation. There is a credit risk if the Corporation does not collect the assessments from LSEs or designees before the regional assessments are due to the regional entities. However, the risk is minimal since the Corporation has the ability to reassess and rebill in a subsequent period for any uncollected assessments. Regional assessments billed and remitted for 2013 and 2012 were as follows:

For the Year Ended December 31,	2013	2012
Total regional assessments billed to WECC, ERCOT, individual LSE's and designees	**$113,584,703**	$110,280,847
Total regional assessments remitted to regional entities	**(113,480,310)**	(110,147,242)
Billings over remittances	**$ 104,393**	$ 133,605

As of December 31, 2013 and 2012, regional assessments collected in advance and not yet remitted to the regional entities based upon the remittance schedule set forth in the delegation agreements totaled $9,427,293 and $9,614,829, respectively.

7 Deferred Compensation

Agreements and Life Insurance Policies

During 2005, the Council entered into a deferred compensation agreement (the "Deferred Compensation Agreement") with a retiring executive that provided benefits to the individual upon reaching normal retirement age and was payable over a period selected by the retiring employee. Under certain circumstances, benefits were payable to his surviving spouse. The Corporation assumed the liabilities upon merger with the Council effective January 1, 2007. The present value of the estimated liability under the agreement at December 31, 2007 was accrued using a discount rate of 4.91%. The Corporation provided for some of the benefit funding through a variable universal life policy. Effective October 15, 2008, the Deferred Compensation Agreement was superseded by a new agreement. The variable universal life policy used to fund the liability, including the cash surrender value of the policy, was assigned and transferred to the retired executive in January 2009. In accordance with the new agreement, the Corporation will continue to pay the policy premiums through 2014. At December 31, 2013 and 2012, the present value of the unfunded liability, using a discount rate of 0.75% was $14,257 and $38,968, respectively. The present value of the unfunded liability as of December 31, 2013 is included in current deferred compensation on the statements of financial position. As of December 31, 2012, $24,712 and $14,257 of the present value of the unfunded liability is included in current and non-current deferred compensation, respectively.

On October 15, 2008, the Corporation entered into various Executive Benefit Agreements (the "Agreements") with certain executives and the aforementioned retired executive. The Agreements supersede and replace all previous written or oral agreements between the Corporation and these executives. In accordance with the Agreements, while employed by the Corporation, the executives shall be provided with life insurance coverage, through individual and/or group policies, providing a death benefit equal to the lesser of three times base salary or $500,000, or three times base salary depending upon the executives' employment date. The executives agreed to issue split dollar endorsement agreements with respect to such policies. The executives retired from the Corporation in 2013, and in accordance with the Agreements, ownership of the policies, including the cash surrender value, transferred to the executives within 60 days following termination of employment. The Corporation paid and expensed all the premiums that were due on these policies in 2013, prior to transfer of ownership. When ownership of the policies transferred, the asset and deferred compensation balances on the statements of financial position were written off. At December 31, 2013 and 2012, the cash surrender value of all remaining policies was $0 and $337,414, respectively.

Deferred Compensation Plan

The Corporation established a deferred compensation plan in 2012 in accordance with Internal Revenue Code Section 457 for certain employees, as defined. The plan provides that eligible employees may make elective salary reduction contributions in accordance with limitations established by the Internal Revenue Code. The asset and liability for this deferred compensation plan of $320,660 and $118,243 at December 31, 2013 and 2012, respectively, are included in 457b Plan Assets and non-current deferred compensation on the statements of financial position.

Retiree Medical Benefits

Effective September 1, 2007, the board of trustees approved and adopted a policy to provide medical coverage for a very limited number of current retirees and any and all dependents and transition retirees and any and all dependents, as defined by the board resolution, up to a maximum monthly benefit of $550 paid directly to the applicable insurer. Assumptions used in recording the retiree medical benefits included the 2009 Social Security Administration Actuarial Period Life Table, annual inflation rate of 1.5% and discount rate of 3.8%. At December 31, 2013 and 2012 the accrued retiree medical benefits liability was $276,855 and $241,394, respectively, and is included in non-current deferred compensation on the statements of financial position. The retiree medical expense related to this policy was $26,616 and $22,170, respectively for the years ended December 31, 2013 and 2012.

8 Commitments

Operating Leases

The Corporation leases office space in Washington, D.C. and Atlanta, Georgia under non-cancellable lease agreements, with expiration dates through 2022. The lease for office space in Princeton, NJ expired in 2013.

In 2012, the Corporation entered into an agreement to expand the amount of leased space in Atlanta, Georgia with an expiration date in 2022, which is coterminous with the term of the lease for the original premises.

In 2011, the Corporation entered into separate sub-lease agreements for a portion of the office space in Princeton, New Jersey, which expired in 2013, and for one of the two locations in Washington D.C., with an expiration date of February 2017. As indicated in Note 2, in April 2014, management became aware that the sub-leasee filed for Chapter 11 bankruptcy, but the full impact of the event is not known at this time.

Approximate future minimum payments on office lease space, net of rental income for sub-leased space, at December 31, 2013, for the next five years are as follows:

Years Ending December 31,	Leased Space	Sub-leased Space	Net
2014	$ 2,966,000	$ (276,000)	$ 2,690,000
2015	3,044,000	(286,000)	2,758,000
2016	3,123,000	(248,000)	2,875,000
2017	2,923,000	(50,000)	2,873,000
2018	2,939,000	-	2,939,000
Thereafter	11,490,000	-	11,490,000
	$ 26,485,000	$ (860,000)	$ 25,625,000

The office leases are subject to escalation clauses covering increases in real estate taxes and operating costs over the base year. The Corporation has received tenant improvement allowances as of December 31, 2013 and 2012 totaling $381,632 and $2,256,634, respectively. The difference between rent expense calculated ratably over the lease term and rent paid according to the lease is recorded as a deferred rent obligation on the statement of financial position in the amount of $3,999,899 and $3,741,537 at December 31, 2013 and 2012, respectively.

Office rent expense, net of sub-lease income of $293,000 and $314,080, was $2,574,909 and $2,508,580 for the years ended December 31, 2013 and 2012, respectively.

In April, 2014, management became aware that the sub-tenant under the Washington, D.C. lease filed for Chapter 11 bankruptcy, but the full impact of the event is not known at this time.

Capital Leases

The Corporation has entered into a capital lease agreements for office equipment. Depreciation expense related to these capital leases was $65,407 for each of the years ended December 31, 2013 and 2012.

Assets leased by the Corporation under capital leases are included in fixed assets and capital lease obligation on the statements of financial position and consisted of the following:

December 31, 2013	
Copier leases	$ 196,221
Accumulated depreciation	(150,837)
Net Book Value	$ 45,384

The following is a schedule of future minimum lease payments under these capital leases, together with the future obligation net of interest and maintenance as of December 31, 2013:

Years ending December 31,	Future Minimum Payments
2014	$ 56,697
Less: Amounts representing interest and maintenance	(9,589)
Future Obligation net of Interest and Maintenance	$ 47,108

Contractual Commitments

The Corporation has software license, maintenance support and data management service agreements with varying expiration dates through 2017. The following table is a schedule of future commitments under the terms of the agreements:

Years ending December 31,		Future Minimum Payments
2014	$	196,000
2015		192,000
2016		197,000
2017		51,000
Total Service Agreements	$	636,000

9 Savings and Investment Plan

The Corporation sponsors an employee savings 401(k) plan (the "Plan") whereby eligible participating employees may elect to contribute up to the Internal Revenue Service Code 402(g) (1) limit. The Corporation contributes a 75% match of the participant's elective contribution, provided that the elective contribution does not exceed 6% of eligible compensation. The Corporation also makes a discretionary contribution equal to a percentage of the eligible compensation of all qualifying participants. The additional discretionary contributions are determined annually by the Board of Trustees and are subject to the limitation imposed by the Internal Revenue Service Code 401(a) (17). The Corporation's expenses related to the Plan for the years ended December 31, 2013 and 2012 were $2,252,973 and $1,793,528, respectively. The contributions accrued as of December 31, 2013 and 2012 amounted to $1,788,624 and $1,409,548, respectively, and are included in accrued retirement liabilities in the statements of financial position.

10 Concentration of Credit Risk

The Corporation receives a significant portion of its income from assessments, based upon "net energy for load", to LSEs within the eight regions which are located throughout the United States of America, Canada and a portion of Baja California, Norte, Mexico. LSEs are assessed a proportional share of the Corporation's operating budget as well as a proportional share of the operating budget of the regional entity in whose territory the LSE is located. The Corporation issues quarterly invoices directly to LSEs or, in some circumstances, designees. With respect to LSEs located within Texas Reliability Entity ("TRE"), the Corporation issues a quarterly invoice to Electric Reliability Council of Texas ("ERCOT") which then issues invoices to the LSEs in its region, collects the assessments and remits the funds to the Corporation. The Corporation then remits the regional assessments to TRE. A similar arrangement exists with respect to LSEs located within the Western Electricity Coordinating Council ("WECC"). For LSEs located within the PJM Interconnection ("PJM"), the Corporation issues invoices to PJM which issues invoices to the LSEs, collects the assessments and remits the funds to the Corporation. The Corporation then forwards the regional assessment to Reliability First Corporation ("RFC"), the regional entity. The Corporation is extending credit to the LSEs and designees and is exposed to credit risk to the extent regional assessments are paid by the Corporation to the regional entities prior to collecting assessments from the LSEs or designees. Based on past history, the Corporation believes that the risk of its trade accounts receivable credit exposure is limited.

11 Functional Classification

The Corporation is required to provide information about expenses reported by their functional classification, which is a method of grouping expenses according to the purpose for which costs are incurred. The Corporation groups expenses by operational programs and by administrative programs as defined by FERC.

The following table shows the functional classification of expenses for the years ended December 31, 2013 and 2012:

For the Years Ended December 31,	2013	2012
Operational Programs:		
Reliability Standards	**$ 5,429,867**	$ 4,392,836
Compliance and Organization Registration Certification	**9,404,714**	9,352,528
Reliability Assessment and Performance Analysis	**4,506,619**	4,648,251
Training and Education	**1,696,223**	2,055,853
Situation Awareness and Infrastructure Security	**8,701,517**	9,815,542
	29,738,940	30,265,010
Administrative Programs:		
General & Administrative	**8,656,304**	7,736,048
Legal and Regulatory	**4,046,516**	4,093,557
Information Technology	**7,815,620**	7,211,151
Human Resources	**1,318,387**	1,456,847
Finance and Accounting	**2,771,726**	2,091,487
	24,608,553	22,589,090
Total Expenses	**$ 54,347,493**	$ 52,854,100

Supplemental Schedules of Expenses

For the Years Ended December 31,	2013	2012
Employee costs:		
Payroll taxes (FICA, SUI, FUI, Medicare)	**$ 1,527,728**	$ 1,417,838
Employee benefits - medical	**2,053,703**	1,961,176
Employee benefits - life / disability	**173,915**	169,987
Employee benefits - officers' life	**33,328**	53,188
Insurance - workers' compensation	**54,219**	64,697
Relocation expenses	**149,215**	201,182
Educational	**402,958**	228,433
	$ 4,395,066	$ 4,096,501
Travel and meetings:		
Meetings	**$ 741,766**	$ 569,258
Workshops	**363,969**	490,591
Travel	**2,001,968**	2,268,587
On-line meetings	**306,603**	287,586
	$ 3,414,306	$ 3,616,022

Supplemental Schedules of Expenses (continued)

For the Years Ended December 31,	2013	2012
Services:		
Insurance - commercial	**$ 109,765**	$ 125,932
Contract and consultants	**8,293,693**	9,429,191
Independent trustee fees	**931,250**	970,000
Search fees	**6,495**	160,314
Temporary office services and agency fees	**180,924**	62,749
Accounting and auditing fees	**143,271**	39,926
Legal fees	**845,602**	1,031,825
	$ 10,511,000	$ 11,819,937
Office costs:		
Publications and subscriptions	**$ 76,993**	$ 43,075
Dues	**40,862**	46,079
Postage	**8,022**	14,007
UPS, express mail, etc.	**29,509**	42,202
Telephone	**517,740**	585,469
Office and equipment repair/services	**86,810**	83,775
Copying	**44,720**	21,754
Stationery and office forms	**176**	1,380
Office supplies	**187,170**	177,589
Bank charges	**22,967**	23,392
Sales and use tax	**3,782**	17,935
Card fees	**81,782**	84,058
Internet expenses	**522,100**	688,891
	$ 1,622,635	$ 1,829,606

ATTACHMENT 2

2013 ACTUAL COST-TO-BUDGET COMPARISON

AND

2013 AUDITED FINANCIAL REPORT

FOR

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.

FRCC
Florida Reliability Coordinating Council, Inc.

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.
3000 BAYPORT DRIVE, SUITE 600
TAMPA, FLORIDA 33607-8411
PHONE 813.289.5644 • FAX 813.289.5646
WWW.FRCC.COM

True Up 2013
2013 Budget Variance Explanations Based on Audited Financials

Statutory Funding

Total Funding – Favorable Variance $10k:

Revenue associated with the System Operator Seminars (SOS) (which is self funding) and Maintenance Pass-through expenses were greater than budgeted. Because these are pass through items, expenses will be up by the same amount.

Statutory Expenditures

Total Favorable Variance $668k

Statutory Personnel Expenses

Total Favorable Variance $625k

Replacement positions were filled later than budgeted and two additional positions that were budgeted were unfilled. The savings were partially offset by relocation expenses being expended (none were budgeted), staff educational costs being budgeted as travel but expensed as educational benefit (these will be budgeted and expensed as educational benefits going forward) and a contract programmer being utilized that will be converted to one of the open positions.

The FTE status by Program is:

Reliability Standards Development	**(0.64)**
Compliance Enforcement	**(1.11)**
Reliability Assessment	**(1.07)**
Training & Education	**(0.51)**
Situational Awareness	**(0.20)**
General Administrative	**(0.67)**
Total Statutory FTE Variance	**(4.20)**

Statutory Meeting Expenses

Total Favorable Variance $90k

Travel costs were less than budgeted: Compliance $54k less and other program areas with the remainder. **Favorable Variance $88k**

Conference Calls costs were less than budgeted **Favorable Variance $5k**

Meal costs for Compliance meetings have been greater than anticipated. **Unfavorable Variance $3k**

Statutory Operating Expenses

Total Favorable Variance $96k

Legal fees less than budgeted	-$129k
Office rent allocation miscalculation	-$59k
Reliability Assessment Contract & Consultant expenses	-$42k

(Gas Supply Study & working group projects postponed or not billed)

General Office Costs (Postage, Supplies)	-$39k
Telephone & Internet costs less than budgeted	-$20k
Training & Education Program (Speakers less than budgeted)	-$17k
CEA(SERC) expenses	+$100k
(2014 RC audit moved to 2013 and increased enforcement costs)	
Compliance Software maintenance not budgeted	+$78k
Reliability Assessment Software greater than budgeted	+$32k

Statutory Fixed Asset Expenditures

Total Unfavorable Variance $143k:

Office space build out, furniture and equipment	+$58k
Capitalized Compliance software greater than budgeted	+$110k
New Building Space Deposit timing difference	-$25k

Non Statutory (Member Services) Funding:

Total Funding – Unfavorable Variance $65k:

Pass through billing to members for the FRCCnet Sprint MPLS network is less than expected. Because this is a pass through item, it will affect the expenses by the same amount.

Total Unfavorable Variance $19k

Non Pension Postretirement Benefit Loss unbudgeted **Total Unfavorable Variance $46k**

Non Statutory Expenditures

Total Unfavorable Variance $154k

Non Statutory Personnel Expenses

Total Unfavorable Variance $102k

Operations -

Reliability Coordinator –Less shared employee time spent on Training and Situational Awareness (both Statutory Functions) than budgeted resulting in more time charged to non-statutory. **+.68 FTE** **Total Unfavorable Variance $128k**

Non RC Operations – Relocation for budgeted addition to staff was expended but not budgeted for in 2013. **(.07) FTE** **Total Unfavorable Variance $13k**

Planning - Programming staff that was budgeted for working on Planning Department projects was not hired as of 3rd quarter end. **(.16) FTE** **Total Favorable Variance $39k**

Non Statutory Meeting Expenses

Total Favorable Variance $32k

Operations

Reliability Coordinator – Travel Costs are less than budgeted -$25k offset by meeting expenses and conference call costs +$8k **Total Favorable Variance $17k**

Non RC Operations – Travel costs and conference calls are down -$17k offset by meeting expenses greater than budgeted by +$3k **Total Favorable Variance $14k**

Planning - Travel costs and conference calls less than budgeted -$7k offset by meeting expenses greater than budgeted by +$6k **Total Favorable Variance $1k**

Non Statutory Operating Expenses

Total Favorable Variance $442k

Operations -

Reliability Coordinator –	
Legal Fees for RC less than budget	-$176k
FTMS & OPWG/ATC Case Conversion delay	-$110k
RC Agent Expenses	-$101k
(EMS changes & Visualization Flow project delay & less infrastructure)	
Restoration Drill Consultant delay	-$50k
FTMS less than budget	-$14k
Contingent Liability per GAAP	+$75k
IDC processing unbudgeted	+$57k
Allocated Rent miscalculation	+$26k
Office Costs (supplies, telephone, printing)	+$7k

Total Favorable Variance $286k

Non RC Operations –	
Fuel Reliability Working Group Study delay	-$37k
GMD Vulnerability Study cancelled	-$30k
Security Assessment of FRCCNet delay	-$20k
Telecommunications (including FRCCnet Sprint MPLS network) costs less than budgeted	-$18k
Legal Fees for Non RC less than budget	-$18k
CIP Seminar at FRCC offices instead of hotel & NERC paid for meals	-$12k
Allocated Rent miscalculation	+$8k
Software Maintenance Agreements greater than anticipated	+$8k

Total Favorable Variance $119k

Planning - Certain studies and projects were budgeted to be billed by various members but they have not billed and are not expected to bill for their services. Additionally, legal costs were budgeted that did not occur.

Total Favorable Variance $37k

Non Statutory Fixed Asset Expenditures

Total Unfavorable Variance $6k

Office space build out, furniture and equipment	+$81k
New Building Space Deposit timing difference	-$75k

Other Non-Operating Expenses

Total Unfavorable Variance $520k

Change in Non Pension, Non Cash Post Retirement Obligation of medical insurance to a limited number of grandfathered individuals from actuarial study unbudgeted

Change in Working Capital for the Year ended 12/31/2013:

Addition to Working Capital **$867k**

Statutory – Addition to Working Capital $520k

Member Services Non Statutory – Addition to Working Capital of $347k

Total Net Assets As Of 12/31/2013: Surplus **$2,554k**

Statutory –Surplus of $1,967k

Member Services Non Statutory – Surplus of $ 587k

Statements Concerning Work Completed in 2013:

Compliance Monitoring & Enforcement Program

Although there was significant surplus, the FRCC did complete all work as scheduled for 2013. Specifically, the Compliance Department verifies that:

1. All O&P Compliance audits (12) planned for 2013 were completed as scheduled;
2. All CIP Audits (10) planned for 2013 were completed as scheduled;
3. No Spot Checks were scheduled for 2013; however, the TFE Part-B reviews were conducted under the Spot Check monitoring process.
4. Part A-CIP reviews were completed for all fifty-two (52) TFEs submitted in 2013 per the ROP Appendix 4D and under the new Rule of procedure (18) review/approvals between September 3 and December 31, 2013;
5. Part B-reviews for fifty-two (52) TFEs were completed in 2013 and fifty-one (51) were completed within the one year rule per the ROP Appendix 4D and under the new Rule of procedure (18) approvals between September 3 and December 31, 2013;
6. The annual self-certification of all registered entities in the region was completed on schedule;
7. Review, acceptance or rejection was completed for ninety-one (91) Mitigation Plans submitted by registered entities in 2013 and 2012;
8. Verification of entity completion was finalized for seventy-five (75) Mitigation plans during 2013; and
9. Regional Compliance Assessments were completed for three (3) entity reliability events during 2013.

Reliability Assessment Program

NERC Reliability Assessments (Summer, Winter and Long Term Reliability Assessment) including a Probabilistic Assessment were all completed as scheduled. In addition, the FRCC is supporting the transition to a new Bulk Electric System (BES) definition including assisting with the testing of the new BESnet application, associated training and the development of reference documents to ensure consistent application of the new BES definition and Exception Process throughout NERC.

The FRCC has actively participated in the ERO Events Analysis Process, developed the necessary procedures, and worked with registered entities and NERC to provide meaningful reports and Lessons Learned. FRCC continues to support the NERC Alerts process including the Facility Rating Alert efforts.

Method used to allocate indirect costs to the direct statutory program or functional areas:

The FRCC uses standard cost accounting procedures to allocate general expenses (that cannot be directly assigned) to a specific function. The system used consists of directly expensing as much as possible directly to the function (whether that function is Statutory or Member Services) that incurred the expense. This is accomplished by routing to the responsible departmental heads all invoices pertaining to their job responsibility. The departmental head assigns the functional category and returns the invoice to accounting who assigns the General Ledger Account Number (as specified in the FRCC Accounting Policy Manual – Coding of Invoices for Goods and Services). If the expense cannot be directly charged to a particular function (example rent, payroll taxes, benefits, general office supplies, etc.), the expense is charged to holding accounts by chart of accounts line item to be allocated back to the program areas (to include General & Administrative) at the end of the month. This is done by using the monthly time accounting summarization of FTE by function. So there are two ways expenses are charged to a particular function, either by direct expense or by allocation from the results of the monthly time accounting summarization of FTE by function (including General & Administrative).

The monthly time accounting summarization of FTE by function is calculated using the time sheets that each employee is required to turn in to HR bi-weekly. Each employee allocates eight (8) hours per day to the functions they worked on that day. Their time sheet is reviewed by their departmental head and initialled bi-weekly.

Employees are categorized into 2 groups: Technical Employees – those employees who work directly on functions and have little or no administrative duties (examples would be the Compliance staff and the Engineers) and Non-Technical Staff – those employees who perform support functions that are 80% or greater nonspecific definable by function (examples would be the Accounting staff, the President, the receptionist, etc.). The time from the time sheets are entered into a macro (by employee and function worked on) for the corresponding month being accounted for. The FTE's by program are then calculated and used to allocate the total of the General & Administrative Department back to the program areas on the line "Miscellaneous".

Cash Reserves Statement

No Cash Reserves were used by the FRCC in 2013.

Statement concerning the use of Statutory Funds for Member Services Expenses:

No Statutory Funds were used to pay for Member Services Functions in 2013 and no Member Services Funds were used to pay for Statutory Functions.

Florida Reliability Coordinating Council, Inc.
2013 Statement of Activities and Capital Expenditures Based on Audited
TOTAL COMPANY
For the Year Ended 12/31/2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%
Funding				
ERO Funding				
ERO Assessments	$ 5,957,970	$ 5,957,971	$ (1)	
Penalty Sanctions	304,500	304,500	-	
Total ERO Funding	$ 6,262,470	$ 6,262,471	$ (1)	$ -
Membership Dues	$ 6,250,976	$ 6,250,975	1	
Testing Fees	-	-	-	
Services & Software	314,641	333,000	(18,359)	
Workshops	99,385	90,000	9,385	
Interest	-	-	-	
Special Assessment	(45,824)	-	(45,824)	
Total Funding	**$ 12,881,648**	**$ 12,936,446**	**$ (54,798)**	-0.4%
Expenses				
Personnel Expenses				
Salaries	$ 5,174,009	$ 5,569,794	(395,785)	
Payroll Taxes	314,794	358,291	(43,497)	
Benefits	783,735	770,937	12,798	
Retirement Costs	688,048	784,397	(96,349)	
Total Personnel Expenses	**$ 6,960,586**	**$ 7,483,419**	**$ (522,833)**	-7.0%
Meeting Expenses				
Meetings	$ 115,998	$ 98,669	17,329	
Travel	182,644	310,787	(128,143)	
Conference Calls	31,301	42,543	(11,242)	
Total Meeting Expenses	**$ 329,943**	**$ 451,999**	**$ (122,056)**	-27.0%
Operating Expenses				
Consultants & Contracts	$ 3,039,370	$ 3,192,699	(153,329)	
Office Rent	720,244	739,044	(18,800)	
Office Costs	573,638	696,392	(122,754)	
Professional Services	83,668	422,504	(338,836)	
Miscellaneous	75,000	-	75,000	
Depreciation	138,050	117,390	20,660	
Total Operating Expenses	**$ 4,629,970**	**$ 5,168,029**	**$ (538,059)**	-10.4%
Total Indirect Expenses	**$ -**	**$ -**	**$ -**	
Other Non-Operating Expenses	**$ 519,831**	**$ -**	**$ 519,831**	
Total Expenses	**$ 12,440,330**	**$ 13,103,447**	**$ (663,117)**	-5.1%
Change in Assets	**$ 441,318**	**$ (167,001)**	**$ 608,319**	-100.0%
Fixed Asset Expenditures				
Depreciation	$ (138,050)	$ (117,390)	$ (20,660)	
Non Pension Post Retir Obligat	$ (565,655)	$ -	(565,655)	
Software CapEx	109,556	25,000	84,556	
Furniture & Fixtures CapEx	27,000	-	27,000	
Equipment & Computers CapE	86,327	4,239	82,088	
Leasehold Improvements	55,137	78,461	(23,324)	
Increase/(Decrease) in Fixed Assets	**$ (425,685)**	**$ (9,690)**	**$ (415,995)**	100.0%
Total Budget	**$ 12,014,645**	**$ 13,093,757**	**$ (1,079,112)**	-8.2%
CHANGE IN WORKING CAPITAI	**$ 867,003**	**$ (157,311)**	**$ 1,024,314**	100.0%
FTEs	41.07	44.82	(3.75)	

Florida Reliability Coordinating Council, Inc.
2013 Statement of Activities and Capital Expenditures Based on Audited
TOTAL STATUTORY ONLY
For the Year Ended 12/31/2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%
Funding				
ERO Funding				
ERO Assessments	$ 5,957,970	$ 5,957,971	$ (1)	
Penalty Sanctions	304,500	304,500	-	
Total ERO Funding	$ 6,262,470	$ 6,262,471	$ (1)	
Membership Dues	-	-	-	
Testing Fees	-	-	-	
Services & Software	22,650	22,000	650	
Workshops	99,385	90,000	9,385	
Interest	-	-	-	
Miscellaneous	-	-	-	
Total Funding	**$ 6,384,505**	**$ 6,374,471**	**$ 10,034**	0.2%
Expenses				
Personnel Expenses				
Salaries	$ 3,286,539	$ 3,741,113	$ (454,574)	
Payroll Taxes	201,113	240,656	(39,543)	
Benefits	489,334	533,629	(44,295)	
Retirement Costs	440,672	526,863	(86,191)	
Total Personnel Expenses	**$ 4,417,658**	**$ 5,042,261**	**$ (624,603)**	-12.4%
Meeting Expenses				
Meetings	$ 86,452	$ 83,259	$ 3,193	
Travel	144,350	232,363	(88,013)	
Conference Calls	14,301	19,347	(5,046)	
Total Meeting Expenses	**$ 245,103**	**$ 334,969**	**$ (89,866)**	-26.8%
Operating Expenses				
Consultants & Contracts	$ 336,548	$ 176,977	$ 159,571	
Office Rent	513,094	572,285	(59,191)	
Office Costs	113,063	199,513	(86,450)	
Professional Services	47,831	176,538	(128,707)	
Miscellaneous	-	-	-	
Depreciation	112,023	93,493	18,530	
Total Operating Expenses	**$ 1,122,559**	**$ 1,218,806**	**$ (96,247)**	-7.9%
Total Indirect Expenses	**$ -**	**$ -**	**$ -**	
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	
Total Expenses	**$ 5,785,320**	**$ 6,596,036**	**$ (810,716)**	-12.3%
Change in Assets	**$ 599,185**	**$ (221,565)**	**$ 820,750**	**-370.4%**
Fixed Asset Expenditures				
Depreciation	$ (112,023)	$ (93,493)	$ (18,530)	
Software CapEx	109,556	25,000	84,556	
Furniture & Fixtures CapEx	-	-	-	
Equipment & Computers CapEx	81,445	4,239	77,206	
Leasehold Improvements	-	-	-	
Increase/(Decrease) in Fixed Assets	**$ 78,978**	**$ (64,254)**	**$ 143,232**	-222.9%
Total Budget	**$ 5,864,298**	**$ 6,531,782**	**$ (667,484)**	-10.2%
CHANGE IN WORKING CAPITAL	**$ 520,207**	**$ (157,311)**	**$ 677,518**	**-430.7%**
FTEs	25.91	30.11	(4.20)	
Beginning Working Capital 1/1/2013	1,367,703	483,900	883,803	
Change in Working Capital	520,207	(157,311)	677,518	
Working Capital at 12/31/2013	1,887,910	326,589	1,561,321	

Florida Reliability Coordinating Council, Inc.
2013 Statement of Activities and Capital Expenditures Based on Audited
RELIABILITY STANDARDS
For the Year Ended 12/31/2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%	Comments (Explain Variances >+/- 10% and >$10,000
Funding					
ERO Funding					
ERO Assessments	$ 381,624	$ 381,622	$ 2		
Penalty Sanctions	19,053	19,053	-		
Total ERO Funding	$ 400,677	$ 400,675	$ 2		
Membership Dues		$ -	-		
Testing Fees		-	-		
Services & Software			-		
Workshops			-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding	$ 400,677	$ 400,675	$ 2	0.0%	
Expenses					
Personnel Expenses					
Salaries	120,361	$ 204,940	(84,579)		1 Position not needed due to delay of the BES implementation
Payroll Taxes	7,613	13,183	(5,570)		Effect of 1 Position not hired
Benefits	17,108	34,059	(16,951)		Effect of 1 Position not hired
Retirement Costs	15,984	28,862	(12,878)		Effect of 1 Position not hired
Total Personnel Expenses	$ 161,066	$ 281,044	$ (119,978)	-42.7%	
Meeting Expenses					
Meetings	$ 876	$ 1,002	(126)		
Travel	17,823	35,721	(17,898)		1 Position not needed due to delay of the BES implementation
Conference Calls	720	767	(47)		
Total Meeting Expenses	$ 19,419	$ 37,490	$ (18,071)	-48.2%	
Operating Expenses					
Consultants & Contracts	$ 1,226	$ -	1,226		
Office Rent	12,837	18,690	(5,853)		New Space reallocated from budget
Office Costs	4,357	9,136	(4,779)		Effect of 1 Position not hired
Professional Services	1,785	12,134	(10,349)		Legal Fees for BES did not materialize
Miscellaneous			-		
Depreciation	890	1,342	(452)		
Total Operating Expenses	$ 21,095	$ 41,302	$ (20,207)	-48.9%	
Total Indirect Expenses	$ 27,565	$ 41,958	$ (14,393)	-34.3%	
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	$ 229,145	$ 401,794	$ (172,649)	-43.0%	
Change in Assets	$ 171,532	$ (1,119)	$ 172,651	100.0%	
Fixed Asset Expenditures					
Depreciation	$ (890)	$ (1,342)	$ 452		
Software CapEx			-		
Furniture & Fixtures CapEx			-		
Equipment & Computers CapE	3,646	223	3,423		
Leasehold Improvements			-		
Increase/(Decrease) in Fixed Assets	$ 2,756	$ (1,119)	$ 3,875	-346.3%	
Total Budget	$ 231,901	$ 400,675	$ (168,774)	-42.1%	
CHANGE IN WORKING CAPITAI	$ 168,776	$ -	$ 168,776		
Direct FTEs	1.01	1.65	(0.64)	-38.8%	
Indirect FTE's	0.14	0.41	(0.27)	-65.9%	
Total FTE's	1.15	2.06	(0.91)	-44.2%	

Florida Reliability Coordinating Council, Inc.
2013 Statement of Activities and Capital Expenditures Based on Audited
COMPLIANCE
For the Year Ended 12/31/2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%	Comments (Explain Variances >+/- 10% and >$10,000
Funding					
ERO Funding					
ERO Assessments	$ 4,082,506	$ 4,082,511	$ (5)		
Penalty Sanctions	207,042	207,042	-		
Total ERO Funding	$ 4,289,548	$ 4,289,553	$ (5)		
Membership Dues	-	$ -	-		
Testing Fees			-		
Services & Software			-		
Workshops			-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding	$ 4,289,548	$ 4,289,553	$ (5)	0.0%	
Expenses					
Personnel Expenses					
Salaries	$ 2,091,678	$ 2,227,031	(135,353)		
Payroll Taxes	126,418	143,260	(16,842)		
Benefits	332,710	321,490	11,220		
Retirement Costs	282,634	313,634	(31,000)		
Total Personnel Expenses	$ 2,833,440	$ 3,005,415	$ (171,975)	-5.7%	
Meeting Expenses					
Meetings	$ 12,154	$ 6,501	5,653		
Travel	76,991	131,336	(54,345)		Cost of Travel Less than anticipated & Travel for Staff Training charged to Personnel Expense
Conference Calls	9,324	3,285	6,039		
Total Meeting Expenses	$ 98,469	$ 141,122	$ (42,653)	-30.2%	
Operating Expenses					
Consultants & Contracts	$ 195,037	$ 16,800	178,237		
Office Rent	385,183	434,212	(49,029)		
Office Costs	72,858	91,091	(18,233)		
Professional Services	34,604	117,809	(83,205)		
Miscellaneous			-		
Depreciation	102,321	80,918	21,403		
Total Operating Expenses	$ 790,003	$ 740,830	$ 49,173	6.6%	
Total Indirect Expenses	$ 448,796	$ 455,943	$ (7,147)	-1.6%	
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	$ 4,170,708	$ 4,343,310	$ (172,602)	-4.0%	
Change in Assets	$ 118,840	$ (53,757)	$ 172,597		
Fixed Asset Expenditures					
Depreciation	$ (102,321)	$ (80,918)	$ (21,403)		
Software CapEx	109,556	25,000	84,556		Guidance Software Enhancements greater than anticipated
Furniture & Fixtures CapEx			-		
Equipment & Computers CapE	57,343	2,161	55,182		Budgeted for in 2012; Actual in 2013
Leasehold Improvements			-		
Increase/(Decrease) in Fixed Assets	$ 64,578	$ (53,757)	$ 118,335		
Total Budget	$ 4,235,286	$ 4,289,553	$ (54,267)	-1.3%	
CHANGE IN WORKING CAPITAL	$ 54,262	$ -	$ 54,262		
Direct FTEs	16.82	17.93	(1.11)	-6.2%	
Indirect FTE's	2.26	2.17	0.09	4.1%	
Total FTE's	19.08	20.10	(1.02)	-5.1%	

Florida Reliability Coordinating Council, Inc.
2013 Statement of Activities and Capital Expenditures Based on Audited
RELIABILITY ASSESSMENT
For the Year Ended 12/31/2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%	Comments (Explain Variances >+/- 10% and >$10,000
Funding					
ERO Funding					
ERO Assessments	$ 1,314,299	$ 1,314,299	$ -		
Penalty Sanctions	62,701	62,701	-		
Total ERO Funding	$ 1,377,000	$ 1,377,000	$ -		
Membership Dues	-	$ -	-		
Testing Fees		-	-		
Services & Software	22,650	22,000	650		
Workshops			-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding	$ 1,399,650	$ 1,399,000	$ 650	0.0%	
Expenses					
Personnel Expenses					
Salaries	$ 555,631	$ 674,444	(118,813)		FTE's are less by 1.4 due to delay of BES Implementation
Payroll Taxes	34,375	43,385	(9,010)		Result of 1.4 fewer FTE's
Benefits	78,830	97,086	(18,256)		Result of 1.4 fewer FTE's
Retirement Costs	73,102	94,982	(21,880)		Result of 1.4 fewer FTE's
Total Personnel Expenses	$ 741,938	$ 909,897	$ (167,959)	-18.5%	
Meeting Expenses					
Meetings	$ 3,021	$ 4,810	(1,789)		Delay of BES Implementation
Travel	45,477	49,865	(4,388)		Result of 1.4 fewer FTE's
Conference Calls	3,309	10,387	(7,078)		Delay of BES Implementation
Total Meeting Expenses	$ 51,807	$ 65,062	$ (13,255)	-20.4%	
Operating Expenses					
Consultants & Contracts	$ 105,426	$ 115,177	$ (9,751)		
Office Rent	59,663	61,504	(1,841)		New Space reallocated from budget
Office Costs	17,254	71,379	(54,125)		New Space reallocated from budget
Professional Services	10,055	37,218	(27,163)		Legal Fees for BES did not materialize
Miscellaneous			-		
Depreciation	4,066	5,309	(1,243)		
Total Operating Expenses	$ 196,464	$ 290,587	$ (94,123)	-32.4%	
Total Indirect Expenses	$ 119,470	$ 138,080	$ (18,610)	-13.5%	
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	$ 1,109,679	$ 1,403,626	$ (293,947)	-20.9%	
Change in Assets	$ 289,971	$ (4,626)	$ 294,597		
Fixed Asset Expenditures					
Depreciation	$ (4,066)	$ (5,309)	$ 1,243		
Software CapEx			-		
Furniture & Fixtures CapEx			-		
Equipment & Computers CapE	15,566	683	14,883		Budgeted for in 2012; Actual in 2013
Leasehold Improvements			-		
Increase/(Decrease) in Fixed Assets	$ 11,500	$ (4,626)	$ 16,126	-348.6%	
Total Budget	$ 1,121,179	$ 1,399,000	$ (277,821)	-19.9%	
CHANGE IN WORKING CAPITAL	$ 278,471	$ -	$ 278,471		
Direct FTEs	4.36	5.43	(1.07)	-19.7%	
Indirect FTE's	0.59	0.92	(0.33)	-35.9%	
Total FTE's	4.95	6.35	(1.40)	-22.0%	

Florida Reliability Coordinating Council, Inc.
2013 Statement of Activities and Capital Expenditures Based on Audited
TRAINING AND EDUCATION
For the Year Ended 12/31/2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%	Comments (Explain Variances >+/- 10% and >$10,000
Funding					
ERO Funding					
ERO Assessments	$ 276,132	$ 276,136	$ (4)		
Penalty Sanctions	12,817	12,817	-		
Total ERO Funding	$ 288,949	$ 288,953	$ (4)		
Membership Dues	-	$ -	-		
Testing Fees		-	-		
Services & Software			-		
Workshops	99,385	90,000	9,385		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding	$ 388,334	$ 378,953	$ 9,381	2.5%	
Expenses					
Personnel Expenses					
Salaries	$ 85,084	$ 137,870	(52,786)		Less time by staff was necessary to prep and conduct seminars
Payroll Taxes	5,417	8,869	(3,452)		Result of less staff time
Benefits	9,594	18,009	(8,415)		Result of less staff time
Retirement Costs	11,743	19,416	(7,673)		Result of less staff time
Total Personnel Expenses	$ 111,838	$ 184,164	$ (72,326)	-39.3%	
Meeting Expenses					
Meetings	$ 70,380	$ 70,908	(528)		
Travel	3,493	12,228	(8,735)		SOS Seminars were held in Tampa - less travel necessary to attend
Conference Calls	922	4,902	(3,980)		Cost of Webinars were less than anticipated
Total Meeting Expenses	$ 74,795	$ 88,038	$ (13,243)	-15.0%	
Operating Expenses					
Consultants & Contracts	$ 28,500	$ 45,000	(16,500)		Cost of Seminar Speakers less than anticipated
Office Rent	9,346	12,573	(3,227)		New Space reallocated from budget
Office Costs	13,091	12,312	779		
Professional Services	1,266	7,502	(6,236)		RE Legal Fees less than anticipated
Miscellaneous			-		
Depreciation	757	823	(66)		
Total Operating Expenses	$ 52,960	$ 78,210	$ (25,250)	-32.3%	
Total Indirect Expenses	$ 19,551	$ 28,226	$ (8,675)	-30.7%	
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	$ 259,144	$ 378,638	$ (119,494)	-31.6%	
Change in Assets	$ 129,190	$ 315	$ 128,875		
Fixed Asset Expenditures					
Depreciation	$ (757)	$ (823)	$ 66		
Software CapEx			-		
Furniture & Fixtures CapEx			-		
Equipment & Computers CapE	4,708	1,138	3,570		
Leasehold Improvements			-		
Increase/(Decrease) in Fixed Assets	$ 3,951	$ 315	$ 3,636	1154.3%	
Total Budget	$ 263,095	$ 378,953	$ (115,858)	-30.6%	
CHANGE IN WORKING CAPITAL	$ 125,239	$ -	$ 125,239		
Direct FTEs	0.60	1.11	(0.51)	-45.9%	
Indirect FTE's	0.08	0.17	(0.09)	-52.9%	
Total FTE's	0.68	1.28	(0.60)	-46.9%	

Florida Reliability Coordinating Council, Inc.
2013 Statement of Activities and Capital Expenditures Based on Audited
SITUATIONAL AWARENESS
For the Year Ended 12/31/2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%	Comments (Explain Variances >+/- 10% and >$10,000
Funding					
ERO Funding					
ERO Assessments	$ 60,714	$ 60,714	$ -		
Penalty Sanctions	2,887	2,887	-		
Total ERO Funding	$ 63,601	$ 63,601	$ -		
Membership Dues	-	$ -	-		
Testing Fees		-	-		
Services & Software			-		
Workshops			-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding	$ 63,601	$ 63,601	$ -	0.0%	
Expenses					
Personnel Expenses					
Salaries	$ 6,217	$ 31,052	(24,835)		Less time was spent on Program than anticipated
Payroll Taxes	379	1,997	(1,618)		Result of less time spent
Benefits	805	4,070	(3,265)		Result of less time spent
Retirement Costs	827	4,373	(3,546)		Result of less time spent
Total Personnel Expenses	$ 8,228	$ 41,492	$ (33,264)	-80.2%	
Meeting Expenses					
Meetings	$ 21	$ 38	(17)		
Travel	516	3,213	(2,697)		
Conference Calls	26	6	20		
Total Meeting Expenses	$ 563	$ 3,257	$ (2,694)	-82.7%	
Operating Expenses					
Consultants & Contracts	$ 1,726	$ -	1,726		
Office Rent	714	2,831	(2,117)		
Office Costs	1,550	7,755	(6,205)		
Professional Services	121	1,875	(1,754)		
Miscellaneous			-		
Depreciation	2,428	2,561	(133)		
Total Operating Expenses	$ 6,539	$ 15,022	$ (8,483)	-56.5%	
Total Indirect Expenses	$ 1,313	$ 6,357	$ (5,044)	-79.3%	
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	$ 16,643	$ 66,128	$ (49,485)	-74.8%	
Change in Assets	$ 46,958	$ (2,527)	$ 49,485		
Fixed Asset Expenditures					
Depreciation	$ (2,428)	$ (2,561)	$ 133		
Software CapEx			-		
Furniture & Fixtures CapEx			-		
Equipment & Computers CapE	182	34	148		
Leasehold Improvements			-		
Increase/(Decrease) in Fixed Assets	$ (2,246)	$ (2,527)	$ 281	-11.1%	
Total Budget	$ 14,397	$ 63,601	$ (49,204)	-77.4%	
CHANGE IN WORKING CAPITAL	$ 49,204	$ -	$ 49,204		
Direct FTEs	0.05	0.25	(0.20)	-80.0%	
Indirect FTE's	0.01	0.07	(0.06)	-85.7%	
Total FTE's	0.06	0.32	(0.26)	-81.3%	

Florida Reliability Coordinating Council, Inc.
2013 Statement of Activities and Capital Expenditures Based on Audited
GENERAL ADMINISTRATIVE
For the Year Ended 12/31/2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%	Comments (Explain Variances >+/- 10% and >$10,000
Funding					
ERO Funding					
ERO Assessments	$ (157,305)	$ (157,311)	$ 6		
Penalty Sanctions		-	-		
Total ERO Funding	$ (157,305)	$ (157,311)	$ 6		
Membership Dues	-	$ -	-		
Testing Fees		-	-		
Services & Software			-		
Workshops			-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding	$ (157,305)	$ (157,311)	$ 6	0.0%	
Expenses					
Personnel Expenses					
Salaries	$ 427,568	$ 465,776	$ (38,208)		
Payroll Taxes	26,911	29,962	(3,051)		
Benefits	50,287	58,915	(8,628)		
Retirement Costs	56,382	65,596	(9,214)		
Total Personnel Expenses	$ 561,148	$ 620,249	$ (59,101)	-9.5%	
Meeting Expenses					
Meetings		$ -	$ -		
Travel	50		50		
Conference Calls		-	-		
Total Meeting Expenses	$ 50	$ -	$ 50	#DIV/0!	
Operating Expenses					
Consultants & Contracts	$ 4,633	$ -	$ 4,633		
Office Rent	45,351	42,475	2,876		
Office Costs	3,953	7,840	(3,887)		
Professional Services		-	-		
Miscellaneous			-		
Depreciation	1,561	2,540	(979)		
Total Operating Expenses	$ 55,498	$ 52,855	$ 2,643	5.0%	
Total Indirect Expenses	$ (616,695)	$ (670,564)	$ 53,869		
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	$ 1	$ 2,540	$ (2,539)	-100.0%	
Change in Assets	$ (157,306)	$ (159,851)	$ 2,545	-1.6%	
Fixed Asset Expenditures					
Depreciation	$ (1,561)	$ (2,540)	$ 979		
Software CapEx			-		
Furniture & Fixtures CapEx			-		
Equipment & Computers CapEx			-		
Leasehold Improvements			-		
Increase/(Decrease) in Fixed Assets	$ (1,561)	$ (2,540)	$ 979	-38.5%	
Total Budget	$ (1,560)	$ -	$ (1,560)		
CHANGE IN WORKING CAPITAL	$ (155,745)	$ (157,311)	$ 1,566	-1.0%	
FTEs	3.07	3.74	(0.67)	-17.9%	

Florida Reliability Coordinating Council, Inc.
2013 Statement of Activities and Capital Expenditures Based on Audited
TOTAL MEMBER SERVICES - NON STATUTORY
For the Year Ended 12/31/2013

(In Whole Dollars)

	2013 Actual	2013 Budget	Variance	%	Comments (Explain Variances >+/- 10% and >$10,000
Funding					
ERO Funding					
ERO Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		
Membership Dues	6,250,976	6,250,975	1		
Testing Fees	-	-	-		
Services & Software	291.991	311.000	(19.009)		
Workshops	-	-	-		
Special Assessment	-	-	-		
Non Cash Postretirement	(45.824)	-	(45.824)		
Total Funding	**$ 6,497,143**	**$ 6,561,975**	**$ (64,832)**	-1.0%	
Expenses					
Personnel Expenses					
Salaries	$ 1.887.470	$ 1.828.681	58.789		
Payroll Taxes	113.681	117.635	(3.954)		
Benefits	294.401	237.308	57.093		
Retirement Costs	247.376	257.534	(10.158)		
Total Personnel Expenses	**$ 2,542,928**	**$ 2,441,158**	**$ 101,770**	4.2%	
Meeting Expenses					
Meetings	$ 29.546	$ 15.410	14.136		
Travel	38.294	78.424	(40.130)		Staff Training budgeted in Travel - Actual Charged to Benefits
Conference Calls	17.000	23.196	(6.196)		
Total Meeting Expenses	**$ 84,840**	**$ 117,030**	**$ (32,190)**	-27.5%	
Operating Expenses					
Consultants & Contracts	$ 2.702.822	$ 3.015.722	(312.900)		FTMS & OPWG-ATC case & Restroation Drill delay, RC Agent Expenses
Office Rent	207.150	166.759	40.391		New Space reallocated from budget
Office Costs	460.575	496.879	(36.304)		Telecommunications over budgeted
Professional Services	35.837	245.966	(210.129)		Legal Fees for RC less than budgeted
Miscellaneous	75.000	-	75,000		Accrued Liability per GAAP
Depreciation	26.027	23.897	2,130		
Total Operating Expenses	**$ 3,507,411**	**$ 3,949,223**	**$ (441,812)**	-11.2%	
Total Indirect Expenses					
Other Non-Operating Expenses	**$ 519,831**	**$ -**	**$ 519,831**		
Total Expenses	**$ 6,655,010**	**$ 6,507,411**	**$ 147,599**	2.3%	
Change in Assets	**$ (157,867)**	**$ 54,564**	**$ (212,431)**		
Fixed Asset Expenditures					
Depreciation	$ (26,027)	$ (23,897)	$ (2,130)		
Non Pension Post Retir. Oblig	(565,655)	-	(565,655)		
Software CapEx	27.000	-	27,000		
Furniture & Fixtures CapEx	4.882	-	4,882		
Equipment & Computers CapE	55.137	78.461	(23,324)		
Leasehold Improvements	-	-	-		
Increase/(Decrease) in Fixed Assets	**$ (504,663)**	**$ 54,564**	**$ (559,227)**	-1024.9%	
Total Budget	**$ 6,150,347**	**$ 6,561,975**	**$ (411,628)**	-6.3%	
CHANGE IN WORKING CAPITAL	**$ 346,796**	**$ -**	**$ 346,796**		
FTEs	15.16	14.71	0.45		

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.

FINANCIAL STATEMENTS AND SUPPLEMENTAL SCHEDULES

December 31, 2013

Certified Public Accountants
Business Consultants
Limited Liability Company

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.

TABLE OF CONTENTS

	PAGE
INDEPENDENT AUDITORS' REPORT	1-2
FINANCIAL STATEMENTS	
Statement of Financial Position	3
Statement of Activities	4
Statement of Cash Flows	5
Notes to Financial Statements	6-17
SUPPLEMENTAL INFORMATION	
Total Summary	18
Statutory Summary	19
Statutory By Program	20-25
Non-statutory Summary	26

INDEPENDENT AUDITORS' REPORT

CRI CARR RIGGS & INGRAM

Carr, Riggs & Ingram, LLC
2111 Drew Street
Clearwater, FL 33765

(727) 446-0504
(727) 461-7384 (fax)
www.cricpa.com

INDEPENDENT AUDITORS' REPORT

To the Board of Directors
Florida Reliability Coordinating Council, Inc.

We have audited the accompanying financial statements of Florida Reliability Coordinating Council, Inc., (a nonprofit organization) which comprise the statement of financial position as of December 31, 2013, and the related statements of activities and cash flows for the year then ended, and the related notes to the financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

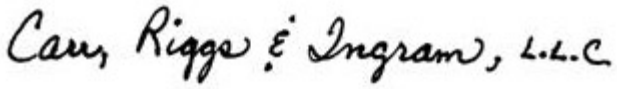
We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the statement of financial position of Florida Reliability Coordinating Council as of December 31, 2013 and the changes in its net assets and its cash flows for the year then ended in accordance with accounting principles generally accepted in the United States of America.

Other Matter

Our audit was conducted for the purpose of forming an opinion on the financial statements as a whole. The statutory and non-statutory schedules on Pages 18 to 26 inclusive are presented for purposes of additional analysis and are not a required part of the financial statements. Such information is the responsibility of management and was derived from and relates directly to the underlying accounting and other records used to prepare the financial statements. The information has been subjected to the auditing procedures applied in the audit of the financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the financial statements or to the financial statements themselves, and other additional procedures in accordance with auditing standards generally accepted in the United States of America. In our opinion, the information is fairly stated in all material respects in relation to the financial statements as a whole.



CARR, RIGGS & INGRAM, LLC
Certified Public Accountants

January 31, 2014

FINANCIAL STATEMENTS

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.

STATEMENT OF FINANCIAL POSITION
December 31, 2013

ASSETS

Current assets:	
Cash	$ 6,558,632
Member receivables	2,835,667
Related party receivable	19,403
Prepaid expenses	18,526
Total current assets	9,432,228
Property and equipment - at cost	
Equipment and computers	560,153
Software	910,964
Furniture and fixtures	317,732
Leasehold improvements	126,636
Total	1,915,485
Less accumulated depreciation and amortization	(1,497,031)
Total property and equipment, net	418,454
Other assets	
Deposits	150,000
457(f) plan	109,175
Total other assets	259,175
Total assets	$ 10,109,857

LIABILITIES AND NET ASSETS

Current liabilities:	
Accounts payable	$ 379,159
Current portion of accrued postretirement benefit obligation	32,914
457(f) plan payable	109,175
Deferred revenue	3,111,955
Compliance penalty assessment	481,000
Accrued expenses	2,067,785
Total current liabilities	6,181,988
Long-term liabilities:	
Accrued postretirement benefit obligation	1,373,908
Net assets:	
Unrestricted statutory - FERC designated	1,966,888
Unrestricted member services - board designated	587,073
Total net assets	2,553,961
Total liabilities and net assets	$ 10,109,857

See Notes to Financial Statements.

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.

STATEMENT OF ACTIVITIES
For the year ended December 31, 2013

Revenues:	
Nonstatutory member assessments	$ 6,250,976
Statutory member assessments	5,957,970
Services and software	314,641
Training and education fees	99,385
Postretirement benefit loss	(45,824)
Gain on 457(f) Plan	22,127
Penalty and sanctions realized	304,500
Total revenue	12,903,775
Expenses:	
Salaries	5,174,009
Payroll taxes	314,794
Employee benefits	783,735
Retirement and deferred compensation plans	688,048
Meetings	115,998
Travel	182,644
Conference calls	31,301
Contracts & consultants	3,039,370
Facilities rental	720,244
Office costs	573,638
Legal and accounting	83,668
Penalty sanctions	75,000
457(f) plan	22,127
Depreciation and amortization	138,050
Total expenses	11,942,626
Increase in net assets before change in accumulated post retirement obligation	961,149
Net periodic change in postretirement obligation	(519,831)
Increase in net assets	441,318
Net assets - beginning of year	2,112,643
Net assets - end of year	$ 2,553,961

See Notes to Financial Statements.

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.

STATEMENT OF CASH FLOWS
For the year ended December 31, 2013

Cash flows from operating activities:	
Cash received from members	$ 12,705,017
Cash paid to suppliers and employees	(10,561,406)
Net cash provided by operating activities	2,143,611
Cash flows from investing activities	
Purchases of software and equipment	(278,020)
Net cash used by investing activities	(278,020)
Net increase in cash	1,865,591
Cash at beginning of year	$ 4,693,041
Cash at end of year	$ 6,558,632
Reconciliation of increase in net assets to net cash used by operating activities	
Increase in net assets	$ 441,318
Adjustments to reconcile increase in net assets to net cash used by operating activities:	
Depreciation and amortization	138,050
Increase in receivables, prepaid expenses, and other assets	(217,496)
Increase in accounts payable and accrued expenses	1,160,116
Change in postretirement benefit obligation	565,655
Increase in deferred income	55,968
Net cash provided by operating activities	$ 2,143,611

See Notes to Financial Statements.

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.

NOTES TO FINANCIAL STATEMENTS
December 31, 2013

1. General and Summary of Significant Accounting Policies

General – Florida Reliability Coordinating Council, Inc. (the "Company") is a group of electric utilities and energy marketers primarily doing business in the State of Florida. The purpose of the Company is to ensure and enhance the reliability and adequacy of the bulk power supply in Florida (which is defined as the general area encompassed by Peninsula Florida) now and into the future. The Company serves as a Regional Entity with delegated authority from the North American Electric Reliability Corporation ("NERC") for the purpose of proposing and enforcing reliability standards within the FRCC region.

On May 2, 2007, the Company entered into a Delegation Agreement with North American Electric Reliability Corporation ("NERC"), an organization certified by the Federal Energy Regulatory Commission pursuant to Section 215(c) of the Federal Power Act. The Company is required by federal law to assess the reliability of the Bulk Power System. The Federal Energy Regulatory Commission ("FERC") empowered the Company through a Delegation Agreement with NERC to monitor, enforce and implement electric reliability standards under Section 215 of the Federal Power Act. The Company is responsible for establishing the process for development, revision, withdrawals and approval of the Company's Regional Reliability Standards for the region. The Company monitors and enforces compliance with NERC and FERC reliability standards through on-site audits, self-certifications, periodic spot checks, self-reports, event investigation, periodic data submittal, exception reporting and through complaints. The initial term of the agreement is for three years and is renewable for five more years upon a successful compliance audit conducted by NERC.

The Company's source of revenue is split into two parts. The statutory functions, defined as those functions being performed for Reliability Standards and Compliance, are funded by NERC. The member services functions are paid by its members who are assessed for costs and expenses of establishing, developing, operating and maintaining the Company.

A summary of the Company's significant accounting policies consistently applied in preparation of the accompanying financial statements follows:

The financial statements have been prepared on the accrual basis of accounting in accordance with accounting principles generally accepted in the United States of America; consequently, revenues and gains are recognized when earned, and expenses and losses are recognized when incurred.

Concentration of Credit Risk – The Company places its cash with high credit quality institutions. At times, these balances may be in excess of the FDIC insurance limit.

Use of Estimates – Management uses estimates and assumptions in preparing these financial statements in accordance with accounting principles generally accepted in the United States of America. Those estimates and assumptions affect the reported amounts of assets, liabilities, revenues and expenses. Actual results could vary from the estimates that are used.

Income Taxes – The Company has been approved for tax-exempt status under Section 501(c) (6) of the Internal Revenue Code and is exempt from federal and state income taxes. Accordingly, no provision for income taxes is included in the financial statements. Tax years after 2009 remain subject to examination by taxing authorities.

1. General and Summary of Significant Accounting Policies (Continued)

The Company follows Accounting Standard Codification (ASC) 740, "Accounting for Income Taxes" with respect to accounting for uncertainty in income taxes. A tax position is recognized as a benefit only if it is "more likely than not" that the tax position would be sustained in a tax examination, with a tax examination being presumed to occur. The amount recognized is the largest amount of tax benefit that is greater than 50% likely of being realized on examination. For tax positions not meeting the "more likely than not" test, no tax benefit is recorded.

Due to its tax-exempt status, the Company is not subject to U.S. federal income tax or state income tax. The Company's Form 990 has not been subject to examination by the Internal Revenue Service or the State of Florida for the last three years. The Company has not recognized liability for unrecognized tax benefits as it has no known tax positions that would subject the Company to any material income tax exposure. A reconciliation of the beginning and ending amount of unrecognized tax benefits and interest accrued related to unrecognized tax benefits are not included nor is there any interest accrued related to unrecognized tax benefits or interest expense and penalties in operating expenses as there are no unrecognized tax benefits.

Member, Related Party, and Other Receivables – The Company considers all receivables to be fully collectible, usually within 30 to 60 days; accordingly, no allowance for doubtful accounts is required and no late fees are assessed. If amounts become uncollectible, they will be charged to operations when that determination is made and will be paid by the remaining members.

Property and Equipment – Property and equipment with a cost over $500 are capitalized and are stated at cost, less accumulated depreciation and amortization. Depreciation and amortization are provided for in amounts sufficient to relate the cost of depreciable assets to operations over their estimated service lives, principally on a straight-line basis. The estimated lives used in determining depreciation are:

Equipment	5 years
Software	3 years
Furniture and fixtures	7 years
Leasehold improvements	5 years

Leasehold improvements are amortized over the lives of the respective leases or the service lives of the improvements, whichever is shorter.

1. General and Summary of Significant Accounting Policies (Continued)

Line of Credit – The Company secured a line of credit from Bank of America, N.A. for two (2) years in the amount of $1,500,000. The line of credit is intended to be used for short term needs that arise between budget funding periods as a bridge between budget years. The covenants call for a funded debt to total unrestricted and temporarily restricted net assets not exceeding 2.0:1.0 and an out of debt period of 30 days each line year. The total charges and fees for 2 year term were paid in 2013 and amounted to $8,095. As of December 31, 2013, the company has not drawn on the line of credit and is in full compliance with all covenants.

Postretirement Benefits Other Than Pensions – The Company sponsors a postretirement health care plan covering employees hired before October 1, 2003 if the retiree completes 10 years of service prior to retirement, is over the age of 60 at retirement and participates in the Company's IRS qualified retirement or profit-sharing plan at the time of retirement. The plan is noncontributory for retirees (see Note 6).

Date of Management's Review – Management has evaluated events and transactions for potential recognition or disclosure through January 31, 2014, which is the date the financial statements were available to be issued.

2. Fair Value Measurements

Financial Accounting Standards Board ASC 820 establishes a framework for measuring fair value. That framework provides a fair value hierarchy that prioritizes the inputs to valuation techniques used to measure fair value. The hierarchy gives the highest priority to unadjusted quoted prices in active markets for identical assets or liabilities (level 1 measurement) and the lowest priority to unobservable inputs (level 3 measurements). The three levels of the fair value hierarchy under FASB ASC 820 are described below:

Level 1: Inputs to the valuation methodology are unadjusted quoted prices for identical assets or liabilities in active markets that the Organization has the ability to access.

Level 2: Inputs to the valuation methodology include:

- Quoted prices for similar assets or liabilities in active markets
- Quoted prices for identical or similar assets or liabilities in inactive markets
- Inputs other than quoted prices that are observable for that asset or liability
- Inputs that are derived principally from or corroborated by observable market data by correlation or other means

If the asset or liability has a specified (contractual) term, the Level 2 input must be observable for substantially the full term of the asset or liability.

Level 3: Inputs to the valuation methodology are unobservable and significant to the fair value measurement.

2. Fair Value Measurements – (Continued)

The asset's or liability's fair value measurement level within the fair value hierarchy is based on the lowest level of any input that is significant to the fair value measurement. Valuation techniques used need to maximize the use of observable inputs and minimize the use of unobservable inputs.

The following is a description of the valuation methodologies used for the Organization's securities invested in the 457(f) Retirement Plan measured at fair value as of December 31, 2013:

Cash and cash equivalents: The carrying amounts reported in the Statements of Financial Position approximate the fair value because of the short maturities of those instruments.

Mutual funds: Measured at net asset value within in the active market on which the individual securities are traded.

The methods described above may produce a fair value calculation that may not be indicative of the net realizable value or reflective of future fair values. Furthermore, while the Organization believes its valuation methods are appropriate and consistent with other market participants, the use of different methodologies or assumptions to determine the fair value of certain financial instruments could result in a different fair value measurement at the reporting date.

The fair values of the Organization's securities invested in the 457(f) Retirement Plan, classified by level, are as follows:

December 31,	2013			
	Fair Value	Level 1	Level 2	Level 3
Cash and equivalents	$ 851	$ 851	$ -	$ -
Mutual funds - fixed income	17,181	17,181	-	-
Mutual funds - equities	91,143	91,143	-	-
Total	$ 109,175	$ 109,175	$ -	$ -

The fair value and cost of the Organization's securities invested in the 457(f) Retirement Plan, as of December 31, 2013 are as follows:

	Cost Value	Market Value
Cash and equivalents	$ 851	$ 851
Mutual funds - fixed income	17,594	17,181
Mutual funds - equities	70,654	91,143
Total	$ 89,099	$ 109,175

3. Deferred Revenues

The contracts with the members of FRCC have a provision in them that provides that they have 30 days from the date of invoice for a new budgetary year (January through December) to withdraw from membership. Therefore, the Company made a decision to invoice all members on December 1 for the first quarterly installment of the 2014 budget, thus at December 31, 2013 it would be known whether all members are continuing with their membership.

4. Commitments

In December 2003, the Company entered into an agreement with Sprint Communications Company L.P. ("Sprint") to provide certain telecommunication services that are passed through to certain members beginning in 2004 for the Company's network. The initial term of the agreement is 36 months and has been renewed for an additional 12-month period each year thereafter. The agreement calls for the Company to make a minimum service commitment of $96,000 for each contract year of the term.

In December 2006, the Company entered into an agreement with Open Access Technology International, Inc. to provide the Florida Transaction Management System ("FTMS") services for the Company's customers. The initial term of the agreement was 36 months at $3,750 per month and has been renewed for an additional 12-month period each year thereafter. In 2013, the Company renewed this contract for 36 months at an annual cost of $57,000. In addition, several enhancements to the FTMS service were agreed upon of which $27,000 was paid for in 2013 and $27,000 will be paid in 2014 at the completion of the enhancements. The Company also has the option to purchase the system for $100,000; however, at this time, the Company has no intention of doing so.

In November 2007, the Company entered into an agreement to purchase Compliance Tracking System software from Guidance Solutions, Inc. In 2008, the Company entered into an agreement with several of the other regional entities to form a consortium and share the cost of future enhancements and program modules to add to the Compliance Tracking System originally purchased from Guidance Solutions, Inc. In June of 2011, the consortium broke up with certain member regions deciding to change software and vendors and go in a different direction for their Compliance Tracking System. The Company decided to remain with Guidance and has agreed to share costs of software enhancements with one other region that remains with Guidance. The cost of enhancements added or in progress for 2013 was $109,556. The Company is obligated for enhancements in progress as of December 31, 2013 from this regional agreement of approximately $28,800 for enhancements to be completed in 2014. The Company is also obligated for enhancements of their own system for $7,000 to be completed in 2014.

In May of 2013, the Company entered into an agreement with other Eastern Interconnection Reliability Coordinators and created the Interchange Distribution Calculator (IDC) Tools Member Association to manage the IDC Application contract that in prior years was managed by NERC. This tool is used to manage transmission congestion across the Eastern Interconnection. The agreement calls for the Company to make a minimum service commitment of $118,600 for each contract year of the term.

In May of 2013 the Company entered into agreements with Cisco Systems Capital Corporation to provide WebEx online presentation and audio conferencing services.

4. Commitments – (Continued)

The initial term of the agreement is for 36 months and call for the Company to make a total commitment of $130,500 over the 36-month term.

In July 2013, the company entered into an agreement with TW Telecom Holdings, Inc. (TW Telecom) to provide required redundant telecommunications for the FRCCnet wide area network that provides data to the FRCC reliability Coordinator. The initial term of the agreement is 36 months and calls for the Company to make a minimum service commitment of $68,400 for each contract year of the term.

5. Operating Leases

The Company leases its facilities and has operating leases that expire September 30, 2020 at its current location on Bayport Drive. The Bayport Plaza lease required a $150,000 deposit. For all leases, rental payments escalate based on the schedules set forth in the lease agreement. Minimum future rental payments are:

Year ended December 31,	
2014	$ 745,740
2015	766,199
2016	787,166
2017	808,832
2018	831,070
2019 and thereafter	1,498,850
	$ 5,437,857

Rent expense charged to operations during the year ended December 31, 2013 was $720,244, including the effects of lease payment escalations over the term of the leases.

For all leases, the future expense to be recognized including the effects of rent abatements and rent escalations are as follows:

Year Ended December 31,	
2014	$ 750,602
2015	750,602
2016	750,602
2017	750,602
2018	750,602
2019 and thereafter	1,313,557
	$ 5,066,567

6. Postretirement Benefits Other Than Pensions

The Company adheres to ASC 715-30, *Defined Benefit Plans - Other Post Retirement,* which requires companies to report the funded status (defined as the difference between the fair value of plan assets and the plan's benefit obligation) of their postretirement plan. The current year effect is a $519,831 increase to unrestricted net assets.

The following table sets forth the plan's funded status reconciled with the amount shown in the Company's statement of financial position at December 31, 2013:

Accumulated postretirement benefit oligation:	
Plan assets at fair value	-0-
Funded status	-0-
Accrued postretirement benefit obligation:	
Current portion	$ 32,914
Long-term portion	1,373,908
	$ 1,406,822

Since the plan is non-contributory, the entire balance of the accumulated benefit obligation is recorded as a liability in the statement of financial position as of December 31, 2013.

Benefits expected to be paid in each of the next five years are as follows:

Year Ended December 31,	
2014	$ 32,914
2015	35,829
2016	38,717
2017	53,993
2018	56,950
2019 and thereafter	391,970
	$ 610,373

6. Postretirement Benefits Other Than Pensions – (Continued)

The following provides the components of net periodic postretirement benefit cost for the year ended December 31, 2013.

Service Cost	$ (25,156)
Interest Cost	(31,214)
Amortization of unrecognized net obligation	(10,664)
Recognition of net actuarial gain	3,607
Net periodic postretirement benefit cost	(63,427)
Benefits paid during 2013	17,603
Net postretirement benefit loss	$ (45,824)
Items not yet recognized as a component of net periodic postretirement benefit costs	
Unrecognized net loss	$ (404,717)
Unrecognized net transition obligations	(39,983)
Transitional effect of ASC 715-30	(444,700)
Postretirement effect of ASC 715-30 as of December 31 2012	$ 75,131
Net periodic change in postretirement obligation	(519,831)
Postretirement obligation recognized as a component of net periodic benefit cost as of December 31, 2013	$ (444,700)

6. Postretirement Benefits Other Than Pensions – (Continued)

Amounts included in unrestricted net assets and expected to be recognized as components of net periodic benefit gain (cost) next year include amortization of unrecognized net obligation and net actuarial gain of approximately ($11,000) and $3,607, respectively. For measurement purposes, an 8% annual rate increase in the per capita cost of covered health care benefits was assumed for 2015; the rate was assumed to decrease to 7% for 2016; 6% for 2017 and remain at 5% thereafter. The health care cost trend rate assumption has a significant effect on the amounts reported. To illustrate, if assumed health care cost trend rates were increased by one percentage point in each year, the accumulated postretirement benefit obligation at December 31, 2013 would be increased $257,009 and the aggregate of the service and interest cost components of net periodic postretirement benefit cost for the year ended December 31, 2013 would be increased by $9,353.

The weighted average discount rate used in estimating the accumulated postretirement benefit obligation was 3.75%. Mortality was based on the RP-2000 Combined Mortality Tables for Healthy Males and Females. The measurement date of the accumulated postretirement benefit obligation was December 31, 2013.

Glossary: Accumulated postretirement benefit obligation – The actuarial present value of benefits attributed to employee service rendered to a particular date.

Net periodic postretirement benefit gain – The amount recognized in the financial statements as the gain of the postretirement benefit plan for a period.

In December of 2003, the Medicare Prescription Drug, Improvement and Modernization Act of 2003 (Act) was signed into law. The Act includes a special subsidy for employers that sponsor retiree health benefit plans with prescription drug benefits that are as favorable as the Medicare Part D benefit. The Company has not determined whether its plan is actuarially equivalent to the Medicare Part D benefit due to the cost of obtaining such an actuarial computation.

7. Retirement Plan

Effective January 1, 2001, the Company adopted a 401(k) Plan ("Plan") intended to benefit substantially all employees with 6 months of service and 21 years of age. On September 30, 2007, the plan was amended to enable employees with one hour of service to be eligible to enter the plan. Participants can contribute any amount of their compensation for the Plan year, not to exceed the limits determined by the Internal Revenue Code. The Company may make matching contributions with prescribed limits. The Company may also make additional non-elective discretionary contributions to the Plan. The Company made matching contributions to the Plan of $250,909 and a discretionary contribution to the Plan of $434,433 (net of forfeitures) for the year ending December 31, 2013.

Deferred Compensation – The Company implemented an executive deferred compensation plan subject to Section 457(f) of the Internal Revenue Code in 2004. For the year ended December 31, 2013, the Company contributed $8,492 to benefit the participant in this Plan.

In 2013, the Company adopted a Nonqualified 457(b) Retirement Plan ("Retirement Plan"), to be effective January 1, 2014, intended to benefit key managerial employees of the Company. The amount expensed in 2013 and to be funded in 2014 is $16,775.

8. Related Parties

Various members of the Company are founding members of Florida Electric Power Coordinating Group, Inc. ("FCG") and the organizations, excluding the board of directors, are under common management. FCG is a nonprofit organization operating under Section 501(c)(6) of the Internal Revenue Code and is exempt from federal and state income taxes.

The Company is providing FCG with administrative and accounting services, including the use of office space. FCG reimbursed the Company approximately 3.46% of the Company's administrative expenses in 2013. The service agreement with FCG is a one-year agreement that will automatically renew unless canceled in advance by either party. The original agreement was renewed for an additional year in February 2013. At December 31, 2013, the Company had billed and collected a total of $276,901 from FCG relating to the service agreement and has a receivable from FCG in the amount of $19,403.

The Company is purchasing the services from Florida Power and Light ("FPL"), a member of the Company, to fulfill the responsibilities of reliability coordinator, operations planning coordinator, state capacity emergency coordinator as well as various other services. The Company paid FPL $2,073,322 relating all of to these services and at December 31, 2013 had $683,463 of accrued expenses recorded on the books.

9. Concentrations

Two members make up approximately 54.8% of the member services assessments and dues. The same two members comprise 67.1% of the statutory assessment that NERC bills directly in order to fund the Company for its statutory functions.

10. Contingencies

As part of the Company's Delegation Agreement with NERC, the Company has the authority to fine entities within its region for violation of reliability standards. During 2013, six (6) notices of penalty were filed with FERC with settlement agreements addressing alleged violations of reliability standards for the entities within the FRCC region. The penalties totaling $248,000 as of December 31, 2013, were approved by FERC and paid by the entities. The Delegation Agreement Rules of Procedures from NERC stipulate that any penalty monies collected by June 30 of each year, which is between budget submissions, are to be held until they can be accounted for in a budget submission. At year-end December 31, 2013, a total of $481,000 penalty assessment is being held for future use of which $343,000 was accounted for in the 2014 budget submission and will be taken into operating income at the beginning of 2014 to offset funding from all entities in the region. The balance, plus any penalties billed and collected prior to June 30, 2014 will be held and accounted for in the 2015 budget submission.

The Company is the registered entity for the FRCC Region Reliability Coordinator functions and as a Planning Authority within the FRCC region. As a NERC registered entity, the Company must comply with applicable NERC reliability standards. Violations of these standards can result in financial penalties. The Company is involved in various enforcement actions for possible violations of electric reliability standards related to the NERC registered entity functions.

10. Contingencies - (Continued)

Several of the possible violations were self-reported by FRCC which may result in no penalty. At this time, the Company cannot fully determine the effect of the possible penalties that may arise. Based on the limited information available at this time the Company estimates that it is reasonably possible for a penalty to be assessed ranging from $75,000 to $125,000, however the Company cannot conclude that any amount within this range is a better estimate than any other, and accordingly the Company has included $75,000 as an accrued contingent liability.

11. Functional Expenses

The detail of functional expenses for the year ended is as follows:

Statutory expenses:		
Reliability Standards Development	$	229,145
Compliance & Enforcement		4,170,708
Reliability Assessment & Performance Analysis		1,109,679
Training & Education		259,144
Situational Awareness & Infrastructure		16,643
Total statutory expenses	$	5,785,319
Member Services expenses:		
Planning Committee		710,959
Operating Committee		5,424,221
General & Administrative		519,831
Total member services expenses		6,655,011
Total Expenses	$	12,440,330

12. Net Assets

Unrestricted net assets that are designated are FERC-approved for statutory expense or board-approved for member services expense segregations of unrestricted net assets for specific projects. Since designations are voluntary and may be reversed or redirected by the governing board at any time, designated portions of net assets are not considered restricted.

The detail of unrestricted FERC or board-designated net assets is as follows at year end:

Statutory	$ 1,966,888
Member Services	$ 587,073
Total unrestricted-board designated net assets	$ 2,553,961

SUPPLEMENTAL INFORMATION

Florida Reliability Coordinating Council, Inc.
Statement of Activities - Total Actual To Total Budget
TOTAL COMPANY
December 31, 2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%
Funding				
ERO Funding				
ERO Assessments	$ 5,957,970	$ 5,957,971	$ (1)	
Penalty Sanctions	304,500	304,500	-	
Total ERO Funding	$ 6,262,470	$ 6,262,471	$ (1)	$ -
Membership Dues	$ 6,250,976	$ 6,250,975	1	
Testing Fees	-	-	-	
Services & Software	314,641	333,000	(18,359)	
Workshops	99,385	90,000	9,385	
Interest	-	-	-	
Special Assessment	-	-	-	
NonCash Post Ret Gain (Loss)	(45,824)	-	(45,824)	
Total Funding	**$ 12,881,648**	**$ 12,936,446**	**$ (54,798)**	-0.4%
Expenses				
Personnel Expenses				
Salaries	$ 5,174,009	$ 5,569,794	(395,785)	
Payroll Taxes	314,794	358,291	(43,497)	
Benefits	783,735	770,937	12,798	
Retirement Costs	688,048	784,397	(96,349)	
Total Personnel Expenses	**$ 6,960,586**	**$ 7,483,419**	**$ (522,833)**	-7.0%
Meeting Expenses				
Meetings	$ 115,998	$ 98,669	17,329	
Travel	182,644	310,787	(128,143)	
Conference Calls	31,301	42,543	(11,242)	
Total Meeting Expenses	**$ 329,943**	**$ 451,999**	**$ (122,056)**	-27.0%
Operating Expenses				
Consultants & Contracts	$ 3,039,370	$ 3,192,699	(153,329)	
Office Rent	720,244	739,044	(18,800)	
Office Costs	573,638	696,392	(122,754)	
Professional Services	83,668	422,504	(338,836)	
Miscellaneous	75,000	-	75,000	
Depreciation	138,050	117,390	20,660	
Total Operating Expenses	**$ 4,629,970**	**$ 5,168,029**	**$ (538,059)**	-10.4%
Total Indirect Expenses	**$ -**	**$ -**	**$ -**	
Other Non-Operating Expenses	**$ 519,831**	**$ -**	**$ 519,831**	
Total Expenses	**$ 12,440,330**	**$ 13,103,447**	**$ (663,117)**	-5.1%
Change in Assets	**$ 441,318**	**$ (167,001)**	**$ 608,319**	-100.0%
Fixed Asset Expenditures				
Depreciation	$ (138,050)	$ (117,390)	$ (20,660)	
Non Pension Post Retir. Oblig	(565,655)	-	(565,655)	
Software CapEx	136,556	25,000	111,556	
Furniture & Fixtures CapEx	4,882	-	4,882	
Equipment & Computers CapEx	136,582	82,700	53,882	
Leasehold Improvements	-	-	-	
Increase/(Decrease) in Fixed Assets	**$ (425,685)**	**$ (9,690)**	**$ (415,995)**	100.0%
Total Budget	**$ 12,014,645**	**$ 13,093,757**	**$ (1,079,112)**	-8.2%
CHANGE IN WORKING CAPITAL	**$ 867,003**	**$ (157,311)**	**$ 1,024,314**	100.0%
FTEs	41.07	44.82	(3.75)	

Florida Reliability Coordinating Council, Inc.
Statement of Activities - Total Actual To Total Budget
TOTAL Statutory Only
December 31, 2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%
Funding				
ERO Funding				
ERO Assessments	$ 5,957,970	$ 5,957,971	$ (1)	
Penalty Sanctions	304,500	304,500	-	
Total ERO Funding	$ 6,262,470	$ 6,262,471	$ (1)	
Membership Dues	-	-	-	
Testing Fees	-	-	-	
Services & Software	22,650	22,000	650	
Workshops	99,385	90,000	9,385	
Interest	-	-	-	
Miscellaneous	-	-	-	
Total Funding	**$ 6,384,505**	**$ 6,374,471**	**$ 10,034**	0.2%
Expenses				
Personnel Expenses				
Salaries	$ 3,286,539	$ 3,741,113	$ (454,574)	
Payroll Taxes	201,113	240,656	(39,543)	
Benefits	489,334	533,629	(44,295)	
Retirement Costs	440,672	526,863	(86,191)	
Total Personnel Expenses	**$ 4,417,658**	**$ 5,042,261**	**$ (624,603)**	-12.4%
Meeting Expenses				
Meetings	$ 86,452	$ 83,259	$ 3,193	
Travel	144,350	232,363	(88,013)	
Conference Calls	14,301	19,347	(5,046)	
Total Meeting Expenses	**$ 245,103**	**$ 334,969**	**$ (89,866)**	-26.8%
Operating Expenses				
Consultants & Contracts	$ 336,548	$ 176,977	$ 159,571	
Office Rent	513,094	572,285	(59,191)	
Office Costs	113,063	199,513	(86,450)	
Professional Services	47,831	176,538	(128,707)	
Miscellaneous	-	-	-	
Depreciation	112,023	93,493	18,530	
Total Operating Expenses	**$ 1,122,559**	**$ 1,218,806**	**$ (96,247)**	-7.9%
Total Indirect Expenses	**$ -**	**$ -**	**$ -**	
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	
Total Expenses	**$ 5,785,320**	**$ 6,596,036**	**$ (810,716)**	-12.3%
Change in Assets	**$ 599,185**	**$ (221,565)**	**$ 820,750**	**-370.4%**
Fixed Asset Expenditures				
Depreciation	$ (112,023)	$ (93,493)	$ (18,530)	
Software CapEx	109,556	25,000	84,556	
Furniture & Fixtures CapEx	-	-	-	
Equipment & Computers CapEx	81,445	4,239	77,206	
Leasehold Improvements	-	-	-	
Increase/(Decrease) in Fixed Assets	**$ 78,978**	**$ (64,254)**	**$ 143,232**	-222.9%
Total Budget	**$ 5,864,298**	**$ 6,531,782**	**$ (667,484)**	-10.2%
CHANGE IN WORKING CAPITAL	**$ 520,207**	**$ (157,311)**	**$ 677,518**	**-430.7%**
FTEs	25.91	30.11	(4.20)	
Beginning Working Capital 1/1/2012	1,367,703	483,900	883,803	
Change in Working Capital	520,207	(157,311)	677,518	
Working Capital at 12/31/2012	1,887,910	326,589	1,561,321	

Florida Reliability Coordinating Council, Inc.
Statement of Activities - Total Actual To Total Budget
RELIABILITY STANDARDS
December 31, 2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%
Funding				
ERO Funding				
ERO Assessments	$ 381,624	$ 381,622	$ 2	
Penalty Sanctions	19,053	19,053	-	
Total ERO Funding	$ 400,677	$ 400,675	$ 2	
Membership Dues		$ -	-	
Testing Fees		-	-	
Services & Software			-	
Workshops			-	
Interest	-	-	-	
Miscellaneous	-	-	-	
Total Funding	**$ 400,677**	**$ 400,675**	**$ 2**	0.0%
Expenses				
Personnel Expenses				
Salaries	120,361	$ 204,940	(84,579)	
Payroll Taxes	7,613	13,183	(5,570)	
Benefits	17,108	34,059	(16,951)	
Retirement Costs	15,984	28,862	(12,878)	
Total Personnel Expenses	**$ 161,066**	**$ 281,044**	**$ (119,978)**	-42.7%
Meeting Expenses				
Meetings	$ 876	$ 1,002	(126)	
Travel	17,823	35,721	(17,898)	
Conference Calls	720	767	(47)	
Total Meeting Expenses	**$ 19,419**	**$ 37,490**	**$ (18,071)**	-48.2%
Operating Expenses				
Consultants & Contracts	$ 1,226	$ -	1,226	
Office Rent	12,837	18,690	(5,853)	
Office Costs	4,357	9,136	(4,779)	
Professional Services	1,785	12,134	(10,349)	
Miscellaneous			-	
Depreciation	890	1,342	(452)	
Total Operating Expenses	**$ 21,095**	**$ 41,302**	**$ (20,207)**	-48.9%
Total Indirect Expenses	**$ 27,565**	**$ 41,958**	**$ (14,393)**	-34.3%
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	
Total Expenses	**$ 229,145**	**$ 401,794**	**$ (172,649)**	-43.0%
Change in Assets	**$ 171,532**	**$ (1,119)**	**$ 172,651**	100.0%
Fixed Asset Expenditures				
Depreciation	$ (890)	$ (1,342)	$ 452	
Software CapEx			-	
Furniture & Fixtures CapEx			-	
Equipment & Computers CapEx	3,646	223	3,423	
Leasehold Improvements			-	
Increase/(Decrease) in Fixed Assets	**$ 2,756**	**$ (1,119)**	**$ 3,875**	-346.3%
Total Budget	**$ 231,901**	**$ 400,675**	**$ (168,774)**	-42.1%
CHANGE IN WORKING CAPITAL	**$ 168,776**	**$ -**	**$ 168,776**	
Direct FTEs	1.01	1.65	(0.64)	-38.8%
Indirect FTE's	0.14	0.41	(0.27)	-65.9%
Total FTE's	1.15	2.06	(0.91)	-44.2%

Florida Reliability Coordinating Council, Inc.
Statement of Activities - Total Actual To Total Budget
COMPLIANCE
December 31, 2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%
Funding				
ERO Funding				
ERO Assessments	$ 4,082,506	$ 4,082,511	$ (5)	
Penalty Sanctions	207,042	207,042	-	
Total ERO Funding	$ 4,289,548	$ 4,289,553	$ (5)	
Membership Dues	-	$ -	-	
Testing Fees		-	-	
Services & Software			-	
Workshops			-	
Interest	-	-	-	
Miscellaneous	-	-	-	
Total Funding	**$ 4,289,548**	**$ 4,289,553**	**$ (5)**	0.0%
Expenses				
Personnel Expenses				
Salaries	$ 2,091,678	$ 2,227,031	(135,353)	
Payroll Taxes	126,418	143,260	(16,842)	
Benefits	332,710	321,490	11,220	
Retirement Costs	282,634	313,634	(31,000)	
Total Personnel Expenses	**$ 2,833,440**	**$ 3,005,415**	**$ (171,975)**	-5.7%
Meeting Expenses				
Meetings	$ 12,154	$ 6,501	5,653	
Travel	76,991	131,336	(54,345)	
Conference Calls	9,324	3,285	6,039	
Total Meeting Expenses	**$ 98,469**	**$ 141,122**	**$ (42,653)**	-30.2%
Operating Expenses				
Consultants & Contracts	$ 195,037	$ 16,800	178,237	
Office Rent	385,183	434,212	(49,029)	
Office Costs	72,858	91,091	(18,233)	
Professional Services	34,604	117,809	(83,205)	
Miscellaneous			-	
Depreciation	102,321	80,918	21,403	
Total Operating Expenses	**$ 790,003**	**$ 740,830**	**$ 49,173**	6.6%
Total Indirect Expenses	**$ 448,796**	**$ 455,943**	**$ (7,147)**	-1.6%
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	
Total Expenses	**$ 4,170,708**	**$ 4,343,310**	**$ (172,602)**	-4.0%
Change in Assets	**$ 118,840**	**$ (53,757)**	**$ 172,597**	
Fixed Asset Expenditures				
Depreciation	$ (102,321)	$ (80,918)	$ (21,403)	
Software CapEx	109,556	25,000	84,556	
Furniture & Fixtures CapEx			-	
Equipment & Computers CapEx	57,343	2,161	55,182	
Leasehold Improvements			-	
Increase/(Decrease) in Fixed Assets	**$ 64,578**	**$ (53,757)**	**$ 118,335**	
Total Budget	**$ 4,235,286**	**$ 4,289,553**	**$ (54,267)**	-1.3%
CHANGE IN WORKING CAPITAL	**$ 54,262**	**$ -**	**$ 54,262**	
Direct FTEs	16.82	17.93	(1.11)	-6.2%
Indirect FTE's	2.26	2.17	0.09	4.1%
Total FTE's	19.08	20.10	(1.02)	-5.1%

Florida Reliability Coordinating Council, Inc.
Statement of Activities - Total Actual To Total Budget
RELIABILITY ASSESSMENT
December 31, 2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%
Funding				
ERO Funding				
ERO Assessments	$ 1,314,299	$ 1,314,299	$ -	
Penalty Sanctions	62,701	62,701	-	
Total ERO Funding	$ 1,377,000	$ 1,377,000	$ -	
Membership Dues	-	$ -	-	
Testing Fees		-	-	
Services & Software	22,650	22,000	650	
Workshops			-	
Interest	-	-	-	
Miscellaneous	-	-	-	
Total Funding	**$ 1,399,650**	**$ 1,399,000**	**$ 650**	0.0%
Expenses				
Personnel Expenses				
Salaries	$ 555,631	$ 674,444	(118,813)	
Payroll Taxes	34,375	43,385	(9,010)	
Benefits	78,830	97,086	(18,256)	
Retirement Costs	73,102	94,982	(21,880)	
Total Personnel Expenses	**$ 741,938**	**$ 909,897**	**$ (167,959)**	-18.5%
Meeting Expenses				
Meetings	$ 3,021	$ 4,810	(1,789)	
Travel	45,477	49,865	(4,388)	
Conference Calls	3,309	10,387	(7,078)	
Total Meeting Expenses	**$ 51,807**	**$ 65,062**	**$ (13,255)**	-20.4%
Operating Expenses				
Consultants & Contracts	$ 105,426	$ 115,177	$ (9,751)	
Office Rent	59,663	61,504	(1,841)	
Office Costs	17,254	71,379	(54,125)	
Professional Services	10,055	37,218	(27,163)	
Miscellaneous			-	
Depreciation	4,066	5,309	(1,243)	
Total Operating Expenses	**$ 196,464**	**$ 290,587**	**$ (94,123)**	-32.4%
Total Indirect Expenses	**$ 119,470**	**$ 138,080**	**$ (18,610)**	-13.5%
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	
Total Expenses	**$ 1,109,679**	**$ 1,403,626**	**$ (293,947)**	-20.9%
Change in Assets	**$ 289,971**	**$ (4,626)**	**$ 294,597**	
Fixed Asset Expenditures				
Depreciation	$ (4,066)	$ (5,309)	$ 1,243	
Software CapEx			-	
Furniture & Fixtures CapEx			-	
Equipment & Computers CapEx	15,566	683	14,883	
Leasehold Improvements			-	
Increase/(Decrease) in Fixed Assets	**$ 11,500**	**$ (4,626)**	**$ 16,126**	-348.6%
Total Budget	**$ 1,121,179**	**$ 1,399,000**	**$ (277,821)**	-19.9%
CHANGE IN WORKING CAPITAL	**$ 278,471**	**$ -**	**$ 278,471**	
Direct FTEs	4.36	5.43	(1.07)	-19.7%
Indirect FTE's	0.59	0.92	(0.33)	-35.9%
Total FTE's	4.95	6.35	(1.40)	-22.0%

Florida Reliability Coordinating Council, Inc.
Statement of Activities - Total Actual To Total Budget
TRAINING AND EDUCATION
December 31, 2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%
Funding				
ERO Funding				
ERO Assessments	$ 276,132	$ 276,136	$ (4)	
Penalty Sanctions	12,817	12,817	-	
Total ERO Funding	$ 288,949	$ 288,953	$ (4)	
Membership Dues	-	$ -	-	
Testing Fees		-	-	
Services & Software			-	
Workshops	99,385	90,000	9,385	
Interest	-	-	-	
Miscellaneous	-	-	-	
Total Funding	**$ 388,334**	**$ 378,953**	**$ 9,381**	2.5%
Expenses				
Personnel Expenses				
Salaries	$ 85,084	$ 137,870	(52,786)	
Payroll Taxes	5,417	8,869	(3,452)	
Benefits	9,594	18,009	(8,415)	
Retirement Costs	11,743	19,416	(7,673)	
Total Personnel Expenses	**$ 111,838**	**$ 184,164**	**$ (72,326)**	-39.3%
Meeting Expenses				
Meetings	$ 70,380	$ 70,908	(528)	
Travel	3,493	12,228	(8,735)	
Conference Calls	922	4,902	(3,980)	
Total Meeting Expenses	**$ 74,795**	**$ 88,038**	**$ (13,243)**	-15.0%
Operating Expenses				
Consultants & Contracts	$ 28,500	$ 45,000	(16,500)	
Office Rent	9,346	12,573	(3,227)	
Office Costs	13,091	12,312	779	
Professional Services	1,266	7,502	(6,236)	
Miscellaneous			-	
Depreciation	757	823	(66)	
Total Operating Expenses	**$ 52,960**	**$ 78,210**	**$ (25,250)**	-32.3%
Total Indirect Expenses	**$ 19,551**	**$ 28,226**	**$ (8,675)**	-30.7%
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	
Total Expenses	**$ 259,144**	**$ 378,638**	**$ (119,494)**	-31.6%
Change in Assets	**$ 129,190**	**$ 315**	**$ 128,875**	
Fixed Asset Expenditures				
Depreciation	$ (757)	$ (823)	$ 66	
Software CapEx			-	
Furniture & Fixtures CapEx			-	
Equipment & Computers CapEx	4,708	1,138	3,570	
Leasehold Improvements			-	
Increase/(Decrease) in Fixed Assets	**$ 3,951**	**$ 315**	**$ 3,636**	1154.3%
Total Budget	**$ 263,095**	**$ 378,953**	**$ (115,858)**	-30.6%
CHANGE IN WORKING CAPITAL	**$ 125,239**	**$ -**	**$ 125,239**	
Direct FTEs	0.60	1.11	(0.51)	-45.9%
Indirect FTE's	0.08	0.17	(0.09)	-52.9%
Total FTE's	0.68	1.28	(0.60)	-46.9%

Florida Reliability Coordinating Council, Inc.
Statement of Activities - Total Actual To Total Budget
SITUATIONAL AWARENESS
December 31, 2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%
Funding				
ERO Funding				
ERO Assessments	$ 60,714	$ 60,714	$ -	
Penalty Sanctions	2,887	2,887	-	
Total ERO Funding	$ 63,601	$ 63,601	$ -	
Membership Dues	-	$ -	-	
Testing Fees		-	-	
Services & Software			-	
Workshops			-	
Interest	-	-	-	
Miscellaneous	-	-	-	
Total Funding	**$ 63,601**	**$ 63,601**	**$ -**	0.0%
Expenses				
Personnel Expenses				
Salaries	$ 6,217	$ 31,052	(24,835)	
Payroll Taxes	379	1,997	(1,618)	
Benefits	805	4,070	(3,265)	
Retirement Costs	827	4,373	(3,546)	
Total Personnel Expenses	**$ 8,228**	**$ 41,492**	**$ (33,264)**	-80.2%
Meeting Expenses				
Meetings	$ 21	$ 38	(17)	
Travel	516	3,213	(2,697)	
Conference Calls	26	6	20	
Total Meeting Expenses	**$ 563**	**$ 3,257**	**$ (2,694)**	-82.7%
Operating Expenses				
Consultants & Contracts	$ 1,726	$ -	1,726	
Office Rent	714	2,831	(2,117)	
Office Costs	1,550	7,755	(6,205)	
Professional Services	121	1,875	(1,754)	
Miscellaneous			-	
Depreciation	2,428	2,561	(133)	
Total Operating Expenses	**$ 6,539**	**$ 15,022**	**$ (8,483)**	-56.5%
Total Indirect Expenses	**$ 1,313**	**$ 6,357**	**$ (5,044)**	-79.3%
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	
Total Expenses	**$ 16,643**	**$ 66,128**	**$ (49,485)**	-74.8%
Change in Assets	**$ 46,958**	**$ (2,527)**	**$ 49,485**	
Fixed Asset Expenditures				
Depreciation	$ (2,428)	$ (2,561)	$ 133	
Software CapEx			-	
Furniture & Fixtures CapEx			-	
Equipment & Computers CapEx	182	34	148	
Leasehold Improvements			-	
Increase/(Decrease) in Fixed Assets	**$ (2,246)**	**$ (2,527)**	**$ 281**	-11.1%
Total Budget	**$ 14,397**	**$ 63,601**	**$ (49,204)**	-77.4%
CHANGE IN WORKING CAPITAL	**$ 49,204**	**$ -**	**$ 49,204**	
Direct FTEs	0.05	0.25	(0.20)	-80.0%
Indirect FTE's	0.01	0.07	(0.06)	-85.7%
Total FTE's	0.06	0.32	(0.26)	-81.3%

Florida Reliability Coordinating Council, Inc.
Statement of Activities - Total Actual To Total Budget
GENERAL ADMINISTRATIVE
December 31, 2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%
Funding				
ERO Funding				
ERO Assessments	$ (157,305)	$ (157,311)	$ 6	
Penalty Sanctions		-	-	
Total ERO Funding	$ (157,305)	$ (157,311)	$ 6	
Membership Dues	-	$ -	-	
Testing Fees		-	-	
Services & Software			-	
Workshops			-	
Interest	-	-	-	
Miscellaneous	-	-	-	
Total Funding	**$ (157,305)**	**$ (157,311)**	**$ 6**	0.0%
Expenses				
Personnel Expenses				
Salaries	$ 427,568	$ 465,776	$ (38,208)	
Payroll Taxes	26,911	29,962	(3,051)	
Benefits	50,287	58,915	(8,628)	
Retirement Costs	56,382	65,596	(9,214)	
Total Personnel Expenses	**$ 561,148**	**$ 620,249**	**$ (59,101)**	-9.5%
Meeting Expenses				
Meetings		$ -	$ -	
Travel	50		50	
Conference Calls		-	-	
Total Meeting Expenses	**$ 50**	**$ -**	**$ 50**	######
Operating Expenses				
Consultants & Contracts	$ 4,633	$ -	$ 4,633	
Office Rent	45,351	42,475	2,876	
Office Costs	3,953	7,840	(3,887)	
Professional Services		-	-	
Miscellaneous			-	
Depreciation	1,561	2,540	(979)	
Total Operating Expenses	**$ 55,498**	**$ 52,855**	**$ 2,643**	5.0%
Total Indirect Expenses	**$ (616,695)**	**$ (670,564)**	**$ 53,869**	
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	
Total Expenses	**$ 1**	**$ 2,540**	**$ (2,539)**	**-100.0%**
Change in Assets	**$ (157,306)**	**$ (159,851)**	**$ 2,545**	-1.6%
Fixed Asset Expenditures				
Depreciation	$ (1,561)	$ (2,540)	$ 979	
Software CapEx			-	
Furniture & Fixtures CapEx			-	
Equipment & Computers CapEx			-	
Leasehold Improvements			-	
Increase/(Decrease) in Fixed Assets	**$ (1,561)**	**$ (2,540)**	**$ 979**	-38.5%
Total Budget	**$ (1,560)**	**$ -**	**$ (1,560)**	
CHANGE IN WORKING CAPITAL	**$ (155,745)**	**$ (157,311)**	**$ 1,566**	-1.0%
FTEs	3.07	3.74	(0.67)	-17.9%

Florida Reliability Coordinating Council, Inc.
Statement of Activities - Total Actual To Total Budget
TOTAL MEMBER SERVICES - NON STATUTORY
December 31, 2013

(In Whole Dollars)

	2013 Actual	2013 Budget	2013 Variance	%
Funding				
ERO Funding				
ERO Assessments	$ -	$ -	$ -	
Penalty Sanctions	-	-	-	
Total ERO Funding	$ -	$ -	$ -	
Membership Dues	6,250,976	6,250,975	1	
Testing Fees	-	-	-	
Services & Software	291,991	311,000	(19,009)	
Workshops	-	-	-	
Special Assessment	-	-	-	
Non Cash Postretirement	(45,824)	-	(45,824)	
Total Funding	**$ 6,497,143**	**$ 6,561,975**	**$ (64,832)**	-1.0%
Expenses				
Personnel Expenses				
Salaries	$ 1,887,470	$ 1,828,681	58,789	
Payroll Taxes	113,681	117,635	(3,954)	
Benefits	294,401	237,308	57,093	
Retirement Costs	247,376	257,534	(10,158)	
Total Personnel Expenses	**$ 2,542,928**	**$ 2,441,158**	**$ 101,770**	4.2%
Meeting Expenses				
Meetings	$ 29,546	$ 15,410	14,136	
Travel	38,294	78,424	(40,130)	
Conference Calls	17,000	23,196	(6,196)	
Total Meeting Expenses	**$ 84,840**	**$ 117,030**	**$ (32,190)**	-27.5%
Operating Expenses				
Consultants & Contracts	$ 2,702,822	$ 3,015,722	(312,900)	
Office Rent	207,150	166,759	40,391	
Office Costs	460,575	496,879	(36,304)	
Professional Services	35,837	245,966	(210,129)	
Miscellaneous	75,000	-	75,000	
Depreciation	26,027	23,897	2,130	
Total Operating Expenses	**$ 3,507,411**	**$ 3,949,223**	**$ (441,812)**	-11.2%
Total Indirect Expenses				
Other Non-Operating Expenses	**$ 519,831**	**$ -**	**$ 519,831**	
Total Expenses	**$ 6,655,010**	**$ 6,507,411**	**$ 147,599**	2.3%
Change in Assets	**$ (157,867)**	**$ 54,564**	**$ (212,431)**	
Fixed Asset Expenditures				
Depreciation	$ (26,027)	$ (23,897)	$ (2,130)	
Non Pension Post Retir. Oblig	(565,655)	-	(565,655)	
Software CapEx	27,000	-	27,000	
Furniture & Fixtures CapEx	4,882	-	4,882	
Equipment & Computers CapEx	55,137	78,461	(23,324)	
Leasehold Improvements	-	-	-	
Increase/(Decrease) in Fixed Assets	**$ (504,663)**	**$ 54,564**	**$ (559,227)**	-1024.9%
Total Budget	**$ 6,150,347**	**$ 6,561,975**	**$ (411,628)**	-6.3%
CHANGE IN WORKING CAPITAL	**$ 346,796**	**$ -**	**$ 346,796**	
FTEs	15.16	14.71	0.45	

ATTACHMENT 3

2013 ACTUAL COST-TO-BUDGET COMPARISON

AND

2013 AUDITED FINANCIAL REPORT

FOR

MIDWEST RELIABILITY ORGANIZATION

MIDWEST RELIABILITY ORGANIZATION

380 St. Peter Street, Ste. 800, Saint Paul, MN 55102 MidwestReliability.org P.651.855.1760 F.651.855.1712

Sue Clarke, VP of Finance and Administration
P: (651) 855-1707
F: (651) 855-1712
E: sa.clarke@midwestreliability.org

April 29, 2014

Mr. Michael Walker
Ms. Susan Turpen
North American Electric Reliability Corporation (NERC)

RE: 2013 Budget Variance Explanation Based on Audited Financials

Dear Mr. Walker and Ms. Turpen:

MRO staff reports the audited final numbers to be 7.63% ***under*** budget ($709k). Prior to the annual actuarial calculation of post-retirement medical benefit obligation (discount rate, expected rate of return on plan assets and health care cost trend rate) MRO staff reported to be 4.91% ***under*** budget ($457k).

While MRO was under budget, MRO staff believes the principal responsibilities under the delegation agreement were met in 2013. During 2013, MRO conducted 19 audits and spot checks including 10 on-site and 6 off-site combined CIP and operations and planning audits and 2 off-site operations and planning audits. Additionally, MRO participated in one on-site operations and planning audit and one on-site CIP audit lead by SERC. No spot checks were conducted in 2013. MRO identified 147 new potential violations and closed 140 instances of noncompliance (violations or remediated issues) in 2013. MRO completed all budgeted reliability assessments for the year. In addition, MRO provided oversight on the event analysis of eight events in the Region during 2013.

As requested, the year-to-date variances greater than $10,000 and 10 percent are explained below.

Meeting Expenses (Actual - $223,169 under budget)

- Meeting expenses were under budget by $40,863. This was due to the new MRO facility having provided more opportunities to host meetings, which enabled staff to reduce cost significantly more than originally expected by eliminating the cost of meeting room and audio visual rentals as well as lower catering costs. These cost savings are trended in the 2014 Budget.
- Travel expenses were under budget by $155,747. Greater than budgeted use of the new MRO facility resulted in less travel by MRO staff. Resources were also shifted from auditing to risk assessment and mitigation, which in 2013 required minimum travel.
- Conference call expenses were under budget by $26,559. Upgrades in mid-year 2013 for audio and web conferencing media eliminated costs for the remaining portion of 2013. These cost savings are trended in the 2014 Budget.

380 St. Peter Street, Ste. 800, Saint Paul, MN 55102 MidwestReliability.org P.651.855.1760 F.651.855.1712

Consultants and Contracts (Actual - $82,453 under budget)
MRO had expected to come in on budget by the end of the year. Two expected projects were outsourced; one was approximately 50% completed. Both are expected to be completed in 2014.

Professional Services (Actual - $99,161 under budget)
External counsel is requested when necessary and this cost is difficult to trend.

Other non-Operating Expenses (Actual - $194,304 under budget)
In addition to the review of financials, MRO's independent financial audit requests support for the annual actuarial calculation of post-retirement medical benefit obligation. The actuarial assumptions take into consideration the discount rate, expected rate of return on plan assets and health care cost trend rate. After review and discussion of provided assessments by the relevant third party advisors, a higher post-retirement discount rate of 5.04% (up from 4.12%) and a 6% expected rate of return applied. This rate remains unchanged from the previous year's assumptions and calculation. This resulted in a positive impact to net revenues of $252k in 2013. $58k was included in the net periodic cost and $194k as a non-operating cost.

Fixed Assets (Actual - $52,355 over budget)
MRO staff accelerated some planned projects from 2014.

Change in Assets and Year End
MRO was **under budget by $709k** as explained above.

If you have any questions regarding this report, please contact me at 651-855-1707.

Thank you,

Sue Clarke

Sue Clarke

Cc: Daniel Skaar, MRO

Midwest Reliability Organization
2012 Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013
Per Audit

Consolidated	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)
Funding			
ERO Funding			
Assessments	9,098,927	9,098,927	-
Penalty Sanctions	14,001	14,001	-
Total ERO Funding	**$ 9,112,928**	**$ 9,112,928**	**$ -**
Federal Grants	-	-	-
Membership Fees	-	-	-
Testing	-	-	-
Services & Software	-	-	-
Workshop Fees	-	-	-
Interest	-	-	-
Miscellaneous	-	-	-
Total Funding (A)	**$ 9,112,928**	**$ 9,112,928**	**$ -**
Expenses			
Personnel Expenses			
Salaries	4,760,887	4,772,320	(11,433)
Payroll Taxes	310,790	312,394	(1,604)
Employee Benefits	380,894	394,086	(13,192)
Savings & Retirement	724,304	833,228	(108,924)
Total Personnel Expenses	**6,176,875**	**6,312,027**	**(135,153)**
Meeting Expenses			
Meetings	91,601	132,464	(40,863)
Travel	475,018	630,765	(155,747)
Conference Calls	15,141	41,700	(26,559)
Total Meeting Expenses	**581,760**	**804,929**	**(223,169)**
Operating Expenses			
Consultants & Contracts	490,647	573,100	(82,453)
Rent & Improvements	487,109	528,827	(41,718)
Office Costs	443,188	428,304	14,884
Professional Services	147,339	246,500	(99,161)
Miscellaneous	-	-	-
Depreciation	410,259	305,665	104,594
Total Operating Expenses	**1,978,542**	**2,082,396**	**(103,854)**
Indirect Expenses	**-**	**1**	**(1)**
Other Non-Operating Expenses	**(194,304)**	**-**	**(194,304)**
Total Expenses (B)	**8,542,873**	**9,199,353**	**(656,481)**
Change in Assets (A - B)	**570,055**	**(86,425)**	**656,481**
Fixed Assets			
Depreciation	(410,259)	(305,665)	(104,594)
Computer & Software CapEx	420,386	339,851	80,535
Furniture & Fixtures CapEx	37,162	-	37,162
Equipment CapEx	-	-	-
Leasehold Improvements	(15,342)	50,000	(65,342)
(Inc)Dec in Fixed Assets	$ 31,947	$ 84,186	$ (52,239)
Allocation of Fixed Assets	-	-	-
Total Inc(Dec) in Fixed Assets (C)	**31,947**	**84,184**	**(52,239)**
TOTAL BUDGET (B + C)	**8,574,820**	**9,283,537**	**(708,720)**
Change in Working Capital (A-B-C)	**538,108**	**(170,609)**	**708,720**
FTEs	**37.9**	**37.8**	**0.2**

Midwest Reliability Organization
2012 Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013
Per Audit

RELIABILITY STANDARDS	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	542,840	542,840	-	0.00%	
Penalty Sanctions	762	762	-	0.00%	
Total ERO Funding	**$ 543,602**	**$ 543,602**	$ -	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	543,602	543,602	-	0.00%	
Expenses					
Personnel Expenses					
Salaries	165,904	210,558	(44,654)	-21.21%	
Payroll Taxes	9,913	12,362	(2,449)	-19.81%	
Employee Benefits	11,425	15,154	(3,729)	-24.61%	
Savings & Retirement	27,194	32,835	(5,641)	-17.18%	
Total Personnel Expenses	214,436	270,909	(56,473)	-20.85%	Reduced staff involvment by increasing alignment with technical stakeholders to address reliability impacts.
Meeting Expenses					
Meetings	843	7,500	(6,657)	-88.76%	Fewer meetings at a much lower cost due to hosting at MRO's facility. Savings resulted from eliminating meeting room and audio visual rental costs as well as lowering catering costs.
Travel	19,540	28,900	(9,360)	-32.39%	Working groups were encouraged to reduce face-to-face meetings so less travel than anticipated. Also, member reimbursements were reduced for our SME application guide developers because there were fewer application guides than anticipated in 2013.
Conference Calls	9,682	15,000	(5,318)	-35.45%	Upgrades in mid-year 2013 for audio and web conferencing media eliminated costs for the remaining portion of 2013.
Total Meeting Expenses	30,065	51,400	(21,335)	-41.51%	
Operating Expenses					
Consultants & Contracts	12,000	12,000	-	0.00%	
Rent & Improvements	-	-	-		
Office Costs	2,436	6,580	(4,144)	-62.98%	A certain amount of training is required over a two or three year span rather than each year. In 2013 staff did not take as much training as they will in 2014 and 2015.
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	14,436	18,580	(4,144)	-22.30%	
Indirect Expenses	121,279	198,132	(76,853)	-38.79%	Total actual indirect costs were under budget, therefore there were less indirect costs than budgeted allocated to this program.
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	380,216	539,021	(158,805)	-29.46%	
Change in Assets (A - B)	163,386	4,581	158,805	3466.61%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
(Inc)Dec in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	1,154	4,581	(3,427)	-74.81%	Total actual fixed costs were under budget, therefore there were less asset costs than budgeted allocated to this program.
Total Inc(Dec) in Fixed Assets (C)	1,154	4,581	(3,427)	-74.81%	
TOTAL BUDGET (B + C)	**381,370**	**543,602**	(162,232)	**-29.84%**	
Change in Working Capital (A-B-C)	**(162,232)**	**-**	**(162,232)**		
FTEs	**1.0**	**1.5**	(0.5)	**-31.79%**	

Midwest Reliability Organization
2012 Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013
Per Audit

COMPLIANCE OPERATIONS, ENFORCEMENT and ORGANIZATION REGISTRATION	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	6,126,145	6,126,145	-	0.00%	
Penalty Sanctions	9,581	9,581	-	0.00%	
Total ERO Funding	**$ 6,135,726**	**$ 6,135,726**	$ -	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	6,135,726	6,135,726	-	0.00%	
Expenses					
Personnel Expenses					
Salaries	2,373,856	2,372,105	1,751	0.07%	
Payroll Taxes	156,873	159,443	(2,570)	-1.61%	
Employee Benefits	199,853	203,097	(3,244)	-1.60%	
Savings & Retirement	318,341	393,579	(75,238)	-19.12%	Annual post-retirement adjustment reduced the cost for 2013 based on higher discount rate provided by third party advisors
Total Personnel Expenses	3,048,923	3,128,224	(79,301)	-2.54%	
Meeting Expenses					
Meetings	2,794	5,600	(2,806)	-50.11%	Fewer meetings at a much lower cost due to hosting at MRO's facility. Savings resulted from eliminating meeting room and audio visual rental costs as well as lowering catering costs.
Travel	130,092	200,300	(70,208)	-35.05%	The overall travel expense was estimated high compared to actual travel costs. Travel for working group meetings was discouraged and MRO staff attended far fewer meetings than anticipated. The travel was replaced with conference calls.
Conference Calls	2,793	8,400	(5,607)	-66.75%	Upgrades in mid-year 2013 for audio and web conferencing media eliminated costs for the remaining portion of 2013.
Total Meeting Expenses	135,679	214,300	(78,621)	-36.69%	
Operating Expenses					
Consultants & Contracts	105,498	157,000	(51,502)	-32.80%	Two expected projects were outsourced; one was approximately 50% completed. Both are expected to be completed in 2014.
Rent & Improvements	-	-	-		
Office Costs	85,015	79,354	5,661	7.13%	
Professional Services	-	7,500	(7,500)	-100.00%	These were contingency dollars for Canadian filings that were not necessary in 2013.
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	190,513	243,854	(53,341)	-21.87%	
Indirect Expenses	2,298,406	2,491,737	(193,331)	-7.76%	Total actual indirect costs were under budget, therefore there were less indirect costs than budgeted allocated to this program
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	5,673,521	6,078,115	(404,594)	-6.66%	
Change in Assets (A - B)	462,205	57,611	404,594	702.29%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
(Inc)Dec in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	21,873	57,611	(35,738)	-62.03%	Total actual fixed costs were under budget, therefore there were less asset costs than budgeted allocated to this program
Total Inc(Dec) in Fixed Assets (C)	21,873	57,611	(35,738)	-62.03%	
TOTAL BUDGET (B + C)	**5,695,394**	**6,135,726**	(440,332)	**-7.18%**	
Change in Working Capital (A-B-C)	**(440,332)**	**-**	**(440,332)**		
FTEs	**19.5**	**19.0**	0.5	**2.79%**	

Midwest Reliability Organization
2012 Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013
Per Audit

RELIABILITY ASSESSMENTS and PERFORMANCE ANALYSIS	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	2,274,076	2,274,076	-	0.00%	
Penalty Sanctions	3,370	3,370	-	0.00%	
Total ERO Funding	**$ 2,277,446**	**$ 2,277,446**	**$ -**	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	2,277,446	2,277,446	-	0.00%	
Expenses					
Personnel Expenses					
Salaries	819,315	795,326	23,989	3.02%	
Payroll Taxes	52,710	54,654	(1,944)	-3.56%	
Employee Benefits	71,461	71,795	(334)	-0.47%	
Savings & Retirement	149,493	160,752	(11,259)	-7.00%	
Total Personnel Expenses	1,092,979	1,082,527	10,452	0.97%	
Meeting Expenses					
Meetings	7,316	20,000	(12,684)	-63.42%	Approximately the same number of meetings at a much lower cost due to hosting at MRO's facility. Savings resulted from eliminating meeting room and audio visual rental costs as well as lowering catering costs.
Travel	147,655	106,150	41,505	39.10%	Due to the increased number of activities in this area there was more travel than anticipated. Activities included but not limited to BES, RAPA, and Event Analysis meetings at the NERC level. MRO staff also knew that travel (most specifically airfare) was low in our original budget. MRO staff was confident that they would be able to manage to the RAPA budget as a whole.
Conference Calls	2,207	2,500	(293)	-11.72%	Upgrades in mid-year 2013 for audio and web conferencing media eliminated costs for the remaining portion of 2013.
Total Meeting Expenses	157,178	128,650	28,528	22.17%	
Operating Expenses					
Consultants & Contracts	60,555	141,100	(80,545)	-57.08%	RAPA has three contracts that are budgeted based on an estimated number of required hours; actual hours can fluctuate greatly. In the case of 2013 the actual dollars in our Model Building came in 50% lower. MRO also had Event Analysis contingency dollars in our 2013 Budget that were unnecessary and were removed in the 2014 budget.
Rent & Improvements	-	-	-		
Office Costs	24,140	28,400	(4,260)	-15.00%	2013 training dollars were budgeted for two different staffers who are no longer in the department. Actual staff required different training requirements; actual cost was lower than budgeted.
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	84,695	169,500	(84,805)	-50.03%	
Indirect Expenses	878,387	876,504	1,883	0.21%	
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	2,213,239	2,257,181	(43,942)	-1.95%	
Change in Assets (A - B)	64,207	20,265	43,942	216.84%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
(Inc)Dec in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	8,359	20,265	(11,906)	-58.75%	Total actual fixed costs were under budget, therefore there were less asset costs than budgeted allocated to this program.
Total Inc(Dec) in Fixed Assets (C)	8,359	20,265	(11,906)	-58.75%	
TOTAL BUDGET (B + C)	**2,221,598**	**2,277,446**	(55,848)	**-2.45%**	
Change in Working Capital (A-B-C)	**(55,848)**	**-**	**(55,848)**		
FTEs	**7.5**	**6.7**	0.8	**11.68%**	

Midwest Reliability Organization
2012 Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013
Per Audit

TRAINING, EDUCATION and OPERATOR CERTIFICATION	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	229,281	229,281	-	0.00%	
Penalty Sanctions	136	136	-	0.00%	
Total ERO Funding	**$ 229,417**	**$ 229,417**	**$ -**	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	229,417	229,417	-	0.00%	
Expenses					
Personnel Expenses					
Salaries	77,308	65,436	11,872	18.14%	
Payroll Taxes	3,320	2,231	1,089	48.81%	
Employee Benefits	3,744	1,935	1,809	93.49%	
Savings & Retirement	12,525	11,469	1,056	9.21%	
Total Personnel Expenses	96,897	81,071	15,826	19.52%	More Sr Management involvement than anticipated with the number of issues that were addressed in 2013 agendas. Some of those issues included but not limited to: BES, New Modeling, and Protection System Standards.
Meetings	56,428	63,500	(7,072)	-11.14%	
Travel	12,313	28,600	(16,287)	-56.95%	Dollars were budgeted for the SME to travel and give forum presentations in 2013 which were not required.
Conference Calls	-	15,000	(15,000)	-100.00%	Upgrades in mid-year 2013 for audio and web conferencing media eliminated costs for the remaining portion of 2013.
Total Meeting Expenses	68,741	107,100	(38,359)	-35.82%	
Operating Expenses					
Consultants & Contracts	-	-	-		
Rent & Improvements	-	-	-		
Office Costs	349	5,000	(4,651)	-93.02%	
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	349	5,000	(4,651)	-93.02%	
Indirect Expenses	38,856	35,428	3,428	9.68%	
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	204,843	228,599	(23,756)	-10.39%	
Change in Assets (A - B)	24,574	818	23,756	2904.13%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
(Inc)Dec in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	370	819	(449)	-54.85%	Total actual fixed costs were under budget, therefore there were less asset costs than budgeted allocated to this program.
Total Inc(Dec) in Fixed Assets (C)	370	819	(449)	-54.85%	
TOTAL BUDGET (B + C)	**205,213**	**229,418**	(24,205)	**-10.55%**	
Change in Working Capital (A-B-C)	**(24,204)**	**1**	**(24,205)**		
FTEs	**0.33**	**0.27**	0.1	**22.22%**	

Midwest Reliability Organization
2012 Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013
Per Audit

SITUATION AWARENESS and INFRASTRUCTURE SECURITY (Includes Critical Infrastructure Protection)	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	97,197	97,197	-	0.00%	
Penalty Sanctions	151	151	-	0.00%	
Total ERO Funding	**$ 97,348**	**$ 97,348**	$ -	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	97,348	97,348	-	0.00%	
Expenses					
Personnel Expenses					
Salaries	27,834	37,373	(9,539)	-25.52%	
Payroll Taxes	2,091	1,824	267	14.64%	
Employee Benefits	2,118	1,935	183	9.46%	
Savings & Retirement	4,134	7,642	(3,508)	-45.90%	
Total Personnel Expenses	36,177	48,774	(12,597)	-25.83%	Less of MRO's time was spent monitoring the system because MRO is able to rely on the BES operators to provide information in the event of a potential risk to reliability.
Meeting Expenses					
Meetings	24	-	24		
Travel	11,149	3,300	7,849	237.85%	
Conference Calls	-	-	-		
Total Meeting Expenses	11,173	3,300	7,873	238.58%	
Operating Expenses					
Consultants & Contracts	-	-	-		
Rent & Improvements	-	-	-		
Office Costs	3,688	5,000	(1,312)	-26.24%	
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	3,688	5,000	(1,312)	-26.24%	
Indirect Expenses	20,017	39,364	(19,347)	-49.15%	Total actual indirect costs were under budget, therefore there were less indirect costs than budgeted allocated to this program.
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	71,055	96,438	(25,383)	-26.32%	
Change in Assets (A - B)	26,293	910	25,383	2789.36%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
(Inc)Dec in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	190	910	(720)	-79.07%	Total actual fixed costs were under budget, therefore there were less asset costs than budgeted allocated to this program.
Total Inc(Dec) in Fixed Assets (C)	190	910	(720)	-79.07%	
TOTAL BUDGET (B + C)	**71,245**	**97,348**	(26,103)	**-26.81%**	
Change in Working Capital (A-B-C)	**(26,103)**	**-**	**(26,103)**		
FTEs	**0.17**	**0.31**	**(0.14)**	**-45.16%**	

Midwest Reliability Organization
2012 Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013
Per Audit

MEMBER FORUMS	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					ELIMINATED 07/01/2013 TO CONFORM TO HOW THE
Assessments	-		-		OTHER REGIONS ARE RECORDING NERC
Penalty Sanctions	-		-		PARTICIPATION
Total ERO Funding	$ -	$ -	$ -		ALL OTHER REGIONS AND NERC RECORD COSTS
					IN THE PROGRAM OF THE PARTICIPANT
Federal Grants	-	-	-		WE WILL TRACK NERC TIME SEPARATELY
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	-	-	-		
Expenses					
Personnel Expenses					
Salaries	153,795	297,396	(143,601)	-48.29%	
Payroll Taxes	11,411	16,595	(5,184)	-31.24%	
Employee Benefits	6,777	18,916	(12,139)	-64.17%	
Savings & Retirement	29,487	57,407	(27,920)	-48.64%	
Total Personnel Expenses	201,470	390,314	(188,844)	-48.38%	Actuals are substantially below budget because as of 7/1/2013 MRO stopped recording costs to Member Forums. Please see above comment for details.
Meeting Expenses					
Meetings	-	-	-		
Travel	66,519	187,000	(120,481)	-64.43%	
Conference Calls	-	-	-		
Total Meeting Expenses	66,519	187,000	(120,481)	-64.43%	Actuals are substantially below budget because as of 7/1/2013 MRO stopped recording costs to Member Forums. Please see above comment for details.
Operating Expenses					
Consultants & Contracts	-	-	-		
Rent & Improvements	-	-	-		
Office Costs	-	-	-		
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	-	-	-		
Indirect Expenses	(267,989)	(577,314)	309,325	-53.58%	Actuals are substantially below budget because as of 7/1/2013 MRO stopped recording costs to Member Forums. Please see above comment for details.
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	-	-	-		
Change in Assets (A - B)	-	-	-		
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
(Inc)Dec in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B + C)	-	-	-		
Change in Working Capital (A-B-C)	-	-	-		
FTEs	-	1.4	(1.4)	-100.00%	Actuals are substantially below budget because as of 7/1/2013 MRO stopped recording costs to Member Forums. Please see above comment for details.

Midwest Reliability Organization
2012 Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013
Per Audit

GENERAL and ADMINISTRATIVE	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	(170,612)	(170,612)	-	0.00%	
Penalty Sanctions	-		-		
Total ERO Funding	**$ (170,612)**	**$ (170,612)**	$ -	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	(170,612)	(170,612)	-	0.00%	
Expenses					
Personnel Expenses					
Salaries	290,642	192,366	98,276	51.09%	
Payroll Taxes	14,177	10,760	3,417	31.76%	
Employee Benefits	14,934	13,435	1,499	11.16%	
Savings & Retirement	44,544	34,693	9,851	28.39%	
Total Personnel Expenses	364,297	251,254	113,043	44.99%	In first quarter 2013 the executives charged their BOD preparation and actual time to G&A rather than to each of their own programs. In addition, costs for third and fourth quarter NERC and BOT meetings were recorded here rather than in Member Forums.
Meeting Expenses					
Meetings	23,221	35,864	(12,643)	-35.25%	Approximately the same number of meetings at a much lower cost due to hosting at MRO's facility. Savings resulted from eliminating meeting room and audio visual rental costs as well as lowering catering costs.
Travel	73,098	60,000	13,098	21.83%	The BOT travel that was budgeted under program Forums(1100) was charged to G&A after 06/30/2013 based on the treatment by the other regions
Conference Calls	163	800	(637)	-79.63%	Upgrades in mid-year 2013 for audio and web conferencing media eliminated costs for the remaining portion of 2013.
Total Meeting Expenses	96,482	96,664	(182)	-0.19%	
Operating Expenses					
Consultants & Contracts	1,912	40,000	(38,088)	-95.22%	Contingent dollars were included for MRO's share of an all-regional project (similar to the Deloitte project in 2012) but were not needed in 2013
Rent & Improvements	-	-	-		
Office Costs	74,806	71,100	3,706	5.21%	
Professional Services	72,500	100,000	(27,500)	-27.50%	Actual compensation required for independent Board members was less than budgeted.
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	149,218	211,100	(61,882)	-29.31%	
Indirect Expenses	(609,997)	(559,018)	(50,979)	9.12%	
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	-	-	-		
Change in Assets (A - B)	(170,612)	(170,612)	-	0.00%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
(Inc)Dec in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B + C)	-	-	-		
Change in Working Capital (A-B-C)	**170,612**	**170,612**	-	0.00%	
FTEs	**1.6**	**1.3**	0.3	**21.97%**	

Midwest Reliability Organization
2012 Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013
Per Audit

LEGAL and REGULATORY	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments			-		
Penalty Sanctions			-		
Total ERO Funding	$ -	$ -	$ -		
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	-	-	-		
Expenses					
Personnel Expenses					
Salaries	195,380	219,355	(23,975)	-10.93%	
Payroll Taxes	12,707	11,538	1,169	10.13%	
Employee Benefits	2,110	2,150	(40)	-1.86%	
Savings & Retirement	28,067	37,375	(9,308)	-24.90%	
Total Personnel Expenses	238,264	270,418	(32,154)	-11.89%	Costs were below budget because in first quarter 2013 the executives charged their BOD preparation and actual time to G&A rather than to each of their own programs
Meeting Expenses					
Meetings	-	-	-		
Travel	9,418	9,515	(97)	-1.02%	
Conference Calls	-	-	-		
Total Meeting Expenses	9,418	9,515	(97)	-1.02%	
Operating Expenses					
Consultants & Contracts	-	-	-		
Rent & Improvements	-	-	-		
Office Costs	5,118	5,050	68	1.35%	
Professional Services	22,115	60,000	(37,885)	-63.14%	Contingency dollars for outside legal counsel to supplement internal resources as necessary. This included funds for MRO's share of the all-region 2014 5-year assessment. By sharing these costs among the regions, each region benefited from the economy of scale.
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	27,233	65,050	(37,817)	-58.14%	
Indirect Expenses	(274,915)	(344,983)	70,068	-20.31%	
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	-	-	-		
Change in Assets (A - B)	-	-	-		
Fixed Assets					
Depreciation	0.00	0.00	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
(Inc)Dec in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B + C)	-	-	-		
Change in Working Capital (A-B-C)	-	-	-		
FTEs	**1.1**	**1.2**	(0.1)	**-8.20%**	

Midwest Reliability Organization
2012 Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013
Per Audit

INFORMATION TECHNOLOGY	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments			-		
Penalty Sanctions			-		
Total ERO Funding	$ -	$ -	$ -		
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	-	-	-		
Expenses					
Personnel Expenses					
Salaries	343,851	291,579	52,272	17.93%	Sr management time in the IT area was significant since the IT Manager was new and MRO began several significant projects: SharePoint, Website and Lync
Payroll Taxes	24,681	22,502	2,179	9.68%	
Employee Benefits	35,665	33,318	2,347	7.04%	
Savings & Retirement	57,973	40,739	17,234	42.30%	
Total Personnel Expenses	462,170	388,138	74,032	19.07%	
Meeting Expenses					
Meetings	918	-	918		
Travel	1,501	4,000	(2,499)	-62.48%	
Conference Calls	-	-	-		
Total Meeting Expenses	2,419	4,000	(1,581)	-39.53%	
Operating Expenses					
Consultants & Contracts	265,966	177,500	88,466	49.84%	Costs were higher than budget due to SharePoint expansion.
Rent & Improvements	-	-	-		
Office Costs	167,837	143,900	23,937	16.63%	
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	410,259	305,665	104,594	34.22%	Impact of depreciating building improvements, equipment, and other capital investments related to our facility move in 2012
Total Operating Expenses	844,062	627,065	216,997	34.61%	
Indirect Expenses	(1,308,651)	(1,019,203)	(289,448)	28.40%	
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	-	-	-		
Change in Assets (A - B)	-	-	-		
Fixed Assets					
Depreciation	(410,259.00)	(305,665.00)	(104,594)	34.22%	
Computer & Software CapEx	420,386	339,851	80,535	23.70%	
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
(Inc)Dec in Fixed Assets	$ 10,127	$ 34,186	$ (24,059)		
Allocation of Fixed Assets	(10,127)	(34,186)	24,059	-70.38%	Total actual fixed costs were under budget, therefore there were less asset costs than budgeted allocated to this program
Total Inc(Dec) in Fixed Assets ©	-	-	-		
TOTAL BUDGET (B + C)	-	-	-		
Change in Working Capital (A-B-C)	-	-	-		
FTEs	**3.6**	**3.1**	0.5	**15.16%**	

Midwest Reliability Organization
2012 Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013
~~**Per Audit**~~

HUMAN RESOURCES	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	-	-	-		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		Human Resources costs are included under the Finance and Accounting program.
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	-	-	-		
Expenses					
Personnel Expenses					
Salaries	-	-	-		
Payroll Taxes	-	-	-		
Employee Benefits	-	-	-		
Savings & Retirement	-	-	-		
Total Personnel Expenses	-	-	-		
Meeting Expenses					
Meetings	-	-	-		
Travel	-	-	-		
Conference Calls	-	-	-		
Total Meeting Expenses	-	-	-		
Operating Expenses					
Consultants & Contracts	-	-	-		
Rent & Improvements	-	-	-		
Office Costs	-	-	-		
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	-	-	-		
Indirect Expenses	-	-	-		
	-	-			
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	-	-	-		
Change in Assets (A - B)	-	-	-		
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
(Inc)Dec in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B + C)	-	-	-		
Change in Working Capital (A-B-C)	-	-	-		
FTEs	-	-	-		

Midwest Reliability Organization
2012 Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013
Per Audit

ACCOUNTING and FINANCE	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	-		-		
Penalty Sanctions	-		-		
Total ERO Funding	$ -	$ -	$ -		
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	-	-	-		
Expenses					
Personnel Expenses					
Salaries	313,002	290,826	22,176	7.63%	
Payroll Taxes	22,907	20,485	2,422	11.82%	
Employee Benefits	32,807	32,351	456	1.41%	
Savings & Retirement	52,546	56,737	(4,191)	-7.39%	
Total Personnel Expenses	421,262	400,399	20,863	5.21%	
Meeting Expenses					
Meetings	57	-	57		
Travel	3,733	3,000	733	24.43%	
Conference Calls	296	-	296		
Total Meeting Expenses	4,086	3,000	1,086	36.20%	
Operating Expenses					
Consultants & Contracts	44,716	45,500	(784)	-1.72%	
Rent & Improvements	487,109	528,827	(41,718)	-7.89%	
Office Costs	79,799	83,920	(4,121)	-4.91%	
Professional Services	52,724	79,000	(26,276)	-33.26%	An IT intrusion test was scheduled in 2013; however the test was not done due to the significant network changes that were planned and implemented in the course of the year. MRO currently has an intrusion test scheduled for the 2nd Qtr of 2014
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	664,348	737,247	(72,899)	-9.89%	
Indirect Expenses	(895,392)	(1,140,646)	245,254	-21.50%	
Other Non-Operating Expenses	(194,304)	-	(194,304)		
Total Expenses (B)	-	-	-		
Change in Assets (A - B)	-	-	-		
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	37,162	-	37,162		
Equipment CapEx	-	-	-		
Leasehold Improvements	(15,342)	50,000	(65,342)	-130.68%	The planned improvements for 2013 were completed in 2012
(Inc)Dec in Fixed Assets	$ 21,820	$ 50,000	$ (28,180)		
Allocation of Fixed Assets	(21,820)	(50,000)	28,180	-56.36%	Total actual fixed costs were under budget, therefore there were less asset costs than budgeted allocated to this program
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B + C)	-	-	-		
Change in Working Capital (A-B-C)	-	-	-		
FTEs	**3.1**	**3.0**	0.1	**2.99%**	

Statement of Activities and Capital Expenditures by Program 2013 Actual	Total	Statutory Total	Non-Statutory Total	Functions in Delegation Agreement: Statutory Total	Reliability Standards (Section 300)	Compliance and Organization Registration and Certification (Section 400 & 500)	Reliability Assessment and Performance Analysis (Section 800)	Training and Education (Section 600 & 900)	Situation Awareness and Infrastructure Security (Section 1000)	Committee and Member Forums	General and Administrative	Legal and Regulatory	Information Technology	Human Resources	Accounting and Finance	Non-Statutory Functions: Non-Statutory Total
Funding																
ERO Funding																
NERC Assessments	9,098,927	9,098,927	-	9,098,927	542,840	6,126,145	2,274,076	229,281	97,197		(170,612)					
Penalty Sanctions	14,000	14,000	-	14,000	762	9,581	3,370	136	151							
Total NERC Funding	**9,112,927**	**9,112,927**	**-**	**9,112,927**	**543,602**	**6,135,726**	**2,277,446**	**229,417**	**97,348**	**-**	**(170,612)**	**-**	**-**	**-**	**-**	**-**
Membership Dues	-	-	-							-						
Testing Fees	-	-	-													
Services & Software	-	-	-													
Workshops	-	-	-													
Interest	-	-	-													
Miscellaneous	-	-	-													
Total Funding (A)	**9,112,927**	**9,112,927**	**-**	**9,112,927**	**543,602**	**6,135,726**	**2,277,446**	**229,417**	**97,348**	**-**	**(170,612)**	**-**	**-**	**-**	**-**	**-**
Expenses																
Personnel Expenses																
Salaries	4,760,887	4,760,887	-	4,760,887	165,904	2,373,856	819,315	77,308	27,834	153,795	290,642	195,380	343,851	-	313,002	
Payroll Taxes	310,790	310,790	-	310,790	9,913	156,873	52,710	3,320	2,091	11,411	14,177	12,707	24,681	-	22,907	
Benefits	380,894	380,894	-	380,894	11,425	199,853	71,461	3,744	2,118	6,777	14,934	2,110	35,665	-	32,807	
Retirement Costs	724,304	724,304	-	724,304	27,194	318,341	149,493	12,525	4,134	29,487	44,544	28,067	57,973	-	52,546	
Total Personnel Expenses	6,176,875	6,176,875	-	6,176,875	214,436	3,048,923	1,092,979	96,897	36,177	201,470	364,297	238,264	462,170	-	421,262	-
Meeting Expenses																
Meetings	91,601	91,601	-	91,601	843	2,794	7,316	56,428	24	-	23,221	-	918	-	57	
Travel	475,018	475,018	-	475,018	19,540	130,092	147,655	12,313	11,149	66,519	73,098	9,418	1,501	-	3,733	
Conference Calls	15,141	15,141	-	15,141	9,682	2,793	2,207	-	-	-	163	-	-	-	296	
Total Meeting Expenses	581,760	581,760	-	581,760	30,065	135,679	157,178	68,741	11,173	66,519	96,482	9,418	2,419	-	4,086	-
Operating Expenses																
Consultants & Contracts	490,647	490,647	-	490,647	12,000	105,498	60,555	-	-	-	1,912	-	265,966	-	44,716	
Office Rent	487,109	487,109	-	487,109	-	-	-	-	-	-	-	-	-	-	487,109	
Office Costs	443,188	443,188	-	443,188	2,436	85,015	24,140	349	3,688	-	74,806	5,118	167,837	-	79,799	
Professional Services	147,339	147,339	-	147,339	-	-	-	-	-	-	72,500	22,115	-	-	52,724	
Miscellaneous	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Depreciation	410,259	410,259	-	410,259	-	-	-	-	-	-	-	-	410,259	-	-	
Total Operating Expenses	1,978,542	1,978,542	-	1,978,542	14,436	190,513	84,695	349	3,688	-	149,218	27,233	844,062	-	664,348	-
Total Direct Expenses	**8,737,177**	**8,737,177**	**-**	**8,737,177**	**258,937**	**3,375,115**	**1,334,852**	**165,987**	**51,038**	**267,989**	**609,997**	**274,915**	**1,308,651**	**-**	**1,089,696**	**-**
Indirect Expenses	-	-	-	-	121,279	2,298,406	878,387	38,856	20,017	(267,989)	(609,997)	(274,915)	(1,308,651)	-	(895,392)	-
Other Non-Operating Expenses	**(194,304)**	**(194,304)**	**-**	**(194,304)**							-	-	-	-	(194,304)	-
Total Expenses (B)	**8,542,873**	**8,542,873**	**-**	**8,542,873**	**380,216**	**5,673,521**	**2,213,239**	**204,843**	**71,055**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
Change in Assets	**570,054**	**570,054**	**-**	**570,054**	**163,386**	**462,205**	**64,207**	**24,574**	**26,293**	**-**	**(170,612)**	**-**	**-**	**-**	**-**	**-**
Fixed Assets																
Depreciation	(410,259)	(410,259)	-	(410,259)	-	-	-	-	-	-	-	-	(410,259)	-	-	-
Computer & Software CapEx	420,386	420,386	-	420,386									420,386		-	-
Furniture & Fixtures CapEx	37,162	37,162	-	37,162											37,162	-
Equipment CapEx	-	-	-	-											-	-
Leasehold Improvements	(15,342)	(15,342)	-	(15,342)											(15,342)	-
Allocation of Fixed Assets	-	-	-	-	1,154	21,873	8,359	370	190		-	-	(10,127)	-	(21,820)	-
Inc(Dec) in Fixed Assets (C)	**31,947**	**31,947**	**-**	**31,947**	**1,154**	**21,873**	**8,359**	**370**	**190**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
TOTAL BUDGET (=B + C)	**8,574,820**	**8,574,820**	**-**	**8,574,820**	**381,370**	**5,695,394**	**2,221,598**	**205,213**	**71,245**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	**538,107**	**538,107**	**-**	**538,107**	**162,232**	**440,332**	**55,848**	**24,204**	**26,103**	**-**	**(170,612)**	**-**	**-**	**-**	**-**	**-**
FTEs	**37.91**	**37.91**	**-**	**37.91**	**1.03**	**19.52**	**7.46**	**0.33**	**0.17**	**-**	1.61	1.12	3.57	-	3.10	**-**

MIDWEST RELIABILITY ORGANIZATION

Saint Paul, Minnesota

FINANCIAL STATEMENTS

Including Independent Auditors' Report

As of and for the Years Ended December 31, 2013 and 2012

MIDWEST RELIABILITY ORGANIZATION

TABLE OF CONTENTS

INDEPENDENT AUDITORS' REPORT	1
FINANCIAL STATEMENTS	
Statements of Financial Position	2
Statements of Operations and Members' Equity	3
Statements of Cash Flows	4
Notes to Financial Statements	5 - 12

BAKER TILLY
VIRCHOW KRAUSE, LLP

Baker Tilly Virchow Krause, LLP
225 S Sixth St, Ste 2300
Minneapolis, MN 55402-4661
tel 612 876 4500
fax 612 238 8900
bakertilly.com

INDEPENDENT AUDITORS' REPORT

To the Board of Directors and Members
Midwest Reliability Organization
Saint Paul, Minnesota

Report on the Financial Statements

We have audited the accompanying financial statements of Midwest Reliability Organization (the "Organization"), which comprise the statements of financial position as of December 31, 2013 and 2012, and the related statements of operations and members' equity and cash flows for the years then ended, and the related notes to the financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibility

Our responsibility is to express an opinion on these financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of the Organization as of December 31, 2013 and 2012, and the changes in its net assets and its cash flows for the years then ended in accordance with accounting principles generally accepted in the United States of America.

Baker Tilly Virchow Krause, LLP

Minneapolis, Minnesota
April 3, 2014

An Affirmative Action Equal Opportunity Employer

MIDWEST RELIABILITY ORGANIZATION

STATEMENTS OF FINANCIAL POSITION
As of December 31, 2013 and 2012

	2013	2012
ASSETS		
CURRENT ASSETS		
Cash and cash equivalents	$ 3,739,704	$ 3,190,832
Restricted cash	136,516	14,002
Accounts receivable	34,726	191,366
Prepaid expenses	263,633	200,276
Total Current Assets	4,174,579	3,596,476
PROPERTY, IMPROVEMENTS AND EQUIPMENT, NET	1,194,569	1,234,867
OTHER ASSETS		
Restricted cash - non-current	320,013	104,003
Security Deposit - non-current	39,858	39,858
Capitalized software costs, net of accumulated amortization of $439,510 and $384,099, respectively	186,220	113,975
TOTAL ASSETS	$ 5,915,239	$ 5,089,179
LIABILITIES AND MEMBERS' EQUITY		
CURRENT LIABILITIES		
Accounts payable - trade	$ 207,901	$ 391,426
Accrued liabilities	638,307	580,367
Retirement plan contribution	407,436	357,800
Deferred assessments	136,512	14,002
Total Current Liabilities	1,390,156	1,343,595
OTHER LIABILITIES		
Postretirement medical benefit obligation	153,171	347,334
Deferred assessments - non-current	320,013	104,003
Deferred rent - non-current	309,572	121,976
Total Liabilities	2,172,912	1,916,908
MEMBERS' EQUITY	3,742,327	3,172,271
TOTAL LIABILITIES AND MEMBERS' EQUITY	$ 5,915,239	$ 5,089,179

See accompanying notes to financial statements.

MIDWEST RELIABILITY ORGANIZATION

STATEMENTS OF OPERATIONS AND MEMBERS' EQUITY
For the Years Ended December 31, 2013 and 2012

	2013	2012
REVENUE		
Assessments	$ 9,098,927	$ 8,349,029
Penalty sanctions	14,000	418,499
Total Revenue	9,112,927	8,767,528
EXPENSES		
Personnel expenses		
Salaries	4,760,887	4,358,348
Payroll taxes	310,791	254,397
Employee benefits	380,894	333,704
Retirement benefits	724,304	730,571
Total personnel expenses	6,176,876	5,677,020
Meeting expenses		
Conference calls	15,142	23,501
Meetings	91,601	55,278
Travel	475,020	424,881
Total meeting expenses	581,763	503,660
Operating expenses		
Building rent and facilities	487,109	351,209
Consulting	490,643	507,918
Office costs	853,446	969,798
Professional services	147,338	63,768
Total operating expenses	1,978,536	1,892,693
Total Expenses	8,737,175	8,073,373
CHANGE IN MEMBERS' EQUITY BEFORE POSTRETIREMENT RELATED CHANGES	375,752	694,155
POSTRETIREMENT-RELATED CHANGES		
Postretirement medical benefit obligation changes other than net periodic cost	(194,304)	51,965
CHANGE IN MEMBERS' EQUITY	570,056	642,190
MEMBERS' EQUITY - Beginning of Year	3,172,271	2,530,081
MEMBERS' EQUITY - END OF YEAR	$ 3,742,327	$ 3,172,271

See accompanying notes to financial statements.

MIDWEST RELIABILITY ORGANIZATION

STATEMENTS OF CASH FLOWS
For the Years Ended December 31, 2013 and 2012

	2013	2012
CASH FLOWS FROM OPERATING ACTIVITIES		
Change in members' equity	$ 570,056	$ 642,190
Adjustments to reconcile excess of revenues over expenses to net cash provided by operating activities		
Depreciation and software amortization	410,259	497,618
Change in assets and liabilities:		
Accounts receivable	156,640	(191,366)
Prepaid expenses	(63,357)	(69,377)
Security deposit	-	-
Accounts payable - trade	(128,156)	(17,846)
Accrued liabilities	57,940	86,846
Retirement plan contribution	49,636	48,436
Deferred assessments	338,520	(310,539)
Deferred rent	187,596	74,232
Postretirement medical benefit obligation	(194,163)	159,270
Change from Operating Activities	1,384,971	919,464
CASH FLOWS FROM INVESTING ACTIVITIES		
Change in restricted cash	(338,524)	310,540
Purchases of property, improvements and equipment and software	(497,575)	(1,082,142)
Change from Investing Activities	(836,099)	(771,602)
Net Change in Cash and Cash Equivalents	548,872	147,862
CASH AND CASH EQUIVALENTS - BEGINNING OF YEAR	3,190,832	3,042,970
CASH AND CASH EQUIVALENTS - END OF YEAR	$ 3,739,704	$ 3,190,832
Supplemental cash flow disclosure		
Equipment and software additions included in accounts payable	$ 53,795	$ 109,164

See accompanying notes to financial statements.

NOTE 1 - SIGNIFICANT ACCOUNTING POLICIES

Services

Midwest Reliability Organization (or the "Organization") is a nonprofit organization dedicated to ensuring the reliability of the bulk power system in the north-central part of North America. The Organization is a Regional Entity under the Energy Policy Act of 2005 (United States) and operates under delegated authority from the Federal Energy Regulatory Commission (FERC) via a delegation agreement with the North American Reliability Corporation. Additionally, the Organization operates in the provinces of Saskatchewan and Manitoba through other agreements. The primary focus of the Organization is ensuring compliance with reliability standards utilizing open, fair processes in the public interest and providing assessments on bulk power system reliability. In addition to the Board of Directors, Midwest Reliability Organization has formed four standing committees: Compliance Committee, Planning Committee, Operating Committee and the Standards Committee. The Board of Directors has four committees: Finance and Audit Committee, Governance and Personnel Committee, Dispute Resolution Committee and Hearing Body Committee.

Cash and Cash Equivalents

The Organization considers all highly liquid investments with original maturities of three months or less to be cash equivalents. Cash and cash equivalents are held by one financial institution, Wells Fargo, in three accounts. Escrowed amounts resulting from penalties assessed and collected in the United States are segregated into a separate account.

Receivables

Receivables, if any, result primarily from assessments related to load serving entities (members and nonmembers). No allowance for doubtful accounts is recorded based on historical experience and management's evaluation of receivables. Bad debts are expensed when deemed uncollectible. Receivables are generally unsecured.

Property, Improvements and Equipment

Property, improvements and equipment are stated at cost less accumulated depreciation and amortization. Significant additions or improvements exceeding $3,000 and $2,000 are capitalized for the years ended December 31, 2013 and 2012, respectively, while expenditures for maintenance and repairs are charged to operations as incurred. Depreciation is recorded using the straight-line method over the estimated useful lives of the assets, ranging from three to seven years. Leasehold improvements are amortized using the straight-line method over the shorter of the estimated useful life or the remaining lease term. The cost and related accumulated depreciation of assets sold or disposed of are removed from the accounts, and the resulting gain or loss is included in operations.

Capitalized Software Costs

The Organization capitalizes software development costs incurred and purchased software in upgrading computer software used internally to serve its members. The Organization begins capitalization of these costs after technological feasibility has been determined. The capitalized software, once placed in service, is amortized on the straight-line method over its estimated useful life of three years. Accumulated amortization totaled $439,510 and $384,099 for the years ended December 31, 2013 and 2012, respectively. Amortization expense totaled $55,411 and $108,054 for the years ended December 31, 2013 and 2012, respectively.

NOTE 1 - SIGNIFICANT ACCOUNTING POLICIES (Continued)

Deferred Assessments

Deferred assessments represents penalty assessments paid by load-serving entities, which will be used to offset budget allocations received from NERC.

Tax Status

The Internal Revenue Service has determined that the Organization is exempt from federal income taxes under Section 501(c)(6) of the Internal Revenue Code. They are also exempt from state income taxes. However, any unrelated business income may be subject to taxation.

The Organization follows the accounting standards for contingencies in evaluating uncertain tax positions. This guidance prescribes recognition threshold principles for the financial statement recognition of tax positions taken or expected to be taken on a tax return that are not certain to be realized. No liability has been recognized by the Organization for uncertain tax positions as of December 31, 2013 and 2012. The Organization's tax returns are subject to review and examination by federal and state authorities. The tax returns for the current year as well as fiscal years 2010 and thereafter are open to examination by federal and state authorities.

Revenue and Assessments

The Organization receives its revenues from NERC through a net energy-to-load allocation for all load-serving entities within its geographical area. The revenue allocation is prescribed under the Energy Policy Act of 2005 in the United States and similar arrangements in Saskatchewan and Manitoba. Any other revenues are collected on a fee-for-service basis at no cost, if applicable.

Use of Estimates

The preparation of financial statements in conformity with accounting principles generally accepted in the United States of America requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities and disclosure of contingent assets and liabilities at the date of the financial statements and the reported amounts of revenues and expenses during the reporting period. Actual results could differ from those estimates.

Subsequent Events

The Organization has evaluated subsequent events through April 3, 2014, which is the date that the financial statements were approved and available to be issued.

NOTE 2 - NERC TRANSACTIONS

On October 30, 2007 the Organization entered into a delegation agreement with the North American Electric Reliability Corporation ("NERC") with an executed version dated April 5, 2008 to enforce the Reliability Standards as set by NERC within a designated region. The delegation agreement, which was set to expire in May 2010, was approved for extension by FERC through May 2, 2011. The Organization and NERC completed work on a five-year delegation agreement which was executed and approved by FERC effective January 1, 2011. In connection with the current delegation agreement, the Organization has the ability to propose Reliability Standards and Regional Variances. The Organization has the authority to enforce the Reliability Standards as set by NERC and approved by regulatory authorities within the geographic boundaries. The Organization is subject to oversight from NERC and applicable regulations in the United States, Manitoba, and Saskatchewan.

To ensure the delegated functions have reasonable funding, NERC is to fund the Organization with the monies necessary to carry out its activities as per the agreement. A formula is devised that equitably allocates charges among the end users within the boundaries served by the Organization, based on net energy for load or through such other formula as provided. The Organization provides NERC with a board approved annual operating budget on or before June 30 of each year. Budgeted revenues from NERC were $9,098,927 and $8,349,029 for the years ended December 31, 2013 and 2012, respectively, which agree with the amounts received.

NOTE 3 - LEASE COMMITMENTS

The Organization executed an operating lease for office space in St Paul, Minnesota on January 20, 2012. Rent expense was $237,745 and $330,188 for the years ended December 31, 2013 and 2012, respectively.

Future expected minimum lease payments under the lease as of December 31, 2013 are as follows:

Years Ending December 31	
2014	$ 94,376
2015	266,514
2016	274,537
2017	282,812
2018	291,277
Thereafter	1,200,135
	$ 2,409,651

NOTE 4 - PROPERTY, IMPROVEMENTS AND EQUIPMENT

The following is a schedule of property, improvements and equipment as of December 31:

	2013	2012
Equipment	$ 1,731,631	$ 1,403,378
Furniture	422,802	421,164
Leasehold improvements	321,206	336,548
	2,475,639	2,161,090
Less: Accumulated depreciation	(1,281,070)	(926,223)
Net Property, Improvements and Equipment	$ 1,194,569	$ 1,234,867

NOTE 5 - LINE OF CREDIT

The Organization obtained a revolving line of credit from National Cooperative Service Corporation (NCSC) in February 2008. The line of credit has a credit limit of $2,000,000 and an interest rate equal to the NCSC Line of Credit Rate in effect from time to time, not to exceed the Prevailing Bank Prime Rate as published in the "Money Rates" column of the eastern edition of the *Wall Street Journal* on the publication day immediately preceding the day on which an adjustment in the interest rate becomes effective. The Organization is required to maintain a Debt Service Coverage Ratio of not less than 1.00. The line of credit is secured by substantially all assets of the Organization, and expires on February 26, 2017. There were no outstanding balances at December 31, 2013 or 2012, respectively.

NOTE 6 - RETIREMENT PLANS

Postretirement Health Plan

The Organization has a defined benefit postretirement health plan available to eligible current and future retirees. Information regarding the plan as of December 31 was as follows:

	2013	2012
Change in projected benefit obligation		
Benefit obligation at beginning of year	$ 880,141	$ 662,945
Service cost	169,757	146,199
Interest cost	36,195	29,632
Plan changes	-	-
Actuarial (gain) loss	(200,476)	44,362
Benefits paid	(3,222)	(2,997)
Benefit obligation at end of year	882,395	880,141
Change in plan assets		
Fair value of plan assets at beginning of year	532,807	474,881
Actual return on plan assets	59,097	57,926
Employer contribution	140,542	2,997
Benefits paid	(3,222)	(2,997)
Fair value of plan assets at end of year	729,224	532,807
Unfunded status recognized as a noncurrent liability	$ (153,171)	$ (347,334)
Weighted average assumptions used to calculate the benefit obligation-discount rate	5.04%	4.12%

Net periodic postretirement benefit expense for the years ending December 31 is comprised of the following:

	2013	2012
Components of net periodic benefit cost		
Service cost	$ 169,757	$ 146,199
Interest cost	36,195	29,632
Expected return on plan assets	(35,073)	(35,173)
Amortization of prior service credit	(38,601)	(38,601)
Amortization of actuarial loss	8,405	8,245
Net periodic benefit cost	$ 140,683	$ 110,302
Weighted-average assumptions used to calculate the net periodic benefit cost		
Discount rate	4.12%	4.48%
Expected return on plan assets	6.00%	7.00%
Rate of compensation increases	N/A	N/A

The expected rates of return on plan assets are based on the weighting of the Organization's asset allocations, the 30-year rolling historical average returns, and recent historical average return.

NOTE 6 - RETIREMENT PLANS (Continued)

Assumed health care cost trend rates at December 31 consist of the following:

	2013	2012
Health care cost trend rate assumed for next year	10.1%	10.6%
Rate to which the cost trend rate is assumed to decline (the ultimate trend rate)	5.0%	5.0%
Year that the rate reaches the ultimate trend rate	2025	2025

Assumed health care cost trend rates have a significant effect on the amounts reported for the health care plan. A one-percentage point change in assumed health care trend rates would have the following effects:

	One-Percentage Point	
	Increase	Decrease
Effect on total of service cost and interest cost	$ 52,259	$ (39,675)
Effect on postretirement benefit obligation	194,953	(151,445)

Plan related changes other than net periodic cost included in retirement benefit expense:

	2013	2012
Actuarial (gain) loss arising during the year	$ (232,905)	$ 13,364
Amortization of prior year service cost	38,601	38,601
	$ (194,304)	$ 51,965

The Organization employs a total return investment approach for plan assets with a mix of equity and debt investments used to maximize the long-term appreciation of plan assets for a prudent level of risk. The Organization's plan assets are invested in various funds, which consist of both stocks and bonds. The equity component includes investment in companies of various sizes, with an emphasis on large cap stocks, and represents several investment styles. The equity portion also includes an allocation to international stocks. Investments in bonds are diversified into three portfolios that invest mainly in U.S. treasuries, high quality corporate issues and mortgage securities.

NOTE 6 - RETIREMENT PLANS (Continued)

The fair values of the Organization's postretirement health plan assets at December 31, by asset category, are as follows:

	2013 Quoted Prices in Active Markets for Identical Assets (Level 1)	2012 Quoted Prices in Active Markets for Identical Assets (Level 1)
Asset category		
Cash equivalents	$ 7,490	$ 11,418
Mutual funds-bonds	383,724	322,492
Mutual funds-equities	265,854	159,657
Mutual funds-balanced	72,156	39,240
	$ 729,224	$ 532,807

Cash equivalents - Investments in cash equivalents consist of money market funds and are classified as Level 1 as they are traded in an active market for which closing prices are readily available.

Mutual Funds - Investments in mutual funds are classified as Level 1 as they are traded in an active market for which closing prices are readily available.

While the plan believes its valuation methods are appropriate and consistent with other market participants, the use of different methodologies or assumptions to determine the fair value of certain financial instruments could result in a different estimate of fair value at the reporting date.

Estimated future benefit payments (which reflect expected future service, as appropriate) as of December 31, 2013 are as follows:

Years Ending December 31	
2014	$ 5,259
2015	6,772
2016	7,947
2017	12,769
2018	22,279
2019 - 2023	281,585

It is reasonably possible that changes in these estimates could occur in the near term and that actual results could differ from these estimates and could have a material effect on the financial statements.

The Organization expects to contribute $105,536 to the plan in 2014.

NOTE 6 - RETIREMENT PLANS (Continued)

Defined Contribution Pension Plan

In 2009, the Organization established a thrift savings plan to replace the terminated multiple-employer plan for the benefit of its employees. The Organization's previous 401(k) plan was converted into the new plan as well as the establishment of a new, non-elective employer contribution plan. In order to participate in the plan, employees must have attained age 20 and have completed one month of service. Employees may contribute up to the IRS limitations for their elective deferral, with a 50% matching contribution from the Organization. For employees to receive the non-elective or employer contribution, they must have worked 1,000 hours during the plan year. The Organization matched $241,044 and $202,250 of employee deferrals as of December 31, 2013 and 2012, respectively. In addition, the Organization elected to make an employer contribution in the amount of $370,263 and $352,412 for the years ended December 31, 2013 and 2012, respectively.

The Organization also established a 457B plan in 2010. Eligible employees may contribute an elective deferral, with a discretionary matching contribution from the Organization. Employee contributions were $16,226 and $14,200, for the years ended December 31, 2013 and 2012, respectively. The Organization matched $6,675 and $7,400, of employee deferrals for the years ended December 31, 2013 and 2012, respectively.

The Organization also established a 457F plan in 2011. Employer contribution amounts for employees in excess of IRS contribution limits are deposited to the 457F. The Organization contributed in the amounts of $20,950 and $11,579, for the years ended December 31, 2013 and 2012, respectively.

ATTACHMENT 4

2013 ACTUAL COST-TO-BUDGET COMPARISON

AND

2013 AUDITED FINANCIAL REPORT

FOR

NORTHEAST POWER COORDINATING COUNCIL, INC.

Via Email

NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS. NEW YORK. NY 10018 (212) 840-1070 FAX (212) 302-2782

April 28, 2014

North American Electric Reliability Corporation
3343 Peachtree Road, NE
Fourth Floor East Tower – Suite 400
Atlanta, Georgia 30326
Attention: Mr. Michael Walker

Subject: NPCC 2013 True Up Actual vs. Budget Variance Analysis
True Up Filing Based on Audited 2013 Financial Statements

Dear Michael:

Enclosed is the Northeast Power Coordinating Council, Inc. (NPCC) submittal regarding the 2013 NPCC actual vs. budget variances. NPCC's independent audit performed by Pricewaterhouse Coopers LLP was concluded on March 27, 2014 and forwarded to NERC for its information and provision to FERC.

As you know, NPCC is a Cross-border Regional Entity which provides Regional Entity functions and services through its regional entity (RE) division. The establishment of Regionally-specific criteria, and monitoring and enforcement of compliance with such criteria are provided through the criteria services (CS) division of NPCC. The CS division is funded by assessments to the Independent System Operators/Balancing Authority Areas within the Region based on their respective Net Energy for Load.

No Regional Entity division assessments were used to fund CS division activities. Allocation between the RE division and CS division represents a 94/6 split for 2013 based upon total corporate FTEs of 35.22 in the RE division and 2.14 in the CS division for the full year. No indirect costs were allocated from the CS division to the RE division and no cross subsidies exist. In addition, NPCC does not budget for interest income and reports such income apportioned based upon its Regional Entity (RE) and Criteria Services (CS) division full time equivalent (FTE) ratio.

Actual total expenses for NPCC's RE division for 2013 were $13,533,519 (excluding non-operating expenses which represent change in pension liability based upon actuarial review) which is $538,216 or 4% under the 2013 operating budget of $14,071,735. Actual total expenses for NPCC's CS division for 2013 were $863,318 (excluding non-operating expenses) which is $173,344 or 17% under the 2013 operating budget of $1,036,662. In the aggregate, actual total expenses for the NPCC RE and CS divisions were $14,396,839 which is $711,558 or nearly 5% under the 2013 total corporate budget of $15,108,397. Indirect expenses are allocated to the direct statutory programs based on FTE ratio. NPCC did not use operating cash reserves to fund any activities or services in 2013.

Significant aggregate expense variations for the Regional Entity division are explained on the following page:

Personnel Expenses

(Actual variance of $346k or 4% under budget at year end)

In 2013 NPCC experienced several partial year vacancies but ended the year fully staffed. Despite not being at a full staff complement at times during the year, NPCC performed all of its 2013 delegated responsibilities as well as its goals and objectives, including:

- Conducted 22 off-site Operations & Planning (O&P) audits, four on-site O&P audits, 39 off-site CIP audits, 11 on-site CIP audits and 483 individual spot checks involving 79 entities;
- Processed 153 Technical Feasibility Exceptions (TFE) from 23 entities, completed TFE Part B review of 135;
- Closed 180 violations;
- Accepted mitigation plans for 152 violations;
- Examined 87 events of which eight were category two or higher;
- Processed 35 new entity registrations, 19 entity removals, 17 entity name changes and three certifications.

WECC CEA Revenue and Expenses

(Actual variance of $75k or 218% over budget at year end)

WECC CEA related expenses and offsetting revenue were greater than budget in 2013 due to ongoing audit follow up and enforcement work resulting from the O&P and CIP audits conducted during 2012. The total actual expenses related to the WECC audits were trued up with WECC, as per the CEA Agreement.

Meeting Expenses

(Actual variance of $157k or 12% under budget at year end)

Continued efforts to hold more meetings onsite and at member facilities or via webinars have kept meeting expenses under budget. Additionally, in 2013 NPCC contracted with a more cost effective teleconference/webinar provider.

No funds were budgeted in association with NPCC conducting compliance hearings and no hearings have been initiated to date in NPCC.

Significant variances by program area are provided on a line-item basis using the template provided by NERC which presents actual and budgeted costs on program-by-program format. A single consolidated budget versus actual cost comparison is presented for Administrative Services in order to be consistent with the presentation in NPCC's 2013 Business Plan and Budget. Should you have any questions please do not hesitate to contact me via email at jhala@npcc.org or via telephone at (212) 840-1070.

Sincerely,

Jessica Hala

Jessica Hala
Manager, Finance and Accounting

JH: jh
Enclosures

cc: Mr. Edward A. Schwerdt – NPCC President & CEO
Ms. Jennifer Budd Mattiello – NPCC Vice President & COO

Northeast Power Coordinating Council, Inc.
2013 Statement of Activities Summary
Total NPCC (RE and CS Divisions)

	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)
Funding			
ERO Funding			
Assessments	12,352,264	12,352,265	-
Penalty Sanctions	297,301	297,301	-
Total ERO Funding	**12,649,565**	**12,649,566**	**-**
Federal Grants	-	-	-
Non-Statutory Assessments	1,139,690	1,139,690	-
Testing	-	-	-
Services & Software	-	-	-
Workshop Fees	58,650	80,000	(21,350)
Interest	17,281	-	17,281
Miscellaneous	109,867	34,500	75,367
Total Funding (A)	**13,975,053**	**13,903,756**	**71,298**
Expenses			
Personnel Expenses			
Salaries	5,738,140	5,946,022	(207,882)
Payroll Taxes	378,195	397,303	(19,108)
Employee Benefits	1,309,704	1,377,863	(68,159)
Savings & Retirement	1,171,746	1,233,209	(61,463)
Total Personnel Expenses	**8,597,785**	**8,954,397**	**(356,612)**
Meeting Expenses			
Meetings	331,604	397,000	(65,396)
Travel	799,657	910,000	(110,343)
Conference Calls	71,988	87,000	(15,012)
Total Meeting Expenses	**1,203,249**	**1,394,000**	**(190,751)**
Operating Expenses			
Consultants & Contracts	2,060,648	2,178,000	(117,352)
Rent & Improvements	740,699	706,500	34,199
Office Costs	540,884	468,500	72,384
Professional Services	910,220	1,120,000	(209,780)
Miscellaneous	43,094	80,000	(36,906)
Depreciation	300,260	207,000	93,260
Total Operating Expenses	**4,595,805**	**4,760,000**	**(164,195)**
Indirect Expenses	**-**	**-**	**-**
Other Non-Operating Expenses	**(2,541,035)**	**-**	**(2,541,034)**
Total Expenses (B)	**11,855,804**	**15,108,397**	**(3,252,592)**
Change in Assets (A - B)	**2,119,249**	**(1,204,641)**	**3,323,890**
Fixed Assets			
Depreciation	(300,260)	(207,000)	(93,260)
Computer & Software CapEx	167,230	-	167,230
Furniture & Fixtures CapEx	1,388	-	1,388
Equipment CapEx	-	-	-
Leasehold Improvements	-	-	-
Incr(Dec) in Fixed Assets	**(131,642)**	**(207,000)**	**75,358**
Allocation of Fixed Assets	(0)	-	(0)
Total Inc(Dec) in Fixed Assets (C)	**(131,642)**	**(206,997)**	**75,355**
TOTAL BUDGET (B + C)	**11,724,162**	**14,901,400**	**(3,177,237)**
Change in Working Capital (A-B-C)	**2,250,891**	**(997,645)**	**3,248,535**
FTE's	**37.36**	**38.00**	**(0.64)**

Northeast Power Coordinating Council, Inc.
2013 Statement of Activities Summary

NON-STATUTORY	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)	
Funding				
ERO Funding				
Assessments	-	-	-	
Penalty Sanctions	-	-	-	
Total ERO Funding	-	-	-	
Federal Grants	-	-	-	
Non-Statutory Assessments	1,139,690	1,139,690	-	0.00%
Testing	-	-	-	
Services & Software	-	-	-	
Workshop Fees	-	-	-	
Interest	547	-	547	
Miscellaneous	-	-	-	
Total Funding (A)	1,140,237	1,139,690	547	0.05%
Expenses				
Personnel Expenses				
Salaries	247,414	268,881	(21,467)	-7.98%
Payroll Taxes	15,240	19,614	(4,374)	-22.30%
Employee Benefits	67,957	46,561	21,396	45.95%
Savings & Retirement	134,183	140,645	(6,462)	-4.59%
Total Personnel Expenses	464,794	475,701	(10,907)	-2.29%
Meeting Expenses				
Meetings	3,602	20,000	(16,398)	-81.99%
Travel	37,492	55,000	(17,508)	-31.83%
Conference Calls	-	-	-	
Total Meeting Expenses	41,094	75,000	(33,906)	-45.21%
Operating Expenses				
Consultants & Contracts	1,425	65,000	(63,575)	-97.81%
Rent & Improvements	(933)	-	(933)	
Office Costs	967	-	967	
Professional Services	918	-	918	
Miscellaneous	583	-	583	
Depreciation	18,655	14,490	4,165	28.74%
Total Operating Expenses	21,615	79,490	(57,875)	-72.81%
Indirect Expenses	335,815	406,471	(70,656)	-17.38%
Other Non-Operating Expenses	(395,997)	-	(395,997)	
Total Expenses (B)	467,321	1,036,662	(569,341)	-54.92%
Change in Assets (A - B)	672,916	103,028	569,888	553.14%
Fixed Assets				
Depreciation	(18,655)	(14,490)	(4,165)	28.74%
Computer & Software CapEx	-	-	-	
Furniture & Fixtures CapEx	-	-	-	
Equipment CapEx	-	-	-	
Leasehold Improvements	-	-	-	
Incr(Dec) in Fixed Assets	(18,655)	(14,490)	(4,165)	
Allocation of Fixed Assets	-	-	-	
Total Inc(Dec) in Fixed Assets (C)	(18,655)	(14,490)	(4,165)	28.74%
TOTAL BUDGET (B + C)	**448,666**	**1,022,172**	**(573,506)**	**-56.11%**
Change in Working Capital (A-B-C)	**691,571**	**117,518**	**574,053**	488.48%
FTE's	**2.14**	**2.14**	**-**	**0.00%**

Northeast Power Coordinating Council, Inc.
2013 Statement of Activities Summary

TOTAL STATUTORY	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	12,352,264	12,352,265	-	0.00%	
Penalty Sanctions	297,301	297,301	-	0.00%	
Total ERO Funding	12,649,565	12,649,566	-	0.00%	
Federal Grants	-	-	-		
Non-Statutory Assessments	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	58,650	80,000	(21,350)	-26.69%	Actual fees charged per person for attending NPCC's standards and compliance workshops were less than originally budgeted.
Interest	16,734	-	16,734		Interest income, while not budgeted, was allocated by FTE ratio between statutory and non-statutory.
Miscellaneous	109,867	34,500	75,367	218.46%	WECC CEA actual expenses and offsetting revenue were greater than budget due to ongoing audit follow up and enforcement work resulting from the O&P and CIP audits conducted during 2012.
Total Funding (A)	12,834,816	12,764,066	70,751	0.55%	
Expenses					
Personnel Expenses					
Salaries	5,490,726	5,677,141	(186,415)	-3.28%	Under budget due to staff vacancies throughout the year and due to at risk compensation component based on corporate goal attainment and individual performance.
Payroll Taxes	362,955	377,689	(14,734)	-3.90%	Under budget due to staff vacancies throughout the year.
Employee Benefits	1,241,747	1,331,302	(89,555)	-6.73%	Under budget due to several employees opting out of health insurance coverage for superior coverage through a prior employer, as well as staff vacancies throughout the year.
Savings & Retirement	1,037,563	1,092,564	(55,001)	-5.03%	Under budget due to staff vacancies throughout the year.
Total Personnel Expenses	8,132,991	8,478,696	(345,705)	-4.08%	
Meeting Expenses					
Meetings	328,002	377,000	(48,998)	-13.00%	Continued efforts to hold more meetings onsite and at member facilities or via webinars have kept meeting expenses under budget.
Travel	762,165	855,000	(92,835)	-10.86%	Travel expenses were controlled by holding more meetings onsite or via webinars.
Conference Calls	71,988	87,000	(15,012)	-17.26%	Contracted with a more cost effective teleconference/webinar provider.
Total Meeting Expenses	1,162,155	1,319,000	(156,845)	-11.89%	
Operating Expenses					
Consultants & Contracts	2,059,223	2,113,000	(53,777)	-2.55%	
Rent & Improvements	741,632	706,500	35,132	4.97%	
Office Costs	539,917	468,500	71,417	15.24%	Over budget primarily related to computer supplies and maintenance due to additional software programs including Diligent Board Books, to support Directors' hardware.
Professional Services	909,302	1,120,000	(210,698)	-18.81%	Legal fees were less than budget due to judicious use of outside counsel.
Miscellaneous	42,511	80,000	(37,489)	-46.86%	Under budget due to ongoing cost cutting efforts in all areas.
Depreciation	281,605	192,510	89,095	46.28%	Over budget due to additional assets placed in service in 2013 related to CMEP Data Administration Application (CDAA) software development to enhance the efficiencies of compliance activities for both registered entities and Regional Entity staffs.
Total Operating Expenses	4,574,190	4,680,510	(106,320)	-2.27%	
Indirect Expenses	(335,817)	(406,471)	70,654	-17.38%	
Other Non-Operating Expenses	(2,145,038)	-	(2,145,037)		Decrease in NPCC's pension liability based on actuarial review at year end.
Total Expenses (B)	11,388,481	14,071,735	(2,683,253)	-19.07%	
Change in Assets (A - B)	1,446,335	(1,307,669)	2,754,004	-210.60%	
Fixed Assets					
Depreciation	(281,605)	(192,510)	(89,095)	46.28%	Over budget due to additional assets placed in service in 2013 related to CMEP Data Administration Application (CDAA) software development to enhance the efficiencies of compliance activities for both registered entities and Regional Entity staffs.
Computer & Software CapEx	167,230	-	167,230		Over budget due to capitalization of costs related to CMEP Data Administration Application (CDAA) software development not included in budget.
Furniture & Fixtures CapEx	1,388	-	1,388		Over budget due to office furniture purchase not included in budget.
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	(112,987)	(192,510)	79,523		
Allocation of Fixed Assets	(0)	-	(0)		
Total Inc(Dec) in Fixed Assets (C)	(112,987)	(192,507)	79,520	-41.31%	
TOTAL BUDGET (B + C)	**11,275,494**	**13,879,228**	**(2,603,733)**	**-18.76%**	
Change in Working Capital (A-B-C)	**1,559,322**	**(1,115,163)**	**2,674,484**	-239.83%	
FTE's	**35.22**	**35.86**	**(0.64)**	**-1.79%**	Fully staffed at year end; variance is due to temporary vacancies during the year.

Northeast Power Coordinating Council, Inc.
2013 Statement of Activities Summary

RELIABILITY STANDARDS	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	1,358,549	1,358,549	-	0.00%	
Penalty Sanctions	32,431	32,431		0.00%	
Total ERO Funding	1,390,980	1,390,980	-	0.00%	
Federal Grants	-	-	-		
Non-Statutory Assessments	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	1,390,980	1,390,980	-	0.00%	
Expenses					
Personnel Expenses					
Salaries	475,495	478,983	(3,488)	-0.73%	
Payroll Taxes	29,163	31,972	(2,809)	-8.79%	
Employee Benefits	96,128	101,361	(5,233)	-5.16%	
Savings & Retirement	70,714	78,141	(7,427)	-9.50%	
Total Personnel Expenses	671,500	690,457	(18,957)	-2.75%	
Meeting Expenses					
Meetings	1,665	30,000	(28,335)	-94.45%	Meeting expenses were under budget due to more meetings held at NPCC offices, member facilities or via webinar. Additionally, meetings that were previously allocated across all programs are now recorded to Admin and allocated through indirect expenses.
Travel	116,046	105,000	11,046	10.52%	Increased volume of meetings attended by staff but not hosted by NPCC.
Conference Calls	-	-	-		
Total Meeting Expenses	117,711	135,000	(17,289)	-12.81%	
Operating Expenses					
Consultants & Contracts	8,561	30,000	(21,439)	-71.46%	Under budget as a result of judicious use of contractor and consultant services to complement staff functions.
Rent & Improvements	-	-	-		
Office Costs	-	-	-		
Professional Services	-	-	-		
Miscellaneous	398	-	398		
Depreciation	-	-	-		
Total Operating Expenses	8,959	30,000	(21,041)	-70.14%	
Indirect Expenses	596,682	556,523	40,159	7.22%	
Other Non-Operating Expenses	(165,783)	-	(165,783)		Decrease in NPCC's pension liability based on actuarial review at year end.
Total Expenses (B)	1,229,069	1,411,980	(182,911)	-12.95%	
Change in Assets (A - B)	161,911	(21,000)	182,911	-871.00%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	(11,883)	(21,000)	9,117	-43.42%	
Total Inc(Dec) in Fixed Assets (C)	(11,883)	(21,000)	9,117	-43.42%	
TOTAL BUDGET (B + C)	**1,217,186**	**1,390,980**	**(173,794)**	**-12.49%**	
Change in Working Capital (A-B-C)	**173,794**	**-**	**173,794**		
FTE's	**2.93**	**2.93**	**-**	**0.00%**	

Northeast Power Coordinating Council, Inc.
2013 Statement of Activities Summary

WECC CEA Responsibilities	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)	Comments (Explain variances > +/- 10% and >$10,000)
Funding				
ERO Funding				
Assessments	-	-	-	
Penalty Sanctions	-	-		
Total ERO Funding	-	-	-	
Federal Grants	-	-	-	
Non-Statutory Assessments	-	-	-	
Testing	-	-	-	
Services & Software	-	-	-	
Workshop Fees	-	-	-	
Interest	-	-	-	
Miscellaneous	109,867	-	109,867	WECC CEA funds budgeted under Compliance are shown here. WECC CEA actual expenses and offsetting revenue were greater than budget due to ongoing audit follow up and enforcement work resulting from the O&P and CIP audits conducted during 2012.
Total Funding (A)	109,867	-	109,867	
Expenses				
Personnel Expenses				
Salaries	46,313	-	46,313	WECC CEA related expenses allocated from Compliance.
Payroll Taxes	-	-	-	
Employee Benefits	-	-	-	
Savings & Retirement	-	-	-	
Total Personnel Expenses	46,313	-	46,313	
Meeting Expenses				
Meetings	-	-	-	
Travel	1,971	-	1,971	WECC CEA related expenses allocated from Compliance.
Conference Calls	-	-	-	
Total Meeting Expenses	1,971	-	1,971	
Operating Expenses				
Consultants & Contracts	61,583	-	61,583	WECC CEA related expenses allocated from Compliance.
Rent & Improvements	-	-	-	
Office Costs	-	-	-	
Professional Services	-	-	-	
Miscellaneous	-	-	-	
Depreciation	-	-	-	
Total Operating Expenses	61,583	-	61,583	
Indirect Expenses	-	-	-	
Other Non-Operating Expenses	-	-	-	
Total Expenses (B)	109,867	-	109,867	
Change in Assets (A - B)	-	-	-	
Fixed Assets				
Depreciation	-	-	-	
Computer & Software CapEx	-	-	-	
Furniture & Fixtures CapEx	-	-	-	
Equipment CapEx	-	-	-	
Leasehold Improvements	-	-	-	
Incr(Dec) in Fixed Assets	-	-	-	
Allocation of Fixed Assets	-	-	-	
Total Inc(Dec) in Fixed Assets (C)	-	-	-	
TOTAL BUDGET (B + C)	**109,867**	**-**	**109,867**	
Change in Working Capital (A-B-C)	**-**	**-**	**-**	
FTE's	**-**	**-**	**-**	

Northeast Power Coordinating Council, Inc.
2013 Statement of Activities Summary

COMPLIANCE OPERATIONS, ENFORCEMENT and ORGANIZATION REGISTRATION	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	7,576,805	7,576,805	-	0.00%	
Penalty Sanctions	166,028	166,028	-	0.00%	
Total ERO Funding	7,742,833	7,742,833	-	0.00%	
Federal Grants	-	-	-		
Non-Statutory Assessments	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	34,500	(34,500)	-100.00%	WECC CEA funds budgeted under Compliance are shown separately under "WECC CEA." WECC CEA actual expenses and offsetting revenue were greater than budget due to ongoing audit follow up and enforcement work resulting from the O&P and CIP audits conducted during 2012.
Total Funding (A)	7,742,833	7,777,333	(34,500)	-0.44%	
Expenses					
Personnel Expenses					
Salaries	1,996,523	2,117,561	(121,038)	-5.72%	Under budget due allocation to WECC, temporary vacancies during the year and at risk compensation component based on corporate goal attainment and individual performance.
Payroll Taxes	137,249	152,612	(15,363)	-10.07%	Under budget due to temporary vacancies during the year and at risk compensation component based on corporate goal attainment and individual performance.
Employee Benefits	471,916	465,444	6,472	1.39%	
Savings & Retirement	240,820	302,129	(61,309)	-20.29%	Under budget due to temporary vacancies during the year.
Total Personnel Expenses	2,846,508	3,037,746	(191,238)	-6.30%	
Meeting Expenses					
Meetings	34,230	45,000	(10,770)	-23.93%	Meeting expenses were under budget due to more meetings held at NPCC offices, member facilities or via webinar. Additionally, meetings that were previously allocated across all programs are now recorded to Admin and allocated through indirect expenses.
Travel	309,852	375,000	(65,148)	-17.37%	Continued efforts to hold more meetings onsite or via webinars have kept travel expenses under budget.
Conference Calls	-	-	-		
Total Meeting Expenses	344,082	420,000	(75,918)	-18.08%	
Operating Expenses					
Consultants & Contracts	1,424,600	1,578,000	(153,400)	-9.72%	Under budget due to allocation to WECC and two on-site audits previously included in the 2013 schedule and budget being moved to 2014 so that NPCC led Certification Reviews of organizational and/or EMS changes by NPCC registered entities could be performed.
Rent & Improvements	-	-	-		
Office Costs	-	-	-		
Professional Services	-	-	-		
Miscellaneous	2,391	-	2,391		
Depreciation	-	-	-		
Total Operating Expenses	1,426,991	1,578,000	(151,009)	-9.57%	
Indirect Expenses	3,009,853	2,849,094	160,759	5.64%	
Other Non-Operating Expenses	(193,685)	-	(193,685)		Decrease in NPCC's pension liability based on actuarial review at year end.
Total Expenses (B)	7,433,749	7,884,840	(451,091)	-5.72%	
Change in Assets (A - B)	309,084	(107,507)	416,591	-387.50%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	(64,888)	(107,507)	42,619	-39.64%	
Total Inc(Dec) in Fixed Assets (C)	(64,888)	(107,507)	42,619	-39.64%	
TOTAL BUDGET (B + C)	**7,368,861**	**7,777,333**	**(408,472)**	**-5.25%**	
Change in Working Capital (A-B-C)	**373,972**	**-**	**373,972**		
FTE's	**14.69**	**15.00**	**(0.31)**	**-2.09%**	Fully staffed at year end; variance is due to temporary vacancies during the year.

Northeast Power Coordinating Council, Inc.
2013 Statement of Activities Summary

RELIABILITY ASSESSMENTS and PERFORMANCE ANALYSIS	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	2,892,110	2,892,110	-	0.00%	
Penalty Sanctions	64,529	64,529		0.00%	
Total ERO Funding	2,956,639	2,956,639	-	0.00%	
Federal Grants	-	-	-		
Non-Statutory Assessments	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	2,956,639	2,956,639	-	0.00%	
Expenses					
Personnel Expenses					
Salaries	807,219	938,733	(131,514)	-14.01%	Under budget due to turnover and at risk compensation component based on corporate goal attainment and individual performance.
Payroll Taxes	56,613	63,449	(6,836)	-10.77%	Under budget due to turnover resulting in temporary vacancies.
Employee Benefits	209,508	215,362	(5,854)	-2.72%	Under budget due to several employees opting out of health insurance coverage for superior coverage through a prior employer, as well as staff vacancies throughout the year.
Savings & Retirement	169,223	183,530	(14,307)	-7.80%	
Total Personnel Expenses	1,242,563	1,401,074	(158,511)	-11.31%	
Meeting Expenses					
Meetings	34,968	45,000	(10,032)	-22.29%	Meeting expenses were under budget due to more meetings held at NPCC offices or via webinar. Additionally, meetings that were previously allocated across all programs are now recorded to Admin and allocated through indirect expenses.
Travel	183,027	160,000	23,027	14.39%	Travel expenses exceeded budget due to travel associated with Bulk Electric System definition related meetings.
Conference Calls	-	-	-		
Total Meeting Expenses	217,995	205,000	12,995	6.34%	
Operating Expenses					
Consultants & Contracts	335,011	285,000	50,011	17.55%	Over budget due primarily due to consulting associated with revision of the Bulk Electric System definition.
Rent & Improvements	-	-	-		
Office Costs	-	-	-		
Professional Services	-	-	-		
Miscellaneous	1,409	-	1,409		
Depreciation	-	-	-		
Total Operating Expenses	336,420	285,000	51,420	18.04%	
Indirect Expenses	1,131,642	1,107,348	24,294	2.19%	
Other Non-Operating Expenses	(443,660)	-	(443,660)		Decrease in NPCC's pension liability based on actuarial review at year end.
Total Expenses (B)	2,484,960	2,998,422	(513,462)	-17.12%	
Change in Assets (A - B)	471,679	(41,783)	513,462	-1228.88%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	(23,644)	(41,783)	18,139	-43.41%	
Total Inc(Dec) in Fixed Assets (C)	(23,644)	(41,783)	18,139	-43.41%	
TOTAL BUDGET (B + C)	**2,461,316**	**2,956,639**	**(495,323)**	**-16.75%**	
Change in Working Capital (A-B-C)	**495,323**	**-**	**495,323**		
FTE's	**5.50**	**5.83**	**(0.33)**	**-5.66%**	Fully staffed at year end; variance is due to temporary vacancies during the year.

Northeast Power Coordinating Council, Inc.
2013 Statement of Activities Summary

TRAINING, EDUCATION and OPERATOR CERTIFICATION	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	136,510	136,510	-	0.00%	
Penalty Sanctions	1,107	1,107		0.00%	
Total ERO Funding	137,617	137,617	-	0.00%	
Federal Grants	-	-	-		
Non-Statutory Assessments	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	58,650	80,000	(21,350)	-26.69%	Actual fees charged per person for attending NPCC's standards and compliance workshops were less than originally budgeted.
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	196,267	217,617	(21,350)	-9.81%	
Expenses					
Personnel Expenses					
Salaries	19,084	17,338	1,746	10.07%	
Payroll Taxes	1,138	1,088	50	4.60%	
Employee Benefits	4,539	4,129	410	9.93%	
Savings & Retirement	4,712	4,785	(73)	-1.53%	
Total Personnel Expenses	29,473	27,340	2,133	7.80%	
Meeting Expenses					
Meetings	125,541	152,000	(26,459)	-17.41%	Workshop expenses were less than budgeted as a result of lower negotiated rates and more meetings held at NPCC offices, member facilities or via webinar.
Travel	2,507	20,000	(17,493)	-87.47%	Under budget due to more meetings held at NPCC offices or via webinar.
Conference Calls	-	-	-		
Total Meeting Expenses	128,048	172,000	(43,952)	-25.55%	
Operating Expenses					
Consultants & Contracts	3,088	-	3,088		
Rent & Improvements	-	-	-		
Office Costs	-	-	-		
Professional Services	-	-	-		
Miscellaneous	1,666	-	1,666		
Depreciation	-	-	-		
Total Operating Expenses	4,754	-	4,754		
Indirect Expenses	20,209	18,994	1,215	6.40%	
Other Non-Operating Expenses	(15,087)	-	(15,087)		Decrease in NPCC's pension liability based on actuarial review at year end.
Total Expenses (B)	167,397	218,334	(50,937)	-23.33%	
Change in Assets (A - B)	28,870	(717)	29,587	-4126.61%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	(406)	(717)	311	-43.44%	
Total Inc(Dec) in Fixed Assets (C)	(406)	(717)	311	-43.44%	
TOTAL BUDGET (B + C)	**166,991**	**217,617**	**(50,626)**	**-23.26%**	
Change in Working Capital (A-B-C)	**29,276**	**-**	**29,276**		
FTE's	**0.10**	**0.10**	**-**	**0.00%**	

Northeast Power Coordinating Council, Inc.
2013 Statement of Activities Summary

SITUATION AWARENESS and INFRASTRUCTURE SECURITY	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	1,503,453	1,503,453	-	0.00%	
Penalty Sanctions	33,206	33,206		0.00%	
Total ERO Funding	1,536,659	1,536,659	-	0.00%	
Federal Grants	-	-	-		
Non-Statutory Assessments	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	1,536,659	1,536,659	-	0.00%	
Expenses					
Personnel Expenses					
Salaries	508,716	519,676	(10,960)	-2.11%	Salaries were under budget due to at risk compensation component based on corporate goal attainment and individual performance.
Payroll Taxes	33,867	33,338	529	1.59%	
Employee Benefits	60,012	82,596	(22,584)	-27.34%	Under budget due to several employees opting out of health insurance coverage for superior coverage through a prior employer.
Savings & Retirement	110,897	117,730	(6,833)	-5.80%	
Total Personnel Expenses	713,492	753,340	(39,848)	-5.29%	
Meeting Expenses					
Meetings	8,014	45,000	(36,986)	-82.19%	Under budget due to continued efforts to hold more meetings onsite, at member facilities or via webinars. Additionally, meetings that were previously allocated across all programs are now recorded to Admin and allocated through indirect expenses.
Travel	43,486	90,000	(46,514)	-51.68%	Continued efforts to hold more meetings onsite or via webinars have kept travel expenses under budget.
Conference Calls	-	-	-		
Total Meeting Expenses	51,500	135,000	(83,500)	-61.85%	
Operating Expenses					
Consultants & Contracts	113,038	100,000	13,038	13.04%	Over budget due to added programs and efforts related to system frequency response and generator governor response and the implementation of the NPCC program for the Simultaneous Activation of Reserve (SAR).
Rent & Improvements	-	-	-		
Office Costs	-	-	-		
Professional Services	-	-	-		
Miscellaneous	603	-	603		
Depreciation	-	-	-		
Total Operating Expenses	113,641	100,000	13,641	13.64%	
Indirect Expenses	610,749	569,819	40,930	7.18%	
Other Non-Operating Expenses	(304,468)	-	(304,468)		Decrease in NPCC's pension liability based on actuarial review at year end.
Total Expenses (B)	1,184,914	1,558,159	(373,245)	-23.95%	
Change in Assets (A - B)	351,745	(21,500)	373,245	-1736.02%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	(12,167)	(21,500)	9,333	-43.41%	
Total Inc(Dec) in Fixed Assets (C)	(12,167)	(21,500)	9,333	-43.41%	
TOTAL BUDGET (B + C)	**1,172,747**	**1,536,659**	**(363,912)**	**-23.68%**	
Change in Working Capital (A-B-C)	**363,912**	**-**	**363,912**		
FTE's	**3.00**	**3.00**	**-**	**0.00%**	

Northeast Power Coordinating Council, Inc.
2013 Statement of Activities Summary

ADMINISTRATIVE SERVICES	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	(1,115,163)	(1,115,163)	-	0.00%	
Penalty Sanctions	-	-			
Total ERO Funding	(1,115,163)	(1,115,163)	-	0.00%	
Federal Grants	-	-	-		
Non-Statutory Assessments	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	16,734	-	16,734		Interest income, while not budgeted, was allocated by FTE ratio between statutory and non-statutory.
Miscellaneous	-	-	-		
Total Funding (A)	(1,098,429)	(1,115,163)	16,734	-1.50%	
Expenses					
Personnel Expenses					
Salaries	1,637,376	1,604,850	32,526	2.03%	
Payroll Taxes	104,925	95,230	9,695	10.18%	
Employee Benefits	399,644	462,410	(62,766)	-13.57%	Under budget due to several employees opting out of health insurance coverage for superior coverage through a prior employer.
Savings & Retirement	441,197	406,249	34,948	8.60%	
Total Personnel Expenses	2,583,142	2,568,739	14,403	0.56%	
Meeting Expenses					
Meetings	123,584	60,000	63,584	105.97%	Company wide meetings that were previously allocated across all programs are now recorded to G&A and allocated across all programs through indirect expenses. Total Statutory meetings are under budget.
Travel	105,276	105,000	276	0.26%	
Conference Calls	71,988	87,000	(15,012)	-17.26%	Contracted with a more cost effective teleconference/webinar provider.
Total Meeting Expenses	300,848	252,000	48,848	19.38%	
Operating Expenses					
Consultants & Contracts	113,342	120,000	(6,658)	-5.55%	
Rent & Improvements	741,632	706,500	35,132	4.97%	
Office Costs	539,917	468,500	71,417	15.24%	Over budget primarily related to computer supplies and maintenance due to additional software programs including Diligent Board Books, to support Directors' hardware.
Professional Services	909,302	1,120,000	(210,698)	-18.81%	Legal fees were less than budget due to judicious use of outside counsel.
Miscellaneous	36,044	80,000	(43,956)	-54.95%	Under budget due to ongoing cost cutting efforts in all areas.
Depreciation	281,605	192,510	89,095	46.28%	Over budget due to additional assets placed in service in 2013. The assets are related to CDAA software development to enhance the efficiencies of compliance activities for both registered entities and Regional Entity staffs.
Total Operating Expenses	2,621,842	2,687,510	(65,668)	-2.44%	
Indirect Expenses	(5,704,951)	(5,508,249)	(196,702)	3.57%	
Other Non-Operating Expenses	(1,022,355)	-	(1,022,355)		Decrease in NPCC's pension liability based on actuarial review at year end.
Total Expenses (B)	(1,221,474)	-	(1,221,474)		
Change in Assets (A - B)	123,045	(1,115,163)	1,238,208	-111.03%	
Fixed Assets					
Depreciation	(281,605)	(192,510)	(89,095)	46.28%	Over budget due to additional assets placed in service in 2013. The assets are related to CDAA software development to enhance the efficiencies of compliance activities for both registered entities and Regional Entity staffs.
Computer & Software CapEx	167,230	-	167,230		Over budget due to capitalization of costs related to CMEP Data Administration Application (CDAA) software development not included in budget.
Furniture & Fixtures CapEx	1,388	-	1,388		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	(112,987)	(192,510)	79,523		
Allocation of Fixed Assets	112,987	192,510	(79,523)	-41.31%	
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B + C)	**(1,221,474)**	**-**	**(1,221,474)**		
Change in Working Capital (A-B-C)	**123,045**	**(1,115,163)**	**1,238,208**	-111.03%	
FTE's	**9.00**	**9.00**	**-**	**0.00%**	

Northeast Power Coordinating Council, Inc.

Financial Statements
December 31, 2013 and 2012

Northeast Power Coordinating Council, Inc.
Index
December 31, 2013 and 2012

Page(s)

Report of Independent Auditors 1

Financial Statements

Statements of Financial Position 2

Statements of Activities 3

Statements of Cash Flows 4

Notes to Financial Statements 5–12

Independent Auditor's Report

To the Board of Directors and the Members of
Northeast Power Coordinating Council, Inc.

We have audited the accompanying financial statements of Northeast Power Coordinating Council, Inc., which comprise the balance sheets as of December 31, 2013 and December 31, 2012, and the related change in net assets and cash flows for the years then ended.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of the financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on the financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on our judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, we consider internal control relevant to the Company's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Company's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of Northeast Power Coordinating Council, Inc. at December 31, 2013 and December 31, 2012, and the results of its operations and its cash flows for the years then ended in accordance with accounting principles generally accepted in the United States of America.

PricewaterhouseCoopers LLP
New York, New York
March 27, 2014

Northeast Power Coordinating Council, Inc.
Statements of Financial Position
December 31, 2013 and 2012

	2013	2012
Assets		
Cash	$ 7,412,184	$ 6,724,986
Restricted cash	611,021	649,950
Investments	2,210,944	2,210,894
Prepaid expenses	236,551	271,074
Other assets	137,191	335,714
Equipment and leasehold improvements, less accumulated depreciation and amortization of $1,100,649 and $800,389, respectively	1,142,418	1,274,059
Total assets	$ 11,750,309	$ 11,466,677
Liabilities and Net Assets		
Accrued expenses and other liabilities	$ 1,572,583	$ 1,287,040
Accrued liability for pension	1,135,117	3,676,153
Deferred revenue	734,117	235,313
Deferred rent	774,268	767,901
Total liabilities	4,216,085	5,966,407
Net assets		
Unrestricted net assets	7,534,224	5,500,270
Total net assets	7,534,224	5,500,270
Total liabilities and net assets	$ 11,750,309	$ 11,466,677

The accompanying notes are an integral part of these financial statements.

Northeast Power Coordinating Council, Inc.
Statements of Activities
Years Ended December 31, 2013 and 2012

	2013	2012
Revenue		
Assessments	$ 1,139,688	$ 956,900
Regional entity ERO funding	12,352,264	12,551,567
Penalty sanctions	212,000	203,300
Workshops	58,650	56,616
Interest income	17,281	22,255
Miscellaneous Income	109,867	314,507
Total revenue	13,889,750	14,105,145
Operating expenses		
Salaries and employee benefits	8,365,952	7,722,983
Administrative and consultant fees	2,398,006	1,944,962
Professional fees	572,229	527,170
Meetings and travel	1,131,260	963,372
Telephone and telecommunications	262,232	227,042
Office supplies and expense	316,019	257,696
Equipment leases	131,353	107,307
Rent expense	643,967	654,281
Insurance expense	39,019	34,768
Miscellaneous	43,092	118,107
Depreciation and amortization	300,260	236,647
Total operating expenses	14,203,389	12,794,335
Change in net assets before nonoperating expenses	(313,639)	1,310,810
Nonoperating expenses		
Pension change other than net periodic pension cost	(2,347,593)	1,080,685
Increase in net assets	2,033,954	230,125
Net assets		
Beginning of year	5,500,270	5,270,145
End of year	$ 7,534,224	$ 5,500,270

The accompanying notes are an integral part of these financial statements.

Northeast Power Coordinating Council, Inc.
Statements of Cash Flows
Years Ended December 31, 2013 and 2012

	2013	2012
Cash flows from operating activities		
Change in net assets	$ 2,033,954	$ 230,125
Depreciation and amortization	300,260	236,647
Decrease (increase) in prepaid expenses	34,523	(65,349)
Decrease (increase) in other assets	198,523	(267,638)
Increase in accrued expenses and other liabilities	285,543	90,135
(Decrease) increase in accrued liability for pension	(2,541,036)	1,019,403
Increase (decrease) in deferred revenue	498,804	(230,210)
Increase in deferred rent	6,367	6,424
Net cash provided by operating activities	816,938	1,019,537
Cash flows from investing activities		
Purchases of equipment and leasehold improvements	(168,619)	(246,623)
Purchases of investments	(50)	(30)
Restricted cash	38,929	687,845
Net cash (used for) provided by investing activities	(129,740)	441,192
Net increase in cash	687,198	1,460,729
Cash		
Beginning of year	6,724,986	5,264,257
End of year	$ 7,412,184	$ 6,724,986

The accompanying notes are an integral part of these financial statements.

1. Background

Northeast Power Coordinating Council, Inc. ("NPCC" or the "Company") is a New York State not-for-profit corporation whose purpose is to promote and enhance the reliable and efficient operation of the international, interconnected bulk power system in Northeastern North America through its regional entity and criteria services divisions. The Company's regional entity division is responsible for the development of regional reliability standards and compliance assessment and enforcement of continent-wide and regional reliability standards, coordination of system planning, design and operations, and assessment of reliability. These responsibilities are pursuant to an agreement with the North American Electric Reliability Corporation ("NERC"), an Electric Reliability Organization ("ERO"), under authority of the U.S. Federal Energy Regulatory Commission ("FERC"), and by Memoranda of Understanding with applicable Canadian Provincial regulatory and/or governmental authorities. The Company's criteria services division establishes regionally-specific criteria, and monitors and enforces compliance with such criteria. In the development of regionally-specific reliability criteria, the Company, to the extent possible, facilitates attainment of fair, effective and efficient competitive electric markets.

The Company is primarily funded through the NERC based on the regional entity division annual business plan and budget submitted to and approved by the FERC and Canadian provincial regulatory and/or governmental authorities. The Company's criteria services division is funded by regional independent system operators or balancing authorities acting as the Load Serving Entities' designees with regard to funding and the criteria services division operates on assessments to and funded from these entities based upon a "Net Energy for Load" formula.

2. Summary of Significant Accounting Policies

Basis of Accounting

For the years ended December 31, 2013 and 2012, the Company used the accrual basis of accounting in conformity with accounting principles generally accepted in the United States of America.

Cash

The Company's cash balance consists of its operating checking account, as well as a savings account. At times, cash balances may be in excess of depository insurance limits.

Restricted Cash

Restricted cash represents amounts in deposit accounts funded with penalties levied and received for noncompliance within NPCC U.S., which are required to be used for statutory activities in years subsequent to which the penalty was received, and amounts in deposit accounts for collateralizing a letter of credit as security for NPCC's office lease. At times, cash balances may be in excess of depository insurance limits.

Equipment and Leasehold Improvements

Equipment and leasehold improvements are stated at cost. Depreciation of furniture and computer equipment is computed on the straight-line basis over the estimated useful lives of the applicable assets. Amortization of leasehold improvements is computed on the straight-line basis over the estimated useful lives of the applicable assets, or over the term of the related lease, whichever is less.

Revenue Recognition
For the criteria services division, membership in the Company is on a calendar year basis. There are no fees assessed to full members other than those members that are Independent System Operators or Balancing Authorities. Assessments received are recorded as income in the year to which the membership applies irrespective of when billed or collected. For the regional entity division, membership in the Company is on a calendar year basis. There are no fees assessed to general members. Funding mechanisms provided through U.S. regulatory and Canadian Provincial governmental and/or regulatory agreements provide for quarterly remittances through the North American Electric Reliability Corporation. Assessments received are recorded as income in the year to which the Business Plan and Budget applies irrespective of when billed or collected. Penalty sanctions are recorded as income when levied and the appeals process has been waived or is concluded.

Rent Expense
The Company's office lease which commenced in 2009 contains predetermined increases and decreases in the rentals payable during the lease term. Rent expense is recognized on a straight-line basis over the lease term. The difference between the rent expense charged to operations during the year and the amount payable under the lease during that year is recorded as "Deferred rent" on the Statements of Financial Position. Deferred rent also includes the landlord's contribution toward the cost of leasehold improvements, which is being amortized over the lease term. The unamortized balance of the landlord's contribution at December 31, 2013 is approximately $372,000.

Income Taxes
The Company has been classified as exempt from federal income taxes under Section 501(c) (6) of the Internal Revenue Code.

Use of Estimates
The Company uses estimates and assumptions in preparing these financial statements in accordance with accounting principles generally accepted in the United States of America. Those estimates and assumptions affect the reported amounts of assets, liabilities, revenues and expenses. Actual results could vary from the estimates that are used.

3. Investments

The Company's primary banking relationship is with JP Morgan Chase. Prior to 2009, both regional entity (ERO funded) and criteria services (Regional Independent System Operators/Balancing Authorities – ISO/BAs) revenues were invested in a JPMorgan 100% U.S. Treasury Security Money Market Fund (the "Fund"). The Fund aims to provide the highest possible level of current income while still maintaining liquidity and providing maximum safety of principal. The Fund is a money market fund managed to meet the requirements of Rule 2a-7 under the Investment Company Act of 1940. The Fund is not insured or guaranteed by the FDIC or any other government agency. In late 2008, the Fund was closed to additional investments. Subsequent excess cash is being deposited into a savings account with JP Morgan Chase.

The Fund invests solely in debt securities of the U.S. Treasury, including Treasury bills, bonds and notes. These investments carry different interest rates, maturities and issue dates. The National Association of Insurance Commissioner ("NAIC"), Moody's, Fitch IBCA and S&P ratings signify that the Fund has historically had a superior capacity to maintain a net asset value of $1.00 per share. The ratings do not eliminate the risks associated with investing in the Fund. The NAIC "approved" status indicates that the Fund meets certain pricing and quality guidelines. Management has determined that the likelihood of sustaining losses from money market funds to be remote based on the marketability of the underlying investment of the funds.

At December 31, 2013 and 2012, the Company owned 2,210,944 and 2,210,894 units of $1 par value per unit, respectively. In 2013 and 2012, the funds earned average yields of less than 1%. Investment income earned on the Fund is reinvested into units of the Fund on a monthly basis.

4. Equipment and Leasehold Improvements

Equipment and leasehold improvements at December 31, 2013 and 2012 consists of the following:

	Depreciable Life	2013	2012
Furniture	10 years	$ 202,906	$ 201,518
Computer equipment	3 years	435,769	435,769
Website	3 years	232,000	232,000
Software	3 years	397,701	230,470
Leasehold improvements	15 years (See note 2)	974,691	974,691
		2,243,067	2,074,448
Less: Accumulated depreciation and amortization		(1,100,649)	(800,389)
		$ 1,142,418	$ 1,274,059

In 2013 and 2012, depreciation and amortization expense totaled $300,260 and $236,647, respectively.

5. Pension Plan

The Company has a trusteed, noncontributory defined benefit pension plan (the "Plan") covering employees hired prior to February 6, 2007. The Company's plan contributions were $700,000 and $600,000 for the years 2013 and 2012, respectively.

The following tables provide information with respect to the defined benefit plan as of and for the years ended December 31, 2013 and 2012:

	2013	2012
Components of net periodic benefit cost		
Service cost	$ 298,867	$ 276,757
Interest cost	477,051	461,524
Expected return on plan assets	(599,893)	(492,785)
Amortization of prior service cost	20,532	20,532
Recognized actuarial loss	310,000	272,690
Net periodic benefit cost	$ 506,557	$ 538,718
Change in benefit obligation		
Benefit obligation at beginning of year	$ 11,279,973	$ 8,957,466
Service cost	298,867	276,757
Interest cost	477,051	461,524
Actuarial (gain) loss	(1,660,662)	1,686,218
Benefits paid	(101,992)	(101,992)
Benefit obligation at end of year	10,293,237	11,279,973
Change in fair value of plan assets		
Fair value of plan assets at beginning of year	7,603,820	6,300,716
Actual return on plan assets	956,292	805,096
Company contribution	700,000	600,000
Benefits paid	(101,992)	(101,992)
Fair value of plan assets at end of year	9,158,120	7,603,820
Funded status at end of year	$ (1,135,117)	$ (3,676,153)
Amounts recognized in unrestricted net assets consist of		
Loss	$ (1,745,933)	$ (4,072,994)
Prior service cost	(160,151)	(180,683)
	$ (1,906,084)	$ (4,253,677)
Changes in unrestricted assets recognized in nonoperating expenses		
Net (gain) loss	$ (2,017,061)	$ 1,373,907
Amortization of prior service cost	(20,532)	(20,532)
Amortization of net gain (loss)	(310,000)	(272,690)
	$ (2,347,593)	$ 1,080,685
Amounts of unrestricted net assets expected to be recognized in net periodic benefit cost in 2014		
Amortization of loss	$ 200,000	

Weighted-average assumptions as of December 31 used for obligation		
Discount rate	5.00 %	4.25 %
Expected return on plan assets	7.50 %	7.50 %
Rate of compensation increase	3.00 %	3.00 %
Weighted-average assumptions as of December 31 used for net periodic benefit cost		
Discount rate	5.00 %	4.25 %
Expected return on plan assets	7.50 %	7.50 %
Rate of compensation increase	3.00 %	3.00 %

The accumulated benefit obligation at December 31, 2013 and 2012 was $9,371,706 and $8,487,636, respectively.

The Company determines its expected return on plan assets assumption by evaluating both historical returns of major asset classes and current market factors. Current market factors include inflation and interest rates, as well as asset diversification.

The Company's defined benefit plan weighted average asset allocation at December 31, 2013 and 2012 by asset category is as follows:

	Allocation Percentage	
	2013	**2012**
Equity securities	70.6%	71.1%
Debt securities	28.0%	28.2%
Cash	1.4%	0.7%
	100.0%	100.0%

The Company's defined benefit plan invests primarily in equity and debt securities that are based upon levels of risk and provide for necessary liquidity requirements. The long-term objective is to limit the variability of its pension funding. The Company's plan assets are measured against benchmarks established by the Pension Committee, which has the authority to recommend changes as deemed appropriate.

Investments in actively traded equity and debt securities are valued using market prices in active markets. Their valuations are obtained from real-time quotes for transactions in active exchange markets involving identical assets. There were no securities for which the fair value was based on other observable or unobservable inputs. At December 31, 2013, the plan assets consisted of $127,177 of cash and cash equivalents, $3,310,439 of domestic equities, $1,346,311 of international equities, $2,563,932 of corporate bonds, $1,126,052 of specific strategy funds, $263,378 of commodity funds and $420,831 of public real estate investment trust investments.

At December 31, 2013, the Company's target allocation percentages for plan assets were approximately 46% equity securities, 29% debt securities and 25% other securities. The targets may be adjusted periodically to reflect current market conditions and trends as well as inflation levels, interest rates and trends thereof.

Expected employer contribution for the year ended December 31, 2014 is $650,000.

Benefits expected to be paid in cash in subsequent years ending December 31 are as follows:

2014	$ 110,150
2015	386,154
2016	377,739
2017	369,074
2018	360,326
2019–2023	3,274,211

6. Savings and Supplemental Plans

The Company maintains a 401(k) plan for which all employees are immediately eligible upon hire. Within this plan, an employee can contribute 2% or greater of his or her compensation up to the IRS limit set for this plan. The Company's policy is to contribute on the employee's behalf 100% of the employee's contribution of the first 3% of his or her compensation, and 50% of his or her contribution for the next 2% of compensation. Additionally, for those employees joining the Company after February 6, 2007, and upon completion of a full calendar year of service, such employees become eligible for a discretionary contribution to be considered annually by the Board of Directors. The discretionary contribution for 2013 and 2012 was 8% of base compensation and totaled $189,215 for 2013 and $189,956 for 2012. Company contributions to the 401(k) plan were $185,546 and $174,392 for 2013 and 2012, respectively. During 2010, the Company adopted a supplemental plan for employees who were not eligible to receive the same percentage level of retirement benefits as other employees under the 401(k) plan due to IRS compensation limits. The Company contributed $26,500 and $23,000 to this supplemental plan for 2013 and 2012, respectively. During 2013, the Company adopted a 457(f) plan for the President and CEO to provide benefits not provided under the Pension Plan as a result of the IRS code limitations. The Company contributed $30,000 to this plan in 2013.

7. Leases

The Company is obligated under long-term operating leases for the rental of office facilities and certain equipment. NPCC executed office and equipment leases with effective rental dates starting in 2009 coordinated with its relocation of offices within New York City. NPCC's office lease provides for additional rent based on increases in real estate taxes and operating expenses over base amounts. The office lease expires on April 30, 2024 and includes an option to renew for five years. The office lease provides for security in the form of a collateralized letter of credit in the amount of $500,000 at lease inception and reduced to $300,000 at December 31, 2012, and reduced amounts in future years. NPCC executed various computer and equipment leases with expiration dates through March, 2016. In addition, the Company rents certain other equipment on a month-to-month basis. Rental expense for office facilities and equipment totaled $775,320 and $761,588 for 2013 and 2012, respectively.

Future minimum rental payments required under the Company's long-term operating leases as of December 31, 2013 are as follows:

	Office Space	Other Leases	Total
Year Ending December 31			
2014	$ 652,380	$ 129,064	$ 781,444
2015	672,392	88,637	761,029
2016	672,392	20,142	692,534
2017	672,392		672,392
2018	672,392		672,392
Thereafter	3,826,091		3,826,091
	$ 7,168,039	$ 237,843	$ 7,405,882

8. Functional Expenses

During 2013 and 2012 salaries and employee benefits consist of the following:

	2013	2012
President, COO and technical staff	$ 5,510,411	$ 5,128,701
Administrative support	175,493	169,254
Payroll taxes, insurance, pension and educational assistance	2,680,048	2,425,028
Total salaries and employee benefits	$ 8,365,952	$ 7,722,983

9. Other Expenses

The Company incurs various costs for administrative, consultant and professional services. Such costs amounted to $2,970,235 and $2,472,132 in 2013 and 2012, respectively, and consist of the following:

	2013	2012
Consultants	$ 1,734,733	$ 1,485,916
Accounting, legal and other services	1,197,113	964,903
Pension administration	38,389	21,313
Total administrative, consultant and professional fees	$ 2,970,235	$ 2,472,132

These costs are reflected in "Administrative and consultant fees" and "Professional fees" in the Statements of Activities.

10. Related Party Transactions

The NERC, through agreements with the FERC in the U.S. and Canadian Provincial regulatory and/or governmental agreements within Canada, delegates enforcement authority to eight Regional Entities. NPCC is the cross-border Regional Entity for Northeastern North America. NERC was certified as the "Electric Reliability Organization" by the FERC on July 20, 2006. As of June 18, 2007, the U.S. FERC granted NERC the legal authority to enforce reliability standards with all U.S. users, owners, and operators of the bulk power system, and made compliance with those standards mandatory and enforceable. NERC relies on the diverse and collective expertise of industry participants to improve the reliability of the bulk power system. These entities account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico. NERC is subject to audit by the U.S. FERC and governmental and/or regulatory authorities in Canada. NERC funded the Regional Entities based upon Business Plans and Budgets submitted to and approved by FERC in the U.S. and Canadian Provincial regulatory and/or governmental authorities.

NPCC's criteria services division was fully funded by regional independent system operator or balancing authorities acting as the Load Serving Entities' designees and operated on assessments to and funded from these six entities. Dues were based upon a "Net Energy for Load" funding formula. During 2013 and 2012, total assessments billed amounted to $1,139,688 and $956,900, respectively.

	2013		2012	
Description	**Percent**	**Total Share**	**Percent**	**Total Share**
Hydro-Quebec TransEnergie	28.56 %	$ 325,481	28.27 %	$ 270,543
Independent Electricity System Operator	21.94 %	250,013	22.11 %	211,520
ISO-New England, Inc.	20.65 %	235,313	20.52 %	196,362
New Brunswick System Operator	2.12 %	24,185	2.12 %	20,242
New York Independent System Operator	24.91 %	283,927	25.08 %	240,034
Nova Scotia Power Inc.	1.82 %	20,769	1.90 %	18,199
Total assessments	100.00 %	$ 1,139,688	100.00 %	$ 956,900

11. Line of Credit

On March 18, 2013, pursuant to an agreement with a lender, the Company obtained a line of credit in the amount of $1,000,000. There were no borrowings against the line of credit as of December 31, 2013.

12. Subsequent Events

Management has evaluated, for potential recognition and disclosure, events subsequent to the date of the Statement of Financial Position through March 27, 2014, the date the financial statements were available to be issued.

ATTACHMENT 5

2013 ACTUAL COST-TO-BUDGET COMPARISON

AND

2013 AUDITED FINANCIAL REPORT

FOR

RELIABILITYFIRST CORPORATION

RELIABILITY FIRST
3 Summit Park Drive, Suite 600
Cleveland, OH 44131

May 5, 2014

Mr. Michael Walker
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, Georgia 30326

Subject: **ReliabilityFirst's 2013 True-up Filing**

Mr. Michael Walker:

As requested, ReliabilityFirst Corporation (ReliabilityFirst) is providing NERC the end of year audited 2013 True-up Filing. Significant variances are explained below, while more detailed variances are provided in the attached Statement of Activities, Fixed Assets and Change in Working Capital document presented by program area.

The explanations of variances are provided based on the following criteria:

1. Variances equal to or greater than +/- 10% of budget, and
2. Variances greater than $10,000, or
3. Variances that are considered significant.

Summary

For the year ending December 31, 2013, Reliability*F*irst was $119K (.68%) over budget. This year end variance included $551K of Leasehold Improvement capital expenditures that related to the 2014 office and data center relocation, which were not included in the 2013 budget. If these capital expenditures were not recorded in 2013, the year-end variance would have been $432K (2.48%) under budget. In addition to completing all statutory objectives, ReliabilityFirst completed these major accomplishments:

- Developed the audit section of the MKInsight Audit Management Software to organize, manage, and improve efficiency of our monitoring processes.
- ReliabilityFirst Staff presented entity training on our Risk-Harm determination tool during the Spring Reliability Workshop. The series included detail on how risk and harm is quantified, the concepts of estimating the likelihood and magnitude of harm occurring, and how to mitigate the risk to reduce the likelihood of the harm occurring.
- Delivered one full day of training to more than 200 representatives from Registered Entities on Reliability Assurance Initiative (RAI) which included the identification of key critical process areas that contribute to reliability and how a systems thinking approach can lead to building a robust set of management practices that can reduce the risk to reliability.
- Supported RAI by conducting a pilot appraisal of key management practice areas with a registered entity.
- To improve ReliabilityFirst's resource assessments, reviewed demand forecast method(s) and data, the weather normalization calculations, and the NERC demand bandwidth analysis used in our footprint. After reviewing this information, researched a method of including load forecast uncertainty (i.e., bandwidth) in future resource assessments.

- Reviewed the September 8, 2011 *Arizona-Southern California Outage* report findings and recommendations and performed a gap analysis to determine what could be missing in existing standards, guidelines, processes, or audit procedures and assessment studies. A report was produced that included suggestions for improvement.
- Examined existing methods to determine reliability of systems and proposed a definition and a method to measure grid reliability for the bulk power system. Existing methods and data considered included misoperations analysis, TADs, GADs, CIP Influence, outages/100 miles/year, etc. A sample report was produced on an entity basis to show the effect of that entity's performance on the overall ReliabilityFirst footprint.
- Quantitatively assessed the effectiveness of two Reliability Standards in achieving the desired reliability outcome including whether, if appropriate to the standard, less than zero-tolerance compliance would achieve essentially the same reliability result as full compliance. The two Standards assessed were PRC-005 and VAR-002. Reports were produced that discussed the benefits and any detriments of the standards and any recommendations for any changes to the standard or other proposals for improvement.
- Provided guidance and education to registered entities to meet compliance obligations through a better understanding of the NERC Reliability Standards by conducting 12 assist visits. Entity issues ranging from compliance concerns associated with their reading of the FERC approved standards, to preparing for new standards, and providing additional guidance and education.
- ReliabilityFirst conducted several successful outreach efforts, including two workshops that were attended by 200 plus registered entities and a Monthly Open Compliance Call that was attended by, on average, 75 registered entities.

Funding

- **Investment Income:** $127K (211%) under budget
  The variance in Investment Income is due to the unrealized change in value of the company's investment portfolio offset by the dividends that were received.

Expenses

- **Personnel Expenses**
  - **Salaries, Payroll Taxes, Employee Benefits and Savings & Retirement Costs:** $651K (5%) under budget
    These personnel expenses were under budget due to the difficulties in hiring qualified personnel.
- **Operating Expenses**
  - **Rent & Utilities:** $98K (21%) over budget
    Rent was over budget due to the early termination penalty for the prior office lease, offset by the board decision not to pursue an offsite disaster recovery site in 2013.
  - **Office Costs:** $213K (31%) over budget
    Office Costs were over budget as a result of variances in Telephone and Internet. Telephone expenses were over budget due to the large capacity phone line that was procured in preparation to support an in house conferencing system. Internet expenses were over budget due to the continued use of the contracted high bandwidth data line.

Fixed Assets

- **Computer Hardware & Software:** $37K (47%) under budget
  Computer Hardware & Software was under budget due to planned hardware purchases being delayed or reassessed in consideration of the planned 2014 office move.
- **Furniture & Fixtures:** $8K over budget
  The variance in Furniture & Fixtures was a result of the purchases of office furniture to accommodate new hires and appliances for the new office.

- **Leasehold Improvements:** $551K over budget
  The variance in Leasehold Improvements was a result of the planned 2014 office and data center relocation. All of these expenditures have been reimbursed from our Tenant Improvement Allowance in 2014.

Cash Reserves

ReliabilityFirst's Operating Reserve of $1,000,000 was never utilized.

Statutory Programs

ReliabilityFirst performed only statutory activities in 2013.

Cost Allocation

ReliabilityFirst records all direct costs to the appropriate program areas. Costs related to the Administrative Services programs are allocated proportionately based on FTE count to the direct programs.

- Direct Programs include:
  - Standards
  - Compliance
  - Reliability Assessment
  - Training & Education
  - Situation Awareness
- Administrative Services Programs include:
  - General & Administrative
  - Legal & Regulatory Affairs
  - Information Technology
  - Human Resources
  - Finance & Accounting

For more information, please contact me at 216.503.0600 or jill.lewton@rfirst.org.

Sincerely,

Jill S. Lewton

Jill S. Lewton
Controller

RELIABILITY FIRST

Statement of Activities, Fixed Assets and Change in Working Capital
Summary
01/01/2013 - 12/31/2013

	2013 Actual	2013 Budget	2013 Variance	
Funding				
ERO Funding				
ERO Assessments	$ 14,165,848	$ 14,165,848	$ -	0.00%
Penalty Sanctions	2,979,800	2,979,800	-	0.00%
Total ERO Funding	$ 17,145,648	$ 17,145,648	$ -	0.00%
Other Funding				
Membership Fees	$ -	$ -	$ -	
Investment Income	(66,853)	60,000	(126,853)	-211.42%
Miscellaneous	-	-	-	
Total Other Funding	$ (66,853)	$ 60,000	$ (126,853)	-211.42%
Total Funding	**$ 17,078,795**	**$ 17,205,648**	**$ (126,853)**	-0.74%
Expenses				
Direct Expenses				
Personnel Expenses				
Salaries	$ 10,007,431	$ 10,610,389	$ (602,958)	-5.68%
Payroll Taxes	611,830	624,720	(12,890)	-2.06%
Employee Benefits	1,306,001	1,318,673	(12,672)	-0.96%
Savings & Retirement	1,491,994	1,514,025	(22,031)	-1.46%
Total Personnel Expenses	$ 13,417,256	$ 14,067,807	$ (650,551)	-4.62%
Meeting Expenses				
Meetings	$ 173,392	$ 157,810	$ 15,582	9.87%
Travel	765,885	773,300	(7,415)	-0.96%
Conference Calls	38,097	43,092	(4,995)	-11.59%
Total Meeting Expenses	$ 977,374	$ 974,202	$ 3,172	0.33%
Operating Expenses				
Consultants & Contracts	$ 609,487	$ 650,140	$ (40,653)	-6.25%
Office Rent	560,012	461,645	98,367	21.31%
Office Costs	899,538	686,864	212,674	30.96%
Professional Services	451,665	483,160	(31,495)	-6.52%
Miscellaneous	30,702	25,021	5,681	22.70%
(Gain)/Loss on Disposal of Assets	(255)	-	(255)	
Depreciation	428,935	433,772	(4,837)	-1.12%
Total Operating Expenses	$ 2,980,084	$ 2,740,602	$ 239,482	8.74%
Total Direct Expenses	**$ 17,374,714**	**$ 17,782,611**	**$ (407,897)**	-2.29%
Indirect Expenses	$ -	$ -	$ (0)	
Other Non-Operating Expenses	$ -	$ -	$ -	
Total Expenses	**$ 17,374,714**	**$ 17,782,611**	**$ (407,897)**	-2.29%
Net Change in Assets	**$ (295,919)**	**$ (576,963)**	**$ 281,044**	-48.71%
Fixed Assets				
Depreciation	$ (428,935)	$ (433,772)	$ 4,837	-1.12%
Computer & Software CapEx	40,989	78,000	(37,011)	-47.45%
Furniture & Fixtures CapEx	8,082	-	8,082	
Equipment CapEx	-	-	-	
Leasehold Improvements	550,734	-	550,734	
Increase/(Decrease) Fixed Assets	**$ 170,870**	**$ (355,772)**	**$ 526,642**	-148.03%
Allocation of Fixed Assets	$ -	$ -	$ -	
Increase/(Decrease) Total Fixed Assets	**$ 170,870**	**$ (355,772)**	**$ 526,642**	-148.03%
Total Budget	**$ 17,545,584**	**$ 17,426,839**	**$ 118,745**	0.68%
Change in Working Capital	**$ (466,789)**	**$ (221,191)**	**$ (245,598)**	111.03%
FTEs	**69.80**	**73.00**	**-3.20**	
- All amounts are based on audited financials				
- All amounts are in whole dollars				
- All functions are Statutory				

RELIABILITY FIRST

Statement of Activities, Fixed Assets and Change in Working Capital
Standards
01/01/2013 - 12/31/2013

	2013 Actual	2013 Budget	2013 Variance	%	Explanation of Variances
Funding					
ERO Funding					
ERO Assessments	$ 148,183	$ 148,183	$ -	0%	
Penalty Sanctions	26,047	26,047	-	0%	
Total ERO Funding	$ 174,230	$ 174,230	$ -	0%	
Other Funding					
Membership Fees	$ -	$ -	$ -		
Investment Income	(1,284)	524	(1,808)	-345%	The variance in Investment Income was due to the unrealized change in value of the company's investment portfolio offset by the dividends that were received.
Miscellaneous	-	-	-		
Total Other Funding	$ (1,284)	$ 524	$ (1,808)	-345%	
Total Funding	**$ 172,946**	**$ 174,754**	**$ (1,808)**		
Expenses					
Direct Expenses					
Personnel Expenses					
Salaries	$ 85,293	$ 87,336	$ (2,043)	-2%	
Payroll Taxes	7,190	4,744	2,446	52%	
Employee Benefits	10,677	10,970	(293)	-3%	
Savings & Retirement	16,969	13,974	2,995	21%	
Total Personnel Expenses	$ 120,129	$ 117,024	$ 3,105	3%	
Meeting Expenses					
Meetings	$ -	$ -	$ -		
Travel	11,216	11,500	(284)	-2%	
Conference Calls	-	-	-		
Total Meeting Expenses	$ 11,216	$ 11,500	$ (284)	-2%	
Operating Expenses					
Consultants & Contracts	$ -	$ -	$ -		
Office Rent	-	-	-		
Office Costs	2,037	2,668	(631)	-24%	
Professional Services	-	-	-		
Miscellaneous	121	-	121		
(Gain)/Loss on Disposal of Assets	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	$ 2,158	$ 2,668	$ (510)	-19%	
Total Direct Expenses	**$ 133,503**	**$ 131,192**	**$ 2,311**	2%	
Indirect Expenses	$ 108,605	$ 44,949	$ 63,656	142%	Indirect Expenses are expenses related to the Administrative Services programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher administrative expenditures being allocated.
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	**$ 242,108**	**$ 176,141**	**$ 65,967**	37%	
Net Change in Assets	**$ (69,162)**	**$ (1,387)**	**$ (67,775)**	4886%	
Fixed Assets					
Depreciation	$ -	$ -	$ -		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Increase/(Decrease) Fixed Assets	**$ -**	**$ -**	**$ -**		
Allocation of Fixed Assets	$ 7,620	$ (1,387)	$ 9,007	-649%	Allocation of Fixed Assets are fixed asset costs related to the Administrative Services programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher fixed asset expenditures being allocated.
Increase/(Decrease) Total Fixed Assets	**$ 7,620**	**$ (1,387)**	**$ 9,007**	-649%	
Total Budget	**$ 249,728**	**$ 174,754**	**$ 74,974**	43%	
Change in Working Capital	**$ (76,782)**	**$ -**	**$ (76,782)**		
FTEs	**0.50**	**0.50**	**0.00**	0%	

RELIABILITY FIRST

Statement of Activities, Fixed Assets and Change in Working Capital
Compliance
01/01/2013 - 12/31/2013

	2013 Actual	2013 Budget	2013 Variance	%	Explanation of Variances
Funding					
ERO Funding					
ERO Assessments	$ 10,736,863	$ 10,736,863	$ -	0%	
Penalty Sanctions	2,240,059	2,240,059	-	0%	
Total ERO Funding	$ 12,976,922	$ 12,976,922	$ -	0%	
Other Funding					
Membership Fees	$ -	$ -	$ -		
Investment Income	(49,800)	45,105	(94,905)	-210%	The variance in Investment Income was due to the unrealized change in value of the company's investment portfolio offset by the dividends that were received.
Miscellaneous	-	-	-		
Total Other Funding	$ (49,800)	$ 45,105	$ (94,905)	-210%	
Total Funding	**$ 12,927,122**	**$ 13,022,027**	**$ (94,905)**		
Expenses					
Direct Expenses					
Personnel Expenses					
Salaries	$ 5,456,087	$ 5,870,101	$ (414,014)	-7%	
Payroll Taxes	355,198	370,369	(15,171)	-4%	
Employee Benefits	751,015	838,359	(87,344)	-10%	
Savings & Retirement	801,891	867,559	(65,668)	-8%	
Total Personnel Expenses	$ 7,364,191	$ 7,946,388	$ (582,197)	-7%	Personnel expenses were under budget due to the difficulties in hiring qualified personne
Meeting Expenses					
Meetings	$ 12,964	$ 8,210	$ 4,754	58%	
Travel	490,598	508,000	(17,402)	-3%	
Conference Calls	0	0	-		
Total Meeting Expenses	$ 503,562	$ 516,210	$ (12,648)	-2%	
Operating Expenses					
Consultants & Contracts	$ 409,642	$ 475,000	$ (65,358)	-14%	Contracts & Consultants expense was under budget as a result of the process improvements and efficiency gains that were achieved during the year.
Office Rent	-	-	-		
Office Costs	273,567	311,989	(38,422)	-12%	Office costs were under budget primarily due to a variance in Telephone. Telephone expense was under budget due to the number of employees receiving wireless devices (i.e. cell phone and air cards) being less than budgeted.
Professional Services	15,000	15,000	-	0%	
Miscellaneous	1,260	1,405	(145)	-10%	
(Gain)/Loss on Disposal of Assets	-	-	-		
Depreciation	225,518	206,421	19,097	9%	Depreciation expense directly correlates to current and prior year fixed asset activities. As a result of the prior year fixed asset purchases being over budget, there was more depreciation expense recorded this year.
Total Operating Expenses	$ 924,987	$ 1,009,815	$ (84,828)	-8%	
Total Direct Expenses	**$ 8,792,740**	**$ 9,472,413**	**$ (679,673)**	-7%	
Indirect Expenses	$ 4,212,979	$ 3,865,608	$ 347,371	9%	Indirect Expenses are expenses related to the Administrative Services programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher administrative expenditures being allocated.
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	**$ 13,005,719**	**$ 13,338,021**	**$ (332,302)**	-2%	
Net Change in Assets	**$ (78,597)**	**$ (315,994)**	**$ 237,397**	-75%	
Fixed Assets					
Depreciation	$ (225,518)	$ (206,421)	$ (19,097)	9%	Depreciation expense directly correlates to current and prior year fixed asset activities. As a result of the prior year fixed asset purchases being over budget, there was more depreciation expense recorded this year.
Computer & Software CapEx	-	9,600	(9,600)	-100%	Computer & Software CapEx was under budget due to the need for further evaluation regarding the analytical software needs for the Reliability Assurance Initiatives.
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Increase/(Decrease) Fixed Assets	**$ (225,518)**	**$ (196,821)**	**$ (28,697)**	15%	
Allocation of Fixed Assets	$ 295,594	$ 183,045	$ 112,549	61%	Allocation of Fixed Assets are fixed asset costs related to the Administrative Services programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher fixed asset expenditures being allocated.
Increase/(Decrease) Total Fixed Assets	**$ 70,076**	**$ (13,776)**	**$ 83,852**	-609%	
Total Budget	**$ 13,075,795**	**$ 13,324,245**	**$ (248,450)**	-2%	
Change in Working Capital	**$ (148,673)**	**$ (302,218)**	**$ 153,545**	-51%	
FTEs	**40.42**	**43.00**	**-2.58**	-6%	The 2013 actual FTE count includes 1.63 FTEs for the graduate prograr

RELIABILITY FIRST

Statement of Activities, Fixed Assets and Change in Working Capital
Reliability Assessment
01/01/2013 - 12/31/2013

	2013 Actual	2013 Budget	2013 Variance	%	Explanation of Variances
Funding					
ERO Funding					
ERO Assessments	$ 2,538,757	$ 2,538,757	$ -	0%	
Penalty Sanctions	520,944	520,944	-	0%	
Total ERO Funding	$ 3,059,701	$ 3,059,701	$ -	0%	
Other Funding					
Membership Fees	$ -	$ -	$ -		
Investment Income	(11,019)	10,490	(21,509)	-205%	The variance in Investment Income was due to the unrealized change in value of the company's investment portfolio offset by the dividends that were received.
Miscellaneous	-	-	-		
Total Other Funding	$ (11,019)	$ 10,490	$ (21,509)	-205%	
Total Funding	**$ 3,048,682**	**$ 3,070,191**	**$ (21,509)**		
Expenses					
Direct Expenses					
Personnel Expenses					
Salaries	$ 1,308,756	$ 1,479,629	$ (170,873)	-12%	
Payroll Taxes	79,803	86,964	(7,161)	-8%	
Employee Benefits	119,349	154,494	(35,145)	-23%	
Savings & Retirement	201,906	218,462	(16,556)	-8%	
Total Personnel Expenses	$ 1,709,814	$ 1,939,549	$ (229,735)	-12%	Personnel expenses were under budget due to the difficulties in hiring qualified personnel.
Meeting Expenses					
Meetings	$ 19,252	$ 15,000	$ 4,252	28%	
Travel	94,243	106,500	(12,257)	-12%	Travel expenses were under budget due to attending less meetings than originally budgeted.
Conference Calls	-	-	-		
Total Meeting Expenses	$ 113,495	$ 121,500	$ (8,005)	-7%	
Operating Expenses					
Consultants & Contracts	$ 79,557	$ 77,140	$ 2,417	3%	
Office Rent	-	-	-		
Office Costs	51,227	60,687	(9,460)	-16%	
Professional Services	-	-	-		
Miscellaneous	59	50	9	18%	
(Gain)/Loss on Disposal of Assets	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	$ 130,843	$ 137,877	$ (7,034)	-5%	
Total Direct Expenses	**$ 1,954,152**	**$ 2,198,926**	**$ (244,774)**	-11%	
Indirect Expenses	$ 932,195	$ 898,979	$ 33,216	4%	Indirect Expenses are expenses related to the Administrative Services programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher administrative expenditures being allocated.
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	**$ 2,886,347**	**$ 3,097,905**	**$ (211,558)**	-7%	
Net Change in Assets	**$ 162,335**	**$ (27,714)**	**$ 190,049**	-686%	
Fixed Assets					
Depreciation	$ -	$ -	$ -		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Increase/(Decrease) Fixed Assets	**$ -**	**$ -**	**$ -**		
Allocation of Fixed Assets	$ 65,405	$ (27,714)	$ 93,119	-336%	Allocation of Fixed Assets are fixed asset costs related to the Administrative Services programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher fixed asset expenditures being allocated.
Increase/(Decrease) Total Fixed Assets	**$ 65,405**	**$ (27,714)**	**$ 93,119**	-336%	
Total Budget	**$ 2,951,752**	**$ 3,070,191**	**$ (118,439)**	-4%	
Change in Working Capital	**$ 96,929**	**$ -**	**$ 96,929**		
FTEs	**9.08**	**10.00**	**-0.92**	-9%	

RELIABILITY FIRST

Statement of Activities, Fixed Assets and Change in Working Capital
Training & Education
01/01/2013 - 12/31/2013

	2013 Actual	2013 Budget	2013 Variance	%	Explanation of Variances
Funding					
ERO Funding					
ERO Assessments	$ 754,962	$ 754,962	$ -	0%	
Penalty Sanctions	161,493	161,493	-	0%	
Total ERO Funding	$ 916,455	$ 916,455	$ -	0%	
Other Funding					
Membership Fees	$ -	$ -	$ -		
Investment Income	(3,980)	3,252	(7,232)	-222%	The variance in Investment Income was due to the unrealized change in value of the company's investment portfolio offset by the dividends that were received.
Miscellaneous	-	-	-		
Total Other Funding	$ (3,980)	$ 3,252	$ (7,232)	-222%	
Total Funding	**$ 912,475**	**$ 919,707**	**$ (7,232)**		
Expenses					
Direct Expenses					
Personnel Expenses					
Salaries	$ 419,851	$ 411,250	$ 8,601	2%	
Payroll Taxes	28,288	27,473	815	3%	
Employee Benefits	54,888	51,900	2,988	6%	
Savings & Retirement	63,056	64,991	(1,935)	-3%	
Total Personnel Expenses	$ 566,083	$ 555,614	$ 10,469	2%	
Meeting Expenses					
Meetings	$ 74,751	$ 90,000	$ (15,249)	-17%	Meetings were under budget due to the decision to host two less workshops than originally budgeted.
Travel	5,367	4,000	1,367	34%	
Conference Calls	-	-	-		
Total Meeting Expenses	$ 80,118	$ 94,000	$ (13,882)	-15%	
Operating Expenses					
Consultants & Contracts	$ -	$ -	$ -		
Office Rent	-	-	-		
Office Costs	-	-	-		
Professional Services	-	-	-		
Miscellaneous	-	-	-		
(Gain)/Loss on Disposal of Assets	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	$ -	$ -	$ -		
Total Direct Expenses	**$ 646,201**	**$ 649,614**	**$ (3,413)**	-1%	
Indirect Expenses	$ 336,676	$ 278,683	$ 57,993	21%	Indirect Expenses are expenses related to the Administrative Services programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher administrative expenditures being allocated.
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	**$ 982,877**	**$ 928,297**	**$ 54,580**	6%	
Net Change in Assets	**$ (70,402)**	**$ (8,590)**	**$ (61,812)**	720%	
Fixed Assets					
Depreciation	$ -	$ -	$ -		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Increase/(Decrease) Fixed Assets	**$ -**	**$ -**	**$ -**		
Allocation of Fixed Assets	$ 23,622	$ (8,590)	$ 32,212	-375%	Allocation of Fixed Assets are fixed asset costs related to the Administrative Services programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher fixed asset expenditures being allocated.
Increase/(Decrease) Total Fixed Assets	**$ 23,622**	**$ (8,590)**	**$ 32,212**	-375%	
Total Budget	**$ 1,006,499**	**$ 919,707**	**$ 86,792**	9%	
Change in Working Capital	**$ (94,024)**	**$ -**	**$ (94,024)**		
FTEs	**3.10**	**3.10**	**0.00**	0%	

RELIABILITY FIRST

Statement of Activities, Fixed Assets and Change in Working Capital
Situation Awareness
01/01/2013 - 12/31/2013

	2013 Actual	2013 Budget	2013 Variance	%	Explanation of Variances
Funding					
ERO Funding					
ERO Assessments	$ 208,273	$ 208,273	$ -	0%	
Penalty Sanctions	31,257	31,257	-	0%	
Total ERO Funding	$ 239,530	$ 239,530	$ -	0%	
Other Funding					
Membership Fees	$ -	$ -	$ -		
Investment Income	(770)	629	(1,399)	-222%	The variance in Investment Income was due to the unrealized change in value of the company's investment portfolio offset by the dividends that were received.
Miscellaneous	-	-	-		
Total Other Funding	$ (770)	$ 629	$ (1,399)	-222%	
Total Funding	**$ 238,760**	**$ 240,159**	**$ (1,399)**		
Expenses					
Direct Expenses					
Personnel Expenses					
Salaries	$ 122,270	$ 120,045	$ 2,225	2%	
Payroll Taxes	6,222	5,984	238	4%	
Employee Benefits	5,141	7,251	(2,110)	-29%	
Savings & Retirement	18,418	19,207	(789)	-4%	
Total Personnel Expenses	$ 152,051	$ 152,487	$ (436)	0%	
Meeting Expenses					
Meetings	$ 9,638	$ 2,000	$ 7,638	382%	
Travel	25,013	30,000	(4,987)	-17%	
Conference Calls	-	-	-		
Total Meeting Expenses	$ 34,651	$ 32,000	$ 2,651	8%	
Operating Expenses					
Consultants & Contracts	$ -	$ -	$ -		
Office Rent	-	-	-		
Office Costs	4,491	2,496	1,995	80%	
Professional Services	-	-	-		
Miscellaneous	881	900	(19)	-2%	
(Gain)/Loss on Disposal of Assets	-	-	-		
Depreciation	425	425	-	0%	
Total Operating Expenses	$ 5,797	$ 3,821	$ 1,976	52%	
Total Direct Expenses	**$ 192,499**	**$ 188,308**	**$ 4,191**	2%	
Indirect Expenses	$ 65,163	$ 53,939	$ 11,224	21%	Indirect Expenses are expenses related to the Administrative Services programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher administrative expenditures being allocated.
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	**$ 257,662**	**$ 242,247**	**$ 15,415**	6%	
Net Change in Assets	**$ (18,902)**	**$ (2,088)**	**$ (16,814)**	805%	
Fixed Assets					
Depreciation	$ (425)	$ (425)	$ -	0%	
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Increase/(Decrease) Fixed Assets	**$ (425)**	**$ (425)**	**$ -**	0%	
Allocation of Fixed Assets	$ 4,572	$ (1,663)	$ 6,235	-375%	Allocation of Fixed Assets are fixed asset costs related to the Administrative Services programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher fixed asset expenditures being allocated.
Increase/(Decrease) Total Fixed Assets	**$ 4,147**	**$ (2,088)**	**$ 6,235**	-299%	
Total Budget	**$ 261,809**	**$ 240,159**	**$ 21,650**	9%	
Change in Working Capital	**$ (23,049)**	**$ -**	**$ (23,049)**		
FTEs	**0.60**	**0.60**	**0.00**	0%	

RELIABILITY FIRST

Statement of Activities, Fixed Assets and Change in Working Capital
General & Adminstrative
01/01/2013 - 12/31/2013

	2013 Actual	2013 Budget	2013 Variance	%	Explanation of Variances
Funding					
ERO Funding					
ERO Assessments	$ (221,190)	$ (221,190)	$ -	0%	
Penalty Sanctions	-	-	-		
Total ERO Funding	$ (221,190)	$ (221,190)	$ -	0%	
Other Funding					
Membership Fees	$ -	$ -	$ -		
Investment Income	-	-	-		
Miscellaneous	-	-	-		
Total Other Funding	$ -	$ -	$ -		
Total Funding	**$ (221,190)**	**$ (221,190)**	**$ -**		
Expenses					
Direct Expenses					
Personnel Expenses					
Salaries	$ 1,209,523	$ 1,245,216	$ (35,693)	-3%	
Payroll Taxes	41,727	40,166	1,561	4%	
Employee Benefits	67,553	68,109	(556)	-1%	
Savings & Retirement	157,352	110,326	47,026	43%	Savings & Retirement costs were over budget due to the reallocation of compensation resulting from the implementation of a deferred compensation plan.
Total Personnel Expenses	$ 1,476,155	$ 1,463,817	$ 12,338	1%	
Meeting Expenses					
Meetings	$ 35,702	$ 25,800	$ 9,902	38%	
Travel	71,650	59,800	11,850	20%	Travel was over budget as a result of the travel required by the office move project coordinator.
Conference Calls	-	-	-		
Total Meeting Expenses	$ 107,352	$ 85,600	$ 21,752	25%	
Operating Expenses					
Consultants & Contracts	$ 32,750	$ 21,000	$ 11,750	56%	Contracts & Consultants were over budget as a result of the leadership training being higher than budgeted, along with the five year regional assessment project that was not budgeted.
Office Rent	560,012	401,645	158,367	39%	Office Rent was over budget due to the early termination penalty for the prior office lease.
Office Costs	72,851	39,623	33,228	84%	Office costs were over budget as a result of variances in Computer Service & Maintenance. Computer Service & Maintenance was over budget as a result of the annual fees associated with the online solutions used to manage board materials and company surveys.
Professional Services	306,661	315,650	(8,989)	-3%	
Miscellaneous	10,236	11,976	(1,740)	-15%	
(Gain)/Loss on Disposal of Assets	-	-	-		
Depreciation	45,631	45,326	305	1%	
Total Operating Expenses	$ 1,028,141	$ 835,220	$ 192,921	23%	
Total Direct Expenses	**$ 2,611,648**	**$ 2,384,637**	**$ 227,011**	10%	
Indirect Expenses	$ (2,611,648)	$ (2,384,637)	$ (227,011)	10%	Indirect Expenses are expenses related to the Administrative Services Programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher General & Administrative expenditures being allocated.
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	**$ -**	**$ -**	**$ -**		
Net Change in Assets	**$ (221,190)**	**$ (221,190)**	**$ -**	0%	
Fixed Assets					
Depreciation	$ (45,631)	$ (45,326)	$ (305)	1%	
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	8,082	-	8,082		The variance in Furniture & Fixtures was a result of the purchases of office furniture to accommodate new hires and appliances for the new office.
Equipment CapEx	-	-	-		
Leasehold Improvements	550,734	-	550,734		The variance in Leasehold Improvements was a result of the planned 2014 office and data center relocation. All of these expenditures were reimbursed from our Tenant Improvement allowance.
Increase/(Decrease) Fixed Assets	**$ 513,185**	**$ (45,326)**	**$ 558,511**	-1232%	
Allocation of Fixed Assets	$ (513,185)	$ 45,326	$ (558,511)	-1232%	Allocation of Fixed Assets are fixed asset costs related to the Administrative Services programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher General & Administrative fixed asset expenditures being allocated.
Increase/(Decrease) Total Fixed Assets	**$ -**	**$ -**	**$ -**		
Total Budget	**$ -**	**$ -**	**$ -**		
Change in Working Capital	**$ (221,190)**	**$ (221,190)**	**$ -**	0%	
FTEs	**4.30**	**4.30**	**0.00**	0%	

RELIABILITY FIRST

Statement of Activities, Fixed Assets and Change in Working Capital
Legal & Regulatory Affairs
01/01/2013 - 12/31/2013

	2013 Actual	2013 Budget	2013 Variance	%	Explanation of Variances
Funding					
ERO Funding					
ERO Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		
Other Funding					
Membership Fees	$ -	$ -	$ -		
Investment Income	-	-	-		
Miscellaneous	-	-	-		
Total Other Funding	$ -	$ -	$ -		
Total Funding	**$ -**	**$ -**	**$ -**		
Expenses					
Direct Expenses					
Personnel Expenses					
Salaries	$ 374,928	$ 373,908	$ 1,020	0%	
Payroll Taxes	20,144	19,523	621	3%	
Employee Benefits	29,042	18,245	10,797	59%	Employee Benefits were over budget as a result of a variance in Medical Benefits. Medical Benefits were over budget due to an existing employee electing medical coverage that was not budgeted, along with an employee selecting a medical plan that was different than what was originally budgeted.
Savings & Retirement	60,471	58,576	1,895	3%	
Total Personnel Expenses	$ 484,585	$ 470,252	$ 14,333	3%	
Meeting Expenses					
Meetings	$ 718	$ -	$ 718		
Travel	43,800	28,000	15,800	56%	Travel expense was over budget due to more travel required of our general counsel than anticipated.
Conference Calls	-	-	-		
Total Meeting Expenses	$ 44,518	$ 28,000	$ 16,518	59%	
Operating Expenses					
Consultants & Contracts	$ -	$ -	$ -		
Office Rent	-	-	-		
Office Costs	13,643	8,308	5,335	64%	
Professional Services	50,095	65,000	(14,905)	-23%	Professional Services expense was under budget as a result of a variance in Legal Fees. Legal Fees were under budget due to negotiating flat fees for certain services and performing more legal work in house.
Miscellaneous	8	-	8		
(Gain)/Loss on Disposal of Assets	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	$ 63,746	$ 73,308	$ (9,562)	-13%	
Total Direct Expenses	**$ 592,849**	**$ 571,560**	**$ 21,289**	4%	
Indirect Expenses	$ (592,849)	$ (571,560)	$ (21,289)	4%	Indirect Expenses are expenses related to the Administrative Services Programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher Legal & Regulatory expenditures being allocated.
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	**$ -**	**$ -**	**$ -**		
Net Change in Assets	**$ -**	**$ -**	**$ -**		
Fixed Assets					
Depreciation	$ -	$ -	$ -		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Increase/(Decrease) Fixed Assets	**$ -**	**$ -**	**$ -**		
Allocation of Fixed Assets	$ -	$ -	$ -		
Increase/(Decrease) Total Fixed Assets	**$ -**	**$ -**	**$ -**		
Total Budget	**$ -**	**$ -**	**$ -**		
Change in Working Capital	**$ -**	**$ -**	**$ -**		
FTEs	**2.00**	**2.00**	**0.00**	0%	

RELIABILITY FIRST

Statement of Activities, Fixed Assets and Change in Working Capital
Information Technology
01/01/2013 - 12/31/2013

	2013 Actual	2013 Budget	2013 Variance	%	Explanation of Variances
Funding					
ERO Funding					
ERO Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		
Other Funding					
Membership Fees	$ -	$ -	$ -		
Investment Income	-	-	-		
Miscellaneous	-	-	-		
Total Other Funding	$ -	$ -	$ -		
Total Funding	**$ -**	**$ -**	**$ -**		
Expenses					
Direct Expenses					
Personnel Expenses					
Salaries	$ 592,533	$ 618,029	$ (25,496)	-4%	
Payroll Taxes	41,223	41,356	(133)	0%	
Employee Benefits	101,658	85,791	15,867	18%	Employee Benefits were over budget as a result of a variance in Individual Training. Individual Training was over budget due to vulnerability remediation training that was not budgeted for.
Savings & Retirement	87,574	97,312	(9,738)	-10%	
Total Personnel Expenses	$ 822,988	$ 842,488	$ (19,500)	-2%	
Meeting Expenses					
Meetings	$ 1,223	$ 600	$ 623	104%	
Travel	11,866	11,000	866	8%	
Conference Calls	38,097	43,092	(4,995)	-12%	
Total Meeting Expenses	$ 51,186	$ 54,692	$ (3,506)	-6%	
Operating Expenses					
Consultants & Contracts	$ 9,031	$ 36,000	$ (26,969)	-75%	Consultants & Contracts were under budget due to the postponement of several projects
Office Rent	-	60,000	(60,000)	-100%	Rent was under budget as a result of the delay in securing an offsite disaster recovery site.
Office Costs	468,239	253,085	215,154	85%	Office Costs were over budget as a result of variances in Telephone and Internet. Telephone expenses were over budget due to the large capacity phone line that was procured in preparation to support an in house conferencing system. Internet expenses were over budget due to the continued use of the contracted high bandwidth data line.
Professional Services	-	-	-		
Miscellaneous	1,639	-	1,639		
(Gain)/Loss on Disposal of Assets	(255)	-	(255)		The variance in Proceeds/Loss on Disposal of Assets was due to the gain on disposal of computer equipment that was returned.
Depreciation	153,419	177,658	(24,239)	-14%	Depreciation expense directly correlates to current and prior year fixed asset activities. As a result of the current year fixed asset purchases being under budget, there was less depreciation expense recorded this year.
Total Operating Expenses	$ 632,073	$ 526,743	$ 105,330	20%	
Total Direct Expenses	**$ 1,506,247**	**$ 1,423,923**	**$ 82,324**	6%	
Indirect Expenses	$ (1,506,247)	$ (1,423,923)	$ (82,324)	6%	
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	**$ -**	**$ -**	**$ -**		
Net Change in Assets	**$ -**	**$ -**	**$ -**		
Fixed Assets					
Depreciation	$ (153,419)	$ (177,658)	$ 24,239	-14%	Depreciation expense directly correlates to current and prior year fixed asset activities. As a result of the current year fixed asset purchases being under budget, there was less depreciation expense recorded this year.
Computer & Software CapEx	40,989	68,400	(27,411)	-40%	Computer & Software CapEx is under budget due to the planned hardware purchases being delayed or reassessed in consideration of the planned 2014 office move.
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Increase/(Decrease) Fixed Assets	**$ (112,430)**	**$ (109,258)**	**$ (3,172)**	3%	
Allocation of Fixed Assets	$ 112,430	$ 109,258	$ 3,172	3%	
Increase/(Decrease) Total Fixed Assets	**$ -**	**$ -**	**$ -**		
Total Budget	**$ -**	**$ -**	**$ -**		
Change in Working Capital	**$ -**	**$ -**	**$ -**		
FTEs	**5.15**	**5.50**	**-0.35**	-6%	

RELIABILITY FIRST

Statement of Activities, Fixed Assets and Change in Working Capital
Human Resources
01/01/2013 - 12/31/2013

	2013 Actual	2013 Budget	2013 Variance	%	Explanation of Variances
Funding					
ERO Funding					
ERO Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		
Other Funding					
Membership Fees	$ -	$ -	$ -		
Investment Income	-	-	-		
Miscellaneous	-	-	-		
Total Other Funding	$ -	$ -	$ -		
Total Funding	**$ -**	**$ -**	**$ -**		
Expenses					
Direct Expenses					
Personnel Expenses					
Salaries	$ 250,700	$ 202,709	$ 47,991	24%	Salaries were over budget due to the reallocation of the Event Planner/Receptionist position from the General & Administrative Program to the Human Resources Program.
Payroll Taxes	18,791	15,076	3,715	25%	
Employee Benefits	134,902	49,487	85,415	173%	Employee Benefits were over budget as a result of a variance in Company Training. Company Training was over budget due to the additional expenses incurred for the week of company training.
Savings & Retirement	60,524	31,626	28,898	91%	Savings & Retirements expenses were over budget due to the reallocation of the Event Planner/Receptionist position from the General & Administrative Program to the Human Resources Program, along with the administrative costs relating to the management of the company's retirement plan that were not budgeted.
Total Personnel Expenses	$ 464,917	$ 298,898	$ 166,019	56%	
Meeting Expenses					
Meetings	$ 19,144	$ 16,200	$ 2,944	18%	
Travel	7,778	8,500	(722)	-8%	
Conference Calls	-	-	-		
Total Meeting Expenses	$ 26,922	$ 24,700	$ 2,222	9%	
Operating Expenses					
Consultants & Contracts	$ 78,507	$ 31,000	$ 47,507	153%	Consultants & Contracts were over budget due to recruitment search fees paid to assist with filling the vacant technical positions.
Office Rent	-	-	-		
Office Costs	8,316	4,404	3,912	89%	
Professional Services	37,250	44,410	(7,160)	-16%	
Miscellaneous	16,498	10,690	5,808	54%	
(Gain)/Loss on Disposal of Assets	-	-	-		
Depreciation	799	799	-	0%	
Total Operating Expenses	$ 141,370	$ 91,303	$ 50,067	55%	
Total Direct Expenses	**$ 633,209**	**$ 414,901**	**$ 218,308**	53%	
Indirect Expenses	$ (633,209)	$ (414,901)	$ (218,308)	53%	Indirect Expenses are expenses related to the Administrative Services Programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the increase is due to higher Human Resource expenditures being allocated.
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	**$ -**	**$ -**	**$ -**		
Net Change in Assets	**$ -**	**$ -**	**$ -**		
Fixed Assets					
Depreciation	$ (799)	$ (799)	$ -	0%	
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Increase/(Decrease) Fixed Assets	**$ (799)**	**$ (799)**	**$ -**	0%	
Allocation of Fixed Assets	$ 799	$ 799	$ -	0%	
Increase/(Decrease) Total Fixed Assets	**$ -**	**$ -**	**$ -**		
Total Budget	**$ -**	**$ -**	**$ -**		
Change in Working Capital	**$ -**	**$ -**	**$ -**		
FTEs	**3.00**	**2.00**	**1.00**	50%	

RELIABILITY FIRST

Statement of Activities, Fixed Assets and Change in Working Capital
Finance & Accounting
01/01/2013 - 12/31/2013

	2013 Actual	2013 Budget	2013 Variance	%	Explanation of Variances
Funding					
ERO Funding					
ERO Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		
Other Funding					
Membership Fees	$ -	$ -	$ -		
Investment Income	-	-	-		
Miscellaneous	-	-	-		
Total Other Funding	$ -	$ -	$ -		
Total Funding	**$ -**	**$ -**	**$ -**		
Expenses					
Direct Expenses					
Personnel Expenses					
Salaries	$ 187,490	$ 202,166	$ (14,676)	-7%	
Payroll Taxes	13,244	13,065	179	1%	
Employee Benefits	31,776	34,067	(2,291)	-7%	
Savings & Retirement	23,833	31,992	(8,159)	-26%	
Total Personnel Expenses	$ 256,343	$ 281,290	$ (24,947)	-9%	
Meeting Expenses					
Meetings	$ -	$ -	$ -		
Travel	4,354	6,000	(1,646)	-27%	
Conference Calls	-	-	-		
Total Meeting Expenses	$ 4,354	$ 6,000	$ (1,646)	-27%	
Operating Expenses					
Consultants & Contracts	$ -	$ 10,000	$ (10,000)	-100%	Contracts & Consultants were under budget as a result of the postponement of the implementation of an automated expense management system.
Office Rent	-	-	-		
Office Costs	5,167	3,604	1,563	43%	
Professional Services	42,659	43,100	(441)	-1%	
Miscellaneous	-	-	-		
(Gain)/Loss on Disposal of Assets	-	-	-		
Depreciation	3,143	3,143	-	0%	
Total Operating Expenses	$ 50,969	$ 59,847	$ (8,878)	-15%	
Total Direct Expenses	**$ 311,666**	**$ 347,137**	**$ (35,471)**	-10%	
Indirect Expenses	$ (311,666)	$ (347,137)	$ 35,471	-10%	Indirect Expenses are expenses related to the Administrative Services Programs that have been allocated proportionately based on FTE count to the direct programs. As a result, the decrease is due to lower Finance & Accounting expenditures being allocated.
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses	**$ -**	**$ -**	**$ -**		
Net Change in Assets	**$ -**	**$ -**	**$ -**		
Fixed Assets					
Depreciation	$ (3,143)	$ (3,143)	$ -	0%	
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Increase/(Decrease) Fixed Assets	**$ (3,143)**	**$ (3,143)**	**$ -**	0%	
Allocation of Fixed Assets	$ 3,143	$ 3,143	$ -	0%	
Increase/(Decrease) Total Fixed Assets	**$ -**	**$ -**	**$ -**		
Total Budget	**$ -**	**$ -**	**$ -**		
Change in Working Capital	**$ -**	**$ -**	**$ -**		
FTEs	**1.65**	**2.00**	**-0.35**	-18%	

Reliability*First* Corporation

Financial Report
December 31, 2013

Contents

Independent Auditor's Report	1 – 2
Financial Statements	
Statements of financial position	3
Statements of activities	4
Statements of cash flows	5
Notes to financial statements	6 – 9
Supplementary Information	
Schedule of program expenses – 2013	10
Schedule of program expenses – 2012	11

McGladrey

Independent Auditor's Report

To the Board of Directors
Reliability*First* Corporation
Akron, Ohio

Report on the Financial Statements

We have audited the accompanying financial statements of Reliability*First* Corporation which comprise the statements of financial position as of December 31, 2013 and 2012, and the related statements of activities and cash flows for the years then ended and the related notes to the financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the financial statements are free of material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our audit opinion.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of Reliability*First* Corporation as of December 31, 2013 and 2012, and the changes in its net assets and its cash flows for the years then ended in accordance with accounting principles generally accepted in the United States of America.

Member of the RSM International network of independent accounting, tax and consulting firms.

Other Matter

Our audits were conducted for the purpose of forming an opinion on the financial statements as a whole. The accompanying supplementary information is presented for purposes of additional analysis and is not a required part of the financial statements. Such information is the responsibility of management and was derived from and relates directly to the underlying accounting and other records used to prepare the financial statements. The information has been subjected to the auditing procedures applied in the audits of the financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the financial statements or to the financial statements themselves, and other additional procedures in accordance with auditing standards generally accepted in the United States of America. In our opinion, the information is fairly stated in all material respects in relation to the financial statements as a whole.

McGladrey LLP

Chicago, Illinois
March 27, 2014

ReliabilityFirst Corporation

Statements of Financial Position
December 31, 2013 and 2012

	2013	2012
Assets		
Current Assets		
Cash	**$ 3,455,309**	$ 3,334,556
Investments	**3,604,721**	5,171,574
Receivables:		
Accounts	**164,055**	891,634
Lease incentives	**855,301**	-
Prepaid expenses	**424,736**	203,305
Total current assets	**8,504,122**	9,601,069
Fixed Assets		
Furniture and equipment	**132,793**	124,711
Leasehold improvements	**859,549**	308,814
Computer software and hardware	**2,272,671**	2,305,326
	3,265,013	2,738,851
Less accumulated depreciation and amortization	**1,956,014**	1,600,979
	1,308,999	1,137,872
Total assets	**$ 9,813,121**	$ 10,738,941
Liabilities and Net Assets		
Current Liabilities		
Accounts payable	**$ 591,485**	$ 87,637
Accrued expenses (current portion)	**3,673,974**	3,455,302
Total current liabilities	**4,265,459**	3,542,939
Long-Term Liabilities		
Accrued expenses (net of current portion)	**228,348**	316,269
Deferred rent	**855,301**	-
	1,083,649	316,269
Net Assets		
Unrestricted:		
Undesignated	**1,620,880**	1,916,800
Designated for reserve fund	**1,000,000**	1,000,000
Temporarily restricted	**1,843,133**	3,962,933
Total net assets	**4,464,013**	6,879,733
Total liabilities and net assets	**$ 9,813,121**	$ 10,738,941

See Notes to Financial Statements.

ReliabilityFirst Corporation

Statements of Activities
Years Ended December 31, 2013 and 2012

	2013	2012
Unrestricted Net Assets		
Revenues:		
Quarterly assessments	**$ 14,165,848**	$ 13,534,272
Investment (loss) income	**(66,853)**	51,880
Penalty sanctions released from restriction	**2,979,800**	792,100
Miscellaneous	**-**	250
	17,078,795	14,378,502
Expenses:		
Program:		
Standards	**133,503**	283,762
Compliance	**8,567,222**	7,735,947
Assessment	**1,954,152**	1,813,756
Training and education	**646,201**	591,483
Situational awareness	**192,074**	175,572
General and administrative	**2,566,017**	2,430,473
Legal and regulatory	**592,849**	532,264
Information technology	**1,353,083**	1,452,954
Human resources	**632,410**	360,093
Finance	**308,523**	324,235
	16,946,034	15,700,539
General:		
Depreciation and amortization	**428,936**	440,645
(Gain) loss on disposal of fixed assets	**(255)**	21,171
	428,681	461,816
	17,374,715	16,162,355
(Decrease) in unrestricted net assets	**(295,920)**	(1,783,853)
Temporarily Restricted Net Assets		
Penalty sanctions	**860,000**	1,583,433
Penalty sanctions released from restriction	**(2,979,800)**	(792,100)
(Decrease) increase in temporarily restricted net assets	**(2,119,800)**	791,333
Decrease in total net assets	**(2,415,720)**	(992,520)
Net assets at beginning of year	**6,879,733**	7,872,253
Net assets at end of year	**$ 4,464,013**	$ 6,879,733

See Notes to Financial Statements.

ReliabilityFirst Corporation

Statements of Cash Flows
Years Ended December 31, 2013 and 2012

	2013	2012
Cash Flows from Operating Activities		
Change in net assets	**$ (2,415,720)**	$ (992,520)
Adjustments to reconcile change in net assets to net cash used in operating activities:		
Depreciation and amortization	**428,936**	440,645
(Gain) loss on disposal of fixed assets	**(255)**	21,171
Unrealized loss on investments	**141,889**	39,996
Realized loss on investments	**6,309**	11,061
Changes in assets and liabilities:		
Accounts receivable	**727,579**	(435,249)
Lease incentives receivable	**(855,301)**	-
Prepaid expenses	**(221,431)**	43,247
Accounts payable	**503,848**	(13,214)
Accrued expenses	**130,751**	579,799
Deferred rent	**855,301**	-
Net cash used in operating activities	**(698,094)**	(305,064)
Cash Flows from Investing Activities		
Purchase of investments	**(81,345)**	(2,021,437)
Sale of investments	**1,500,000**	1,500,000
Additions to fixed assets	**(599,808)**	(292,993)
Proceeds from sale of fixed assets	**-**	5,740
Net cash provided by (used) in investing activities	**818,847**	(808,690)
Net increase (decrease) in cash	**120,753**	(1,113,754)
Cash at beginning of year	**3,334,556**	4,448,310
Cash at end of year	**$ 3,455,309**	$ 3,334,556

See Notes to Financial Statements.

Note 1. Organization and Significant Accounting Policies

Organization: ReliabilityFirst Corporation (the Corporation) is a not-for-profit corporation whose mission is to preserve and enhance electric service reliability and security for the interconnected electric systems within its territory. The Corporation was approved by the North American Electric Reliability Corporation (NERC) to become one of eight Regional Entities of NERC. The Corporation conducts its activities from leased offices in Akron, Ohio.

The Corporation receives its quarterly assessments from NERC. A significant reduction in the level of this support, if this were to occur, may have a significant effect on the Corporation's operations.

The following is a summary of the Corporation's significant accounting policies which conform to accounting principles generally accepted in the United States of America (U.S. GAAP).

Use of estimates: The preparation of financial statements in conformity with U.S. GAAP requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities and disclosure of contingent assets and liabilities at the date of the financial statements and the reported amounts of revenue and expenses during the reporting period. Actual results could differ from those estimates.

Revenue recognition: The Corporation currently derives its revenues primarily from quarterly assessments. Revenues from such assessments are recognized as unrestricted revenues at the time services are performed and the cost of these services is recognized when incurred. Penalty sanctions are recognized after the entire appeals process has been exhausted and a Federal Electric Regulatory Commission (FERC) order has been issued and are non-appealable. Penalty sanctions received on or prior to June 30 of each year shall be applied as a general offset to budget requirements for the subsequent fiscal year. Penalty sanctions received after June 30 of each year shall be applied as a general offset to budget requirements for the next subsequent fiscal year.

Cash: The Corporation maintains its cash in non-interest-bearing bank deposit accounts. Management believes it is not exposed to any significant credit risk on cash.

Receivables: Accounts receivable are carried at actual billed amounts relating to penalty sanctions and subcontractor receivables. There was no allowance for doubtful accounts recorded in 2013 or 2012. During 2013, the Corporation recorded a receivable of $855,301 from its new landlord relating to lease incentives provided to reimburse leasehold improvements and a termination penalty on an existing lease, which related to 2013.

Investments: Investments are carried at fair value. The fair values of marketable debt securities are based on quoted market prices. Realized investment gains and losses represent the difference between the proceeds on sales of investments and their carrying value. Investment income includes interest, dividends and both realized and unrealized gains and losses. All realized and unrealized gains and losses on investments are reported as increases or decreases, respectively, to unrestricted net assets.

The Corporation invests in fixed income mutual funds. Such investments are exposed to various risks such as interest rate, market and credit. Due to the level of risk associated with such investments and the level of uncertainty related to changes in the value of such investments, it is at least reasonably possible that changes in risks in the near term would materially affect investment balances and the amounts reported in the financial statements.

Prepaid expenses: Prepaid expenses consist of expenses paid for in advance that will be recognized within a future operating cycle.

Note 1. Organization and Significant Accounting Policies (Continued)

Fixed assets: Fixed assets are stated at cost. Depreciation is computed on the straight-line method over the estimated useful lives (generally 3 to 7 years) of the depreciable assets. Amortization for the leasehold improvements is computed on the lesser of the useful life or the lease term.

Income taxes: The Corporation is exempt from federal income taxes under Section 501(c)(6) of the Internal Revenue Code and applicable state law, except for taxes pertaining to unrelated business income, if any.

In accordance with the accounting standard on accounting for uncertainty in income taxes, the Corporation addresses the determination of whether tax benefits claimed or expected to be claimed on a tax return should be recorded in the financial statements. Under this guidance, the Corporation may recognize the tax benefit from an uncertain tax position only if it is more likely than not that the tax position will be sustained on examination by taxing authorities, based on the technical merits of the position. Examples of tax positions include the tax-exempt status of the Corporation and various positions related to the potential sources of unrelated business taxable income (UBIT). The tax benefits recognized in the financial statements from such a position are measured based on the largest benefit that has a greater than 50 percent likelihood of being realized upon ultimate settlement. There were no unrecognized tax benefits identified or recorded as liabilities during the periods covered by these financial statements.

The Corporation files forms 990 in the U.S. federal jurisdiction and the State of Ohio. The Corporation is generally no longer subject to examination by the Internal Revenue Service for years before 2010.

Net assets: Of the unrestricted net asset balance, $1,000,000 has been designated by the Board of Directors for its operating reserve fund at December 31, 2013 and 2012.

Temporarily restricted net assets result from the receipt of penalty sanctions which are restricted based on timing conditions as described in the Corporation's revenue recognition policy. Penalty monies are governed by a restriction by NERC as to when the funds can be used. Temporary restricted net assets at December 31, 2013 and 2012, were $1,843,133 and $3,962,933, respectively.

Subsequent events: The Corporation has evaluated subsequent events for potential recognition and/or disclosure through the date these financial statements were available to be issued.

Note 2. Investments

The Corporation maintains an investment portfolio which consists of fixed income securities. The fair values of the investments at December 31, 2013 and 2012, were $3,604,721 and $5,171,574, respectively. The composition of investment income (loss) is as follows at December 31:

	2013	2012
Interest/dividends	$ 81,345	$ 102,937
Realized loss	(6,309)	(11,061)
Unrealized loss	(141,889)	(39,996)
	$ (66,853)	$ 51,880

Note 3. Fair Value

As described in Note 1, the Corporation records its investments at fair value. Fair value is the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date. The Financial Accounting Standards Board's (FASB) authoritative guidance on fair value measurements establishes a framework for measuring fair value, and expands disclosure about fair value measurements. This guidance enables the reader of the financial statements to assess the inputs used to develop those measurements by establishing a hierarchy for ranking the quality and reliability of the information used to determine fair values. Under this guidance, assets and liabilities carried at fair value must be classified and disclosed in one of the following three categories:

- Level 1: Valuations for assets and liabilities traded in active exchange markets, such as the New York Stock Exchange. Level 1 also includes U.S. Treasury and federal agency securities and federal agency mortgage-backed securities, which are traded by dealers or brokers in active markets. Valuations are obtained from readily available pricing sources for market transactions involving identical assets or liabilities.
- Level 2: Valuations for assets and liabilities traded in less active dealer or broker markets. Valuations are obtained from third-party pricing services for identical or similar assets or liabilities.
- Level 3: Valuations for assets and liabilities that are derived from other valuation methodologies, including option pricing models, discounted cash flow models and similar techniques, and not based on market exchange, dealer, or broker-traded transactions. Level 3 valuations incorporate certain assumptions and projections in determining the fair value assigned to such assets or liabilities.

In determining the appropriate levels, the Corporation performs a detailed analysis of the assets and liabilities that are measured and reported on a fair value basis. At each reporting period, all assets and liabilities for which the fair value measurement is based on significant unobservable inputs would be classified as Level 3.

The Corporation assesses the levels at each measurement date, and transfers between levels are recognized on the date of the actual event or change in the circumstances that caused the transfer in accordance with the Corporation's accounting policy regarding the recognition of the transfer between levels of the fair value hierarchy. For the years ended December 31, 2013 and 2012, there were no such transfers.

As of December 31, 2013 and 2012, the Corporation's investments are fixed income class A mutual funds, which are classified as Level 1.

Note 4. Line of Credit

The Corporation has a $1,000,000 line of credit due on September 24, 2014. The line is collateralized by substantially all assets of the Corporation and interest is charged at LIBOR plus 2.75 percent. The Corporation did not make any drawdowns on the line during the year and had no outstanding balance as of December 31, 2013 or 2012. The Corporation intends to renew the line when it becomes due on September 24, 2014.

Note 5. Operating Leases

The Corporation leases its office and additional storage space from unrelated third parties. On July 16, 2013, the Corporation provided written notice exercising its early termination right for its existing lease with Bath Springside, Ltd. As a result, the Corporation's lease with Bath Springside, Ltd. will terminate on December 31, 2014 and the Corporation will incur a lease termination penalty of $200,000, which will be reimbursed by its new landlord, Investors Warranty of America, Inc. The penalty was recorded in accounts payable at December 31, 2013.

On June 14, 2013, the Corporation signed a 13 year lease with Investors Warranty of America, Inc. (Landlord), with an estimated commencement date of March 1, 2014. According to the lease, the Landlord will provide the Corporation with a $1,854,956 tenant improvement allowance for leasehold improvements and other soft costs. In 2013, the Corporation capitalized $550,734 in leasehold improvements and $104,567 in soft costs.

The above reimbursement of the lease termination penalty and the leasehold improvements were recorded in lease incentives receivable and deferred rent at December 31, 2013. This liability will be amortized over the life of the lease against rent expense, starting on the commencement date of the new lease.

Rental expense for operating leases amounted to $508,704 and $346,873 for the years ended December 31, 2013 and 2012, respectively. The 2013 rent expense includes $32,114 in accelerated straight-line amortization of the previous deferred rent liability due to the early termination of the lease. The remaining deferred rent liability of $72,537 will be recognized against the 2014 straight-line rent expense of $346,873.

The future minimum lease payments relating to the new lease on a straight-line basis are as follows:

2014	$ 496,336
2015	595,603
2016	595,603
2017	595,603
2018	595,603
Thereafter	4,864,089
	$ 7,742,837

Note 6. Employee Retirement Plan

The Corporation has a salary deferral plan under Section 401(k) of the Internal Revenue Code. All employees are eligible for 100 percent match of their first 6 percent of voluntary salary deferral savings and the 3 percent Safe Harbor provision of the plan. Employees who have at least 1,000 hours during the year are eligible for a certain percentage discretionary provision of the plan (7 percent in 2013 and 2012). Therefore, under this plan, the Corporation provided for a potential maximum contribution of up to 16 percent of employees' eligible compensation in 2013 and 2012. The Corporation's contributions to the plan for 2013 and 2012 were approximately $1,469,000 and $1,213,000, respectively.

ReliabilityFirst Corporation

Schedule of Program Expenses
Year Ended December 31, 2013

	Standards	Compliance	Assessment	Training and Education	Situational Awareness	General and Administrative	Legal and Regulatory	Information Technology	Human Resources	Finance	Total
Personnel Expenses											
Salaries	$ 85,293	$ 5,456,087	$ 1,308,756	$ 419,851	$ 122,270	$ 1,209,523	$ 374,928	$ 592,533	$ 250,700	$ 187,490	$ 10,007,431
Payroll taxes	7,190	355,198	79,803	28,288	6,222	41,727	20,144	41,223	18,791	13,244	611,830
Employee benefits	10,677	751,014	119,349	54,888	5,141	67,553	29,042	101,658	134,902	31,776	1,306,000
Savings and retirement	16,969	801,891	201,906	63,056	18,418	157,352	60,471	87,574	60,524	23,833	1,491,994
Total personnel expenses	120,129	7,364,190	1,709,814	566,083	152,051	1,476,155	484,585	822,988	464,917	256,343	13,417,255
Meeting Expenses											
Meetings	-	12,964	19,252	74,751	9,638	35,702	718	1,223	19,144	-	173,392
Travel	11,216	490,599	94,243	5,367	25,013	71,650	43,800	11,866	7,778	4,354	765,886
Conference calls	-	-	-	-	-	-	-	38,097	-	-	38,097
Total meeting expenses	11,216	503,563	113,495	80,118	34,651	107,352	44,518	51,186	26,922	4,354	977,375
Operating Expenses											
Rent and improvements	-	-	-	-	-	560,012	-	-	-	-	560,012
Contracts	-	409,643	79,557	-	-	32,750	-	9,031	78,507	-	609,488
Office costs	2,037	84,876	11,266	-	2,571	30,601	13,643	317,073	3,143	1,917	467,127
Professional services	-	15,000	-	-	-	306,661	50,095	-	37,250	42,659	451,665
Computer purchase and maintenance	-	188,691	39,961	-	1,920	39,603	-	151,166	5,173	3,250	429,764
Furniture and equipment	-	-	-	-	-	2,647	-	-	-	-	2,647
Miscellaneous	121	1,259	59	-	881	10,236	8	1,639	16,498	-	30,701
Total operating expenses	2,158	699,469	130,843	-	5,372	982,510	63,746	478,909	140,571	47,826	2,551,404
Subtotal	$ 133,503	$ 8,567,222	$ 1,954,152	$ 646,201	$ 192,074	$ 2,566,017	$ 592,849	$ 1,353,083	$ 632,410	$ 308,523	16,946,034
Depreciation and amortization											428,936
Loss on disposal of assets											(255)
Total expenses											$ 17,374,715

ReliabilityFirst Corporation

Schedule of Program Expenses
Year Ended December 31, 2012

	Standards	Compliance	Assessment	Training and Education	Situational Awareness	General and Administrative	Legal and Regulatory	Information Technology	Human Resources	Finance	Total
Personnel Expenses											
Salaries	$ 202,280	$ 4,864,355	$ 1,220,240	$ 401,640	$ 119,921	$ 1,283,618	$ 371,782	$ 599,465	$ 196,143	$ 196,068	$ 9,455,512
Payroll taxes	12,109	349,122	83,346	29,842	9,031	52,293	22,263	41,266	16,193	15,657	631,122
Employee benefits	20,887	665,552	111,461	53,703	4,719	61,454	15,038	96,411	49,682	31,877	1,110,784
Savings and retirement	26,683	662,668	171,091	57,556	14,105	79,279	53,096	87,895	29,755	31,195	1,213,323
Total personnel expenses	261,959	6,541,697	1,586,138	542,741	147,776	1,476,644	462,179	825,037	291,773	274,797	12,410,741
Meeting Expenses											
Meetings	-	4,722	21,947	46,004	4,477	56,397	227	1,109	3,792	214	138,889
Travel	19,214	469,686	90,214	2,738	19,449	62,559	31,947	6,577	6,228	6,879	715,491
Conference calls	75	4,551	1,830	-	77	384	-	28,976	-	-	35,893
Total meeting expenses	19,289	478,959	113,991	48,742	24,003	119,340	32,174	36,662	10,020	7,093	890,273
Operating Expenses											
Rent and improvements	-	-	-	-	-	396,974	-	-	-	-	396,974
Contracts	-	465,337	59,124	-	-	59,285	-	9,515	5,195	-	598,456
Office costs	2,514	103,402	13,183	-	2,945	43,987	10,145	310,398	4,024	725	491,323
Professional services	-	22,439	-	-	-	321,308	27,766	-	37,854	37,642	447,009
Computer purchase and maintenance	-	122,892	40,945	-	-	2,727	-	271,342	932	3,978	442,816
Furniture and equipment	-	-	-	-	-	-	-	-	-	-	-
Miscellaneous	-	1,221	375	-	848	10,208	-	-	10,295	-	22,947
Total operating expenses	2,514	715,291	113,627	-	3,793	834,489	37,911	591,255	58,300	42,345	2,399,525
Subtotal	$ 283,762	$ 7,735,947	$ 1,813,756	$ 591,483	$ 175,572	$ 2,430,473	$ 532,264	$ 1,452,954	$ 360,093	$ 324,235	15,700,539
										Depreciation and amortization	440,645
										Loss on disposal of assets	21,171
										Total expenses	$ 16,162,355

ATTACHMENT 6

2013 ACTUAL COST-TO-BUDGET COMPARISON

AND

2013 AUDITED FINANCIAL REPORT

FOR

SERC RELIABILITY CORPORATION

SERC Reliability Corporation
2815 Coliseum Centre Drive | Suite 500
Charlotte, NC 28217
704.357.7372 | Fax 704.357.7914 | www.serc1.org

May 1, 2014

Mike Walker
Chief Financial Officer
North American Electric Reliability Corporation

SERC 2013 Budget vs. Actual Variance Analysis

Enclosed is SERC's response to your request for information on variances between the 2013 SERC budget and year-end financials.

Overall, SERC over ran 2013 budgeted revenues by $93,264 and under spent its 2013 budgeted expenses of $16,094,659 by $551,358. The net impact was a $644,622 positive variance on SERC's cash position for the year.

During 2013, SERC conducted 55 audits and spot checks including 16 on-site and 9 off-site operations and planning audits, 4 operations and planning audits of multi-regional Registered Entities, and 9 on-site and 21 off-site CIP audits. SERC adjusted the planned audits and spot checks pursuant to supplemental guidance provided by NERC and FERC. SERC identified 363 new potential violations and closed 323 enforcement actions addressing possible violations identified during the period from 2008 through 2012. In addition, SERC completed all budgeted reliability assessments for the year.

There are several mitigating circumstances, as explained below:

- During 2013, total personnel costs were lower than budget due to several factors. SERC was not fully staffed during 2013 by 7.56 FTEs. Additionally, when preparing the budget, SERC budgeted retirement costs based on historical data. The actual employee contribution for 2013 was lower than budgeted, causing the corresponding company match to be lower than budgeted.
- Due to the strains on the economy, SERC has emphasized the use of conference calls and Webex capabilities to reduce the number of face to face meetings, which reduced travel and meeting costs. Additionally, SERC continues to work with the same hotels, which provides cost savings on larger meetings, and SERC is now hosting more meetings in the Charlotte office at a significantly reduced cost.
- SERC used contractors to support audit and enforcement activities; engaged a management consulting firm to support SERC's corporate initiative for management training; and a project manager and architecture firm to assist with the design, construction, and coordination of the relocation of SERC's offices in 2014, causing an unplanned overrun in Consultants and Contractors.

- In a coordinated effort with the other regional entities on the preparation of the Five Year Assessment, SERC managed the contract with the consultant, subject to reimbursement from the other regional entities. The offsetting revenue is recorded in Miscellaneous income.
- SERC purchased office furniture and equipment to furnish the new office space, causing the over run in Office Costs.

SERC has no non-statutory activity, and therefore no statutory funding was used for non-statutory activities.

All personnel costs for the other administrative functions, including Information Technology, Legal, Finance, and Human Resources, are recorded within General and Administrative to protect the confidentiality of individual compensation information of employees in these programs.

SERC allocates indirect or administrative expenses and capital expenditures to the statutory programs based upon the ratio of FTEs in those program areas to total statutory program FTEs. The variances associated with this allocation are the result of the differences in the actual versus budgeted ratio of FTEs and the actual versus budgeted spend in the administrative cost centers.

SERC performs the Compliance Enforcement Activities for FRCC and SPP. The regional entity reimburses SERC for the actual costs incurred, including an overhead calculation. These costs have been recorded separately on the Compliance Enforcement Activity Statement of Activities.

Detailed descriptions of budget to actual variances are provided in the attached file. If you have any questions, please feel free to call or email me.

Yours truly,

Jennifer Kelly

cc: R. Scott Henry

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013

Total Statutory	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)
Funding			
ERO Funding			
Assessments	13,829,878	13,829,878	-
Penalty Sanctions	51,000	51,000	-
Total ERO Funding	**$ 13,880,878**	**$ 13,880,878**	**$ -**
Federal Grants	-	-	-
Membership Fees	-	-	-
Testing	-	-	-
Services & Software	-	-	-
Workshop Fees	173,997	246,000	(72,003)
Interest	1,271	10,000	(8,729)
Miscellaneous	238,996	65,000	173,996
Total Funding (A)	**$ 14,295,142**	**$ 14,201,878**	**$ 93,264**
Expenses			
Personnel Expenses			
Salaries	9,176,085	9,925,148	(749,063)
Payroll Taxes	632,913	595,509	37,404
Employee Benefits	896,790	916,101	(19,311)
Savings & Retirement	1,169,319	1,353,523	(184,204)
Total Personnel Expenses	**11,875,107**	**12,790,281**	**(915,174)**
Meeting Expenses			
Meetings	276,839	309,160	(32,321)
Travel	646,398	595,023	51,375
Conference Calls	49,760	60,000	(10,240)
Total Meeting Expenses	**972,997**	**964,183**	**8,814**
Operating Expenses			
Consultants & Contracts	1,410,698	1,166,947	243,751
Rent & Improvements	403,731	405,407	(1,676)
Office Costs	633,768	361,552	272,216
Professional Services	107,705	105,900	1,805
Miscellaneous	2,148	-	2,148
Depreciation	137,147	300,389	(163,242)
Total Operating Expenses	**2,695,197**	**2,340,195**	**355,002**
Indirect Expenses	**-**	**-**	**-**
Other Non-Operating Expenses	**-**	**-**	**-**
Total Expenses (B)	**15,543,301**	**16,094,659**	**(551,358)**
Change in Assets (A - B)	**(1,248,159)**	**(1,892,781)**	**644,622**
Fixed Assets			
Depreciation	(137,147)	(300,389)	163,242
Computer & Software CapEx	474,813	113,333	361,480
Furniture & Fixtures CapEx	-	-	-
Equipment CapEx	-	-	-
Leasehold Improvements	-	-	-
Incr(Dec) in Fixed Assets	(337,666)	187,056	(524,722)
Allocation of Fixed Assets	-	-	-
Total Inc(Dec) in Fixed Assets (C)	**(337,666)**	**187,056**	**(524,722)**
TOTAL BUDGET (B - C)	**15,880,967**	**15,907,603**	**(26,636)**
Change in Working Capital (A-B+C)	**(1,585,825)**	**(1,705,725)**	**119,900**
FTE's	**69.89**	**77.45**	**(7.56)**

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013
Per Audit

RELIABILITY STANDARDS	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	698,880	698,880	-	0.00%	
Penalty Sanctions	2,358	2,358	-	0.00%	
Total ERO Funding	**$ 701,238**	**$ 701,238**	**$ -**	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	87	-	87		
Total Funding (A)	701,325	701,238	87	0.01%	
Expenses					
Personnel Expenses					
Salaries	226,234	337,825	(111,591)	-33.03%	SERC budgeted 2.66 FTE's in the Standards program during 2013. SERC finished 2013 with 1.72 FTEs, a difference of 0.94 FTEs, causing SERC to be under budget.
Payroll Taxes	17,470	20,270	(2,800)	-13.81%	
Employee Benefits	26,540	34,294	(7,754)	-22.61%	
Savings & Retirement	13,925	46,701	(32,776)	-70.18%	SERC budgeted based on historical employee contributions. The actual employee contribution for 2013 was lower than budgeted, causing the corresponding company match to be lower than budgeted. Additionally, as noted above in Salaries Expense, SERC was not fully staffed. Due to this, SERC incurred less expense.
Total Personnel Expenses	284,169	439,090	(154,921)	-35.28%	
Meeting Expenses					
Meetings	302	-	302		
Travel	5,804	9,101	(3,297)	-36.23%	SERC continues to emphasize the use of technology by hosting meetings using WebEx. By doing this, travel costs have decreased.
Conference Calls	-	-	-		
Total Meeting Expenses	6,106	9,101	(2,995)	-32.91%	
Operating Expenses					
Consultants & Contracts	-	-	-		
Rent & Improvements	-	-	-		
Office Costs	799	355	444	125.07%	
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	799	355	444	125.07%	
Indirect Expenses	300,056	261,342	38,714	14.81%	Expenses related to indirect programs have been allocated proportionately to the direct programs for 2013 based on the number of FTEs in those programs
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	591,130	709,888	(118,758)	-16.73%	
Change in Assets (A - B)	110,195	(8,650)	118,845	-1373.93%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	(17,273)	8,650	(25,923)	-299.69%	
Total Inc(Dec) in Fixed Assets (C)	(17,273)	8,650	(25,923)	-299.69%	
TOTAL BUDGET (B - C)	**608,403**	**701,238**	**(92,835)**	**-13.24%**	
Change in Working Capital (A-B+C)	**92,922**	**-**	**92,922**		
FTE's	**1.72**	**2.66**	**(0.94)**	**-35.34%**	

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013
Per Audit

COMPLIANCE OPERATIONS, ENFORCEMENT and ORGANIZATION REGISTRATION	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	11,150,647	11,150,647	-	0.00%	
Penalty Sanctions	36,796	36,796	-	0.00%	
Total ERO Funding	**$ 11,187,443**	**$ 11,187,443**	**$ -**	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	1,467	-	1,467		
Total Funding (A)	11,188,910	11,187,443	1,467	0.01%	
Expenses					
Personnel Expenses					
Salaries	4,422,701	5,080,600	(657,899)	-12.95%	SERC budgeted 41.5 FTE's in the Compliance program during 2013. SERC finished 2013 with 37.14 FTEs, a difference of 4.36 FTEs, causing SERC to be under budget. SERC used contractors to assist in completing the work.
Payroll Taxes	331,116	307,536	23,580	7.67%	
Employee Benefits	470,656	483,979	(13,323)	-2.75%	
Savings & Retirement	636,236	705,345	(69,109)	-9.80%	SERC budgeted based on historical employee contributions. The actual employee contribution for 2013 was lower than budgeted, causing the corresponding company match to be lower than budgeted.
Total Personnel Expenses	5,860,709	6,577,460	(716,751)	-10.90%	
Meeting Expenses					
Meetings	26,743	17,910	8,833	49.32%	
Travel	380,406	377,966	2,440	0.65%	
Conference Calls	-	-	-		
Total Meeting Expenses	407,149	395,876	11,273	2.85%	
Operating Expenses					
Consultants & Contracts	474,637	249,167	225,470	90.49%	SERC is over budget in Consultants & Contracts due to the use of contractors to support audit and enforcement activities. Additionally, SERC developed tools to allow for handling of protected entity information and an audit checklist tool, causing an unplanned overrun.
Rent & Improvements	-	-	-		
Office Costs	16,050	12,578	3,472	27.60%	
Professional Services	8,513	15,000	(6,487)	-43.25%	
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	499,200	276,745	222,455	80.38%	
Indirect Expenses	4,174,852	4,072,321	102,531	2.52%	Expenses related to indirect programs have been allocated proportionately to the direct programs for 2013 based on the number of FTEs in those programs
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	10,941,910	11,322,402	(380,492)	-3.36%	
Change in Assets (A - B)	247,000	(134,959)	381,959	-283.02%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	(241,171)	134,959	(376,130)	-278.70%	
Total Inc(Dec) in Fixed Assets (C)	(241,171)	134,959	(376,130)	-278.70%	
TOTAL BUDGET (B - C)	**11,183,081**	**11,187,443**	**(4,362)**	**-0.04%**	
Change in Working Capital (A-B+C)	**5,829**	**-**	**5,829**		
FTE's	**37.14**	**41.50**	**(4.36)**	**-10.51%**	

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013
Per Audit

COMPLIANCE ENFORCEMENT ACTIVITY	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	-	-	-		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	175,852	65,000	110,852	170.54%	The income recorded in Miscellaneous relates to the cross regional monitoring activities for FRCC and SPP. The regional entity audited reimburses SERC for actual costs incurred. The 2013 Budget includes $15,000 related to enforcement activities for FRCC and $50,000 related to auditing and enforcement activities for SPP. During 2013, SERC continued to execute its contracted duties and participated on an unbudgeted audit, in accordance with a coordination agreement with FRCC RE.
Total Funding (A)	175,852	65,000	110,852	170.54%	
Expenses					
Personnel Expenses					
Salaries	134,025	45,000	89,025	197.83%	Amount represents the total personnel expenses related to the cross regional monitoring activities for FRCC and SPP. During 2013, SERC continued to execute its contracted duties and participated on an unbudgeted audit, in accordance with a coordination agreement with FRCC RE.
Payroll Taxes	-	-	-		
Employee Benefits	-	-	-		
Savings & Retirement	-	-	-		
Total Personnel Expenses	134,025	45,000	89,025	197.83%	
Meeting Expenses					
Meetings	-	-	-		
Travel	27,173	15,000	12,173	81.15%	Amount represents the travel expenses related to the cross regional monitoring activities for FRCC. During 2013, SERC continued to execute its contracted duties and participated on an unbudgeted audit, in accordance with a coordination agreement with FRCC RE, causing an over run.
Conference Calls	-	-	-		
Total Meeting Expenses	27,173	15,000	12,173	81.15%	
Operating Expenses					
Consultants & Contracts	-	-	-		
Rent & Improvements	-	-	-		
Office Costs	-	-	-		
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	-	-	-		
Indirect Expenses	14,654	5,000	9,654	193.08%	
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	175,852	65,000	110,852	170.54%	
Change in Assets (A - B)	-	-	-		
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B - C)	**175,852**	**65,000**	**110,852**	**170.54%**	
Change in Working Capital (A-B+C)	-	-	-		
FTE's	-	-	-		

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013
Per Audit

RELIABILITY ASSESSMENTS and PERFORMANCE ANALYSIS	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	1,937,756	1,937,756	-	0.00%	
Penalty Sanctions	6,384	6,384	-	0.00%	
Total ERO Funding	**$ 1,944,140**	**$ 1,944,140**	**$ -**	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	1,944,140	1,944,140	-	0.00%	
Expenses					
Personnel Expenses					
Salaries	723,751	743,697	(19,946)	-2.68%	SERC budgeted 7.20 FTE's in the RAPA program during 2013. SERC finished 2013 with 6.69 FTEs, a difference of 0.51 FTEs, causing SERC to be under budget. This was offset by the positions within RAPA were filled at a higher than budgeted salary.
Payroll Taxes	56,925	44,622	12,303	27.57%	Payroll Tax expense was higher than budgeted due to filling positions in RAPA at higher than budgeted salaries.
Employee Benefits	93,610	99,594	(5,984)	-6.01%	
Savings & Retirement	93,427	103,868	(10,441)	-10.05%	SERC budgeted based on historical employee contributions. The actual employee contribution for 2013 was lower than budgeted, causing the corresponding company match to be lower than budgeted.
Total Personnel Expenses	967,713	991,781	(24,068)	-2.43%	
Meeting Expenses					
Meetings	28,428	32,285	(3,857)	-11.95%	A greater emphasis on the use of technology by hosting WebEx meetings, as well as utilizing member facilities, has lowered meeting costs.
Travel	69,856	30,667	39,189	127.79%	In an effort to train and develop new staff, SERC sent additional employees to meetings, causing an overrun.
Conference Calls	-	-	-		
Total Meeting Expenses	98,284	62,952	35,332	56.13%	
Operating Expenses					
Consultants & Contracts	194,865	203,000	(8,135)	-4.01%	
Rent & Improvements	-	-	-		
Office Costs	4,648	2,431	2,217	91.20%	
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	199,513	205,431	(5,918)	-2.88%	
Indirect Expenses	754,653	707,391	47,262	6.68%	Expenses related to indirect programs have been allocated proportionately to the direct programs for 2013 based on the number of FTEs in those programs
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	2,020,163	1,967,555	52,608	2.67%	
Change in Assets (A - B)	(76,023)	(23,415)	(52,608)	224.68%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	(43,442)	23,415	(66,857)	-285.53%	
Total Inc(Dec) in Fixed Assets (C)	(43,442)	23,415	(66,857)	-285.53%	
TOTAL BUDGET (B - C)	**2,063,605**	**1,944,140**	**119,465**	**6.14%**	
Change in Working Capital (A-B+C)	**(119,465)**	**-**	**(119,465)**		
FTE's	**6.69**	**7.20**	**(0.51)**	**-7.08%**	

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013
Per Audit

TRAINING, EDUCATION and OPERATOR CERTIFICATION	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	701,400	701,400	-	0.00%	
Penalty Sanctions	2,137	2,137	-	0.00%	
Total ERO Funding	**$ 703,537**	**$ 703,537**	**$ -**	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	173,997	246,000	(72,003)	-29.27%	In 2013, SERC began holding most meetings in house, resulting in a savings in costs, and therefore an offsetting decrease in revenue allowing SERC to charge a reduced attendance fee, from when the budget was developed
Interest	-	-	-		
Miscellaneous	87	-	87		
Total Funding (A)	877,621	949,537	(71,916)	-7.57%	
Expenses					
Personnel Expenses					
Salaries	300,729	334,005	(33,276)	-9.96%	SERC budgeted 7.20 FTE's in the Standards program during 2013. SERC finished 2013 with 6.69 FTEs, a difference of 0.51 FTEs, causing SERC to be under budget.
Payroll Taxes	20,837	20,040	797	3.98%	
Employee Benefits	27,231	26,612	619	2.33%	
Savings & Retirement	35,589	41,864	(6,275)	-14.99%	SERC budgeted based on historical employee contributions. The actual employee contribution for 2013 was lower than budgeted, causing the corresponding company match to be lower than budgeted.
Total Personnel Expenses	384,386	422,521	(38,135)	-9.03%	
Meeting Expenses					
Meetings	142,043	192,975	(50,932)	-26.39%	SERC continues to work with the same hotels, which provides cost savings on larger meetings. Additionally, as noted in the workshop fee revenue, SERC is now hosting more meetings in the Charlotte office at a significantly reduced cost. Finally, a greater emphasis on the use of technology by hosting WebEx meetings has lowered meeting costs.
Travel	13,986	22,781	(8,795)	-38.61%	SERC continues to emphasize the use of technology by hosting meetings using WebEx. Additionally, SERC is now hosting more meetings in the Charlotte office, which does not require staff to travel. By doing this, travel costs have decreased.
Conference Calls	-	-	-		
Total Meeting Expenses	156,029	215,756	(59,727)	-27.68%	
Operating Expenses					
Consultants & Contracts	90,077	82,000	8,077	9.85%	
Rent & Improvements	-	-	-		
Office Costs	4,971	318	4,653	1463.21%	
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	95,048	82,318	12,730	15.46%	
Indirect Expenses	269,599	236,779	32,820	13.86%	Expenses related to indirect programs have been allocated proportionately to the direct programs for 2013 based on the number of FTEs in those programs
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	905,062	957,374	(52,312)	-5.46%	
Change in Assets (A - B)	(27,441)	(7,837)	(19,604)	250.15%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	(15,520)	7,837	(23,357)	-298.03%	
Total Inc(Dec) in Fixed Assets (C)	(15,520)	7,837	(23,357)	-298.03%	
TOTAL BUDGET (B - C)	**920,582**	**949,537**	**(28,955)**	**-3.05%**	
Change in Working Capital (A-B+C)	**(42,961)**	**-**	**(42,961)**		
FTE's	**2.39**	**2.41**	**(0.02)**	**-0.83%**	

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013
Per Audit

SITUATION AWARENESS and INFRASTRUCTURE SECURITY (Includes Critical Infrastructure Protection)	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	1,046,920	1,046,920	-	0.00%	
Penalty Sanctions	3,325	3,325	-	0.00%	
Total ERO Funding	**$ 1,050,245**	**$ 1,050,245**	**$ -**	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	87	-	87		
Total Funding (A)	1,050,332	1,050,245	87	0.01%	
Expenses					
Personnel Expenses					
Salaries	380,862	500,945	(120,083)	-23.97%	SERC budgeted 3.75 FTE's in the Situation Awareness program during 2013. SERC finished 2013 with 3.12 FTEs, a difference of 0.63 FTEs, causing SERC to be under budget.
Payroll Taxes	20,980	30,057	(9,077)	-30.20%	As noted above in Salaries Expense, decrease in payroll taxes is due to not being fully staffed.
Employee Benefits	32,467	45,882	(13,415)	-29.24%	As noted above in Salaries Expense, there was less participation in benefits due to not being fully staffed.
Savings & Retirement	61,989	57,116	4,873	8.53%	
Total Personnel Expenses	496,298	634,000	(137,702)	-21.72%	
Meeting Expenses					
Meetings	3,225	16,575	(13,350)	-80.54%	A greater emphasis on the use of technology by hosting WebEx meetings has lowered meeting costs. Additionally, SERC is now hosting more meetings in the Charlotte office at a significantly reduced cost, further reducing expenses, causing the under run.
Travel	55,399	43,172	12,227	28.32%	In an effort to train and develop new staff, SERC sent additional employees to meetings, causing an overrun.
Conference Calls	-	-	-		
Total Meeting Expenses	58,624	59,747	(1,123)	-1.88%	
Operating Expenses					
Consultants & Contracts	-		-		
Rent & Improvements	-	-	-		
Office Costs	2,316	260	2,056	790.77%	
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	2,316	260	2,056	790.77%	
Indirect Expenses	351,946	368,433	(16,487)	-4.47%	Expenses related to indirect programs have been allocated proportionately to the direct programs for 2013 based on the number of FTEs in those programs
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	909,184	1,062,440	(153,256)	-14.42%	
Change in Assets (A - B)	141,148	(12,195)	153,343	-1257.43%	
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	(20,260)	12,195	(32,455)	-266.13%	
Total Inc(Dec) in Fixed Assets (C)	(20,260)	12,195	(32,455)	-266.13%	
TOTAL BUDGET (B - C)	**929,444**	**1,050,245**	**(120,801)**	**-11.50%**	
Change in Working Capital (A-B+C)	**120,888**	**-**	**120,888**		
FTE's	**3.12**	**3.75**	**(0.63)**	**-16.80%**	

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013
Per Audit

MEMBER FORUMS	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	-	-	-		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	87	-	87		
Total Funding (A)	87	-	87		
Expenses					
Personnel Expenses					
Salaries	639,983	751,690	(111,707)	-14.86%	SERC budgeted 7.20 FTE's in the Committees and Members Forum program during 2013. SERC finished 2013 with 6.69 FTEs, a difference of 0.51 FTEs, causing SERC to be under budget.
Payroll Taxes	46,782	45,101	1,681	3.73%	
Employee Benefits	57,156	61,616	(4,460)	-7.24%	
Savings & Retirement	65,562	99,754	(34,192)	-34.28%	SERC budgeted based on historical employee contributions. The actual employee contribution for 2013 was lower than budgeted, causing the corresponding company match to be lower than budgeted.
Total Personnel Expenses	809,483	958,161	(148,678)	-15.52%	
Meeting Expenses					
Meetings	11,598	26,125	(14,527)	-55.61%	A greater emphasis on the use of technology by hosting WebEx meetings has lowered meeting costs.
Travel	28,345	34,849	(6,504)	-18.66%	SERC continues to emphasize the use of technology by hosting meetings using WebEx. Additionally, SERC is now hosting more meetings in the Charlotte office, which does not require staff to travel. By doing this, travel costs have decreased.
Conference Calls	-	-	-		
Total Meeting Expenses	39,943	60,974	(21,031)	-34.49%	
Operating Expenses					
Consultants & Contracts	2,756	-	2,756		
Rent & Improvements	-	-	-		
Office Costs	1,477	1,505	(28)	-1.86%	
Professional Services	-	-	-		
Miscellaneous	110	-	110		
Depreciation	-	-	-		
Total Operating Expenses	4,343	1,505	2,838	188.57%	
Indirect Expenses	(853,769)	(1,020,640)	166,871	-16.35%	Expenses related to indirect programs have been allocated proportionately to the direct programs for 2013 based on the number of FTEs in those programs
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	-	-	-		
Change in Assets (A - B)	87	-	87		
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B - C)	-	-	-		
Change in Working Capital (A-B+C)	87	-	87		
FTE's	4.39	4.93	(0.54)	-10.95%	

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013
Per Audit

GENERAL and ADMINISTRATIVE	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	(1,705,725)	(1,705,725)	-	0.00%	
Penalty Sanctions	-	-	-		
Total ERO Funding	**$ (1,705,725)**	**$ (1,705,725)**	**$ -**	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	61,329	-	61,329		SERC is working in a coordinated effort with the other regional entities on the preparation of the Regional Five Year Assessment. SERC is managing the contract with the consultant, subject to reimbursement from the other regional entities. This reimbursement is included in Miscellaneous Income, as an offset to the expense recorded in Contracts and Consultants.
Total Funding (A)	(1,644,396)	(1,705,725)	61,329	-3.60%	
Expenses					
Personnel Expenses					
Salaries	2,347,800	2,131,386	216,414	10.15%	While SERC is under budget by .56 FTEs in General & Administrative, the positions within G&A were filled at a higher than budgeted salary, causing an over run.
Payroll Taxes	138,803	127,883	10,920	8.54%	
Employee Benefits	189,130	164,124	25,006	15.24%	There was higher usage of SERC's medical benefits in 2013, causing an over run.
Savings & Retirement	262,591	298,875	(36,284)	-12.14%	SERC budgeted based on historical employee contributions. The actual employee contribution for 2013 was lower than budgeted, causing the corresponding company match to be lower than budgeted.
Total Personnel Expenses	2,938,324	2,722,268	216,056	7.94%	
Meeting Expenses					
Meetings	64,500	23,290	41,210	176.94%	The over run in meetings expenses is due to actual meeting spaces charged more than anticipated in the budget, as well as additional in-house meetings.
Travel	65,429	61,487	3,942	6.41%	
Conference Calls	49,760	60,000	(10,240)	-17.07%	SERC renegotiated lower rates for the telecommunications component of SERC's web based conferencing platform, causing the under run.
Total Meeting Expenses	179,689	144,777	34,912	24.11%	
Operating Expenses					
Consultants & Contracts	211,984	-	211,984		SERC engaged a management consulting firm to support SERC's corporate initiative for management training; a project manager and architecture firm to assist with the design, construction, and coordination of the relocation of SERC's offices in 2014. Both were unbudgeted, but deemed necessary. Additionally, in a coordinated effort with the other regional entities on the preparation of the Five Year Assessment, SERC managed the contract with the consultant, subject to reimbursement from the other regional entities. This was an unbudgeted project, causing an overrun. The offsetting revenue is recorded in Miscellaneous income, as noted above.
Rent & Improvements	403,731	405,407	(1,676)	-0.41%	
Office Costs	481,725	189,061	292,664	154.80%	The over run in office costs includes one time costs for the purchase of office furniture and equipment to furnish the new office space. Individually, all items were below SERC's capitalization policy and were therefore expensed.
Professional Services	37,366	20,000	17,366	86.83%	The variance is comprised of various unbudgeted items, including a property tax bill, and an increase in our general liability insurances.
Miscellaneous	1,038	-	1,038		
Depreciation	137,147	300,389	(163,242)	-54.34%	Due to the actual cost of the assets and the timing of when the assets were placed into service, depreciation expense and capital expenditures were lower than the budget, causing the under run.
Total Operating Expenses	1,272,991	914,857	358,134	39.15%	
Indirect Expenses	(4,391,004)	(3,781,902)	(609,102)	16.11%	Expenses related to indirect programs have been allocated proportionately to the direct programs for 2013 based on the number of FTEs in those programs
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	-	-	-		
Change in Assets (A - B)	(1,644,396)	(1,705,725)	61,329	-3.60%	
Fixed Assets					
Depreciation	(137,147)	(300,389)	163,242	-54.34%	Due to the actual cost of the assets and the timing of when the assets were placed into service, depreciation expense was lower than the budget, causing the under run.
Computer & Software CapEx	474,813	113,333	361,480	318.95%	Due to delays in 2012, several 2012 software projects were completed and capitalized throughout 2013, causing an over run.
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-		-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	(337,666)	187,056	(524,722)		
Allocation of Fixed Assets	337,666	(187,056)	524,722	-280.52%	
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B - C)	**-**	**-**	**-**		
Change in Working Capital (A-B+C)	**(1,644,396)**	**(1,705,725)**	**61,329**	-3.60%	
FTE's	**14.44**	**15.00**	**(0.56)**	**-3.73%**	

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013
Per Audit

LEGAL and REGULATORY	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	-	-	-		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	-	-	-		
Expenses					
Personnel Expenses					
Salaries	-	-	-		
Payroll Taxes	-	-	-		
Employee Benefits	-	-	-		
Savings & Retirement	-	-	-		
Total Personnel Expenses	-	-	-		
Meeting Expenses					
Meetings	-	-	-		
Travel	-	-	-		
Conference Calls	-	-	-		
Total Meeting Expenses	-	-	-		
Operating Expenses					
Consultants & Contracts	-	-	-		
Rent & Improvements	-	-	-		
Office Costs	1,215	1,768	(553)	-31.28%	
Professional Services	26,147	30,000	(3,853)	-12.84%	
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	27,362	31,768	(4,406)	-13.87%	
Indirect Expenses	(27,362)	(31,768)	4,406	-13.87%	Expenses related to indirect programs have been allocated proportionately to the direct programs for 2013 based on the number of FTEs in those programs
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	-	-	-		
Change in Assets (A - B)	-	-	-		
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B - C)	-	-	-		
Change in Working Capital (A-B+C)	-	-	-		
FTE's	-	-	-		

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013
Per Audit

INFORMATION TECHNOLOGY	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	-	-	-		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	-	-	-		
Expenses					
Personnel Expenses					
Salaries	-	-	-		
Payroll Taxes	-	-	-		
Employee Benefits	-	-	-		
Savings & Retirement	-	-	-		
Total Personnel Expenses	-	-	-		
Meeting Expenses					
Meetings	-	-	-		
Travel	-	-	-		
Conference Calls	-	-	-		
Total Meeting Expenses	-	-	-		
Operating Expenses					
Consultants & Contracts	424,779	632,780	(208,001)	-32.87%	Participation in the OATI schedule checkout tool was lower than planned in 2013, resulting in an under run from the budgeted cost. However, a change was made to the tool to accommodate the users' need for intra-hour scheduling. The net effect caused an overrun . Additionally, actual costs for hosting and maintaining SERC's servers are lower than budgeted. Finally, SERC did not incur significant costs related to various IT projects, causing an under run.
Rent & Improvements	-	-	-		
Office Costs	107,609	144,916	(37,307)	-25.74%	The budget included funds the purchase of computers and equipment for existing staff replacements and for the budgeted new positions. The majority of these items were purchased in 2012, causing an under run in 2013. Additionally, SERC negotiated better rates on the telephone and internet service, causing an under run.
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	532,388	777,696	(245,308)	-31.54%	
Indirect Expenses	(532,388)	(777,696)	245,308	-31.54%	Expenses related to indirect programs have been allocated proportionately to the direct programs for 2013 based on the number of FTEs in those programs
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	-	-	-		
Change in Assets (A - B)	-	-	-		
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B - C)	-	-	-		
Change in Working Capital (A-B+C)	-	-	-		
FTE's	-	-	-		

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013
Per Audit

HUMAN RESOURCES	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	-	-	-		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	-	-	-		
Expenses					
Personnel Expenses					
Salaries	-	-	-		
Payroll Taxes	-	-	-		
Employee Benefits	-	-	-		
Savings & Retirement	-	-	-		
Total Personnel Expenses	-	-	-		
Meeting Expenses					
Meetings	-	-	-		
Travel	-	-	-		
Conference Calls	-	-	-		
Total Meeting Expenses	-	-	-		
Operating Expenses					
Consultants & Contracts	10,000	-	10,000		SERC engaged a consultant to offer a climate survey to employees. This was an unbudgeted expense, but deemed necessary.
Rent & Improvements	-	-	-		
Office Costs	699	360	339	94.17%	
Professional Services	6,975	10,000	(3,025)	-30.25%	
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	17,674	10,360	7,314	70.60%	
Indirect Expenses	(17,674)	(10,360)	(7,314)	70.60%	Expenses related to indirect programs have been allocated proportionately to the direct programs for 2013 based on the number of FTEs in those programs
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	-	-	-		
Change in Assets (A - B)	-	-	-		
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B - C)	-	-	-		
Change in Working Capital (A-B+C)	-	-	-		
FTE's	-	-	-		

SERC Reliability Corporation
Statement of Activities
From 1/1/2013 through 12/31/2013
Per Audit

ACCOUNTING and FINANCE	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
Funding					
ERO Funding					
Assessments	-	-	-		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	1,271	10,000	(8,729)	-87.29%	
Miscellaneous	-	-	-		
Total Funding (A)	1,271	10,000	(8,729)	-87.29%	
Expenses					
Personnel Expenses					
Salaries	-	-	-		
Payroll Taxes	-	-	-		
Employee Benefits	-	-	-		
Savings & Retirement	-	-	-		
Total Personnel Expenses	-	-	-		
Meeting Expenses					
Meetings	-	-	-		
Travel	-	-	-		
Conference Calls	-	-	-		
Total Meeting Expenses	-	-	-		
Operating Expenses					
Consultants & Contracts	1,600	-	1,600		
Rent & Improvements	-	-	-		
Office Costs	12,259	8,000	4,259	53.24%	
Professional Services	28,704	30,900	(2,196)	-7.11%	
Miscellaneous	1,000	-	1,000		
Depreciation	-	-	-		
Total Operating Expenses	43,563	38,900	4,663	11.99%	
Indirect Expenses	(43,563)	(28,900)	(14,663)	50.74%	Expenses related to indirect programs have been allocated proportionately to the direct programs for 2013 based on the number of FTEs in those programs
Other Non-Operating Expenses	-	-	-		
Total Expenses (B)	-	10,000	(10,000)	-100.00%	
Change in Assets (A - B)	1,271	-	1,271		
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	-	-	-		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	-	-	-		
TOTAL BUDGET (B - C)	**-**	**10,000**	**(10,000)**	**-100.00%**	
Change in Working Capital (A-B+C)	**1,271**	**-**	**1,271**		
FTE's	**-**	**-**	**-**		

SERC RELIABILITY CORPORATION

FINANCIAL STATEMENTS AND SUPPLEMENTAL SCHEDULES

As of and for the Year Ended December 31, 2013 and 2012

And Report of Independent Auditor

Cherry Bekaert LLP
CPAs & Advisors

SERC RELIABILITY CORPORATION

TABLE OF CONTENTS

REPORT OF INDEPENDENT AUDITOR 1-2

FINANCIAL STATEMENTS

Statements of Financial Position 3
Statements of Activities 4
Statements of Cash Flows 5
Notes to the Financial Statements 6-9

SUPPLEMENTAL SCHEDULES

Statutory Financial Statements 10-11
Statutory Financial Statements by Function 12-13

Cherry Bekaert LLP
CPAs & Advisors

Report of Independent Auditor

To the Board of Directors
SERC Reliability Corporation
Charlotte, North Carolina

Report on the Financial Statements

We have audited the accompanying financial statements of SERC Reliability Corporation (the "Corporation"), which comprise the statements of financial position as of December 31, 2013 and 2012, and the related statements of activities and cash flows for the years then ended, and the related notes to the financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of SERC Reliability Corporation as of December 31, 2013 and 2012, and the changes in net assets and its cash flows for the years then ended in conformity with accounting principles generally accepted in the United States of America.

Supplemental Schedules

Our audits were conducted for the purpose of forming an opinion on the financial statements as a whole. The supplemental schedules on pages 10 through 13 are presented for purposes of additional analysis and are not a required part of the financial statements. Such information is the responsibility of management and was derived from and relates directly to the underlying accounting and other records used to prepare the financial statements. The information has been subjected to the auditing procedures applied in the audits of the financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the financial statements or to the financial statements themselves, and other additional procedures in accordance with auditing standards generally accepted in the United States of America. In our opinion, the information is fairly stated in all material respects in relation to the financial statements as a whole.

Cherry Bekaert LLP

Charlotte, North Carolina
April 11, 2014

SERC RELIABILITY CORPORATION

STATEMENTS OF FINANCIAL POSITION

DECEMBER 31, 2013 AND 2012

	2013	2012
ASSETS		
Current assets		
Cash and cash equivalents	$ 7,685,935	$ 7,192,908
Accounts receivable	68,691	18,487
Prepaid expenses and other current assets	172,213	127,403
Total current assets	7,926,839	7,338,798
Property and equipment, net	662,478	324,812
Total Assets	$ 8,589,317	$ 7,663,610
LIABILITIES AND NET ASSETS		
Current liabilities		
Accounts payable	$ 452,530	$ 465,519
Accrued salaries and related benefits	2,407,098	1,981,820
Deferred revenue	2,318,183	556,606
Total current liabilities	5,177,811	3,003,945
Net assets		
Unrestricted and undesignated	2,215,987	3,473,073
Unrestricted and designated operating reserve	1,195,519	1,186,592
Total Net Assets	3,411,506	4,659,665
Total Liabilities and Net Assets	$ 8,589,317	$ 7,663,610

The accompanying notes to the financial statements are an integral part of these statements.

SERC RELIABILITY CORPORATION

STATEMENTS OF ACTIVITIES

YEARS ENDED DECEMBER 31, 2013 AND 2012

	2013	2012
Funding		
Member assessments	$ 13,829,878	$ 14,845,275
Penalty sanctions	51,000	434,500
Workshops	173,997	226,574
Interest	1,271	7,665
Miscellaneous	238,996	113,822
Total funding	14,295,142	15,627,836
Expenses		
Personnel expenses:		
Salaries	9,176,085	8,003,504
Payroll taxes	632,913	561,010
Employee benefits	896,790	665,615
Savings and retirement	1,169,319	1,060,293
Total personnel expenses	11,875,107	10,290,422
Meeting expenses:		
Meetings	276,839	341,082
Travel	646,398	581,263
Conference calls	49,760	42,622
Total meeting expenses	972,997	964,967
Operating expenses:		
Contracts and consultants	1,410,698	899,931
Rent and improvements	403,731	404,835
Office costs	633,768	402,242
Professional services	107,705	143,214
Depreciation	137,147	129,449
Miscellaneous	2,148	8,170
Total operating expenses	2,695,197	1,987,841
Total expenses	15,543,301	13,243,230
Change in net assets	(1,248,159)	2,384,606
Net assets		
Beginning of year	4,659,665	2,275,059
End of year	$ 3,411,506	$ 4,659,665

The accompanying notes to the financial statements are an integral part of these statements.

SERC RELIABILITY CORPORATION
STATEMENTS OF CASH FLOWS

YEARS ENDED DECEMBER 31, 2013 AND 2012

	2013	2012
Cash flows from operating activities		
Change in net assets	$ (1,248,159)	$ 2,384,606
Adjustments to reconcile change in net assets to net cash provided by operating activities:		
Depreciation	137,147	129,449
Changes in operating assets and liabilities:		
Accounts receivable	(50,204)	29,475
Prepaid expenses and other current assets	(44,810)	(4,102)
Accounts payable	(12,989)	253,723
Accrued salaries and related benefits	425,278	618,500
Deferred revenue	1,761,577	80,279
Net cash provided by operating activities	967,840	3,491,930
Cash flows from investing activities		
Additions to property and equipment	(474,813)	(146,827)
Net increase in cash and cash equivalents	493,027	3,345,103
Cash and cash equivalents		
Beginning of year	7,192,908	3,847,805
End of year	$ 7,685,935	$ 7,192,908

The accompanying notes to the financial statements are an integral part of these statements.

Note 1—Organization and nature of operations

SERC Reliability Corporation (the "Corporation") is a non-profit corporation which qualifies as a Regional Reliability Organization under the Energy Policy Act of 2005. The Corporation's mission is to promote the reliability of the electricity supply for the southeastern United States. The activities of the Corporation are directed by its Board of Directors. The Corporation's members are electricity suppliers, brokers and consumers from various ownership segments of the electricity supply industry, investor-owned utilities rural electric cooperatives, municipal utilities, independent power producers, power marketers and customers. These entities account for virtually all the electricity supplied in the southeastern United States.

Note 2—Summary of significant accounting policies

Accounting Principles - The financial statements of the Corporation have been prepared on the accrual basis of accounting in accordance with accounting principles generally accepted in the United States of America ("GAAP"). The Corporation is required to report information regarding its financial position and activities according to three classes of net assets - unrestricted net assets, temporarily restricted net assets and permanently restricted net assets. The Corporation had only unrestricted net assets as of December 31, 2013 and 2012, including unrestricted net assets that have been designated by the Board of Directors as an operating reserve.

Management Estimates - The preparation of financial statements in conformity with GAAP requires management to make estimates, including estimates relating to assumptions that affect the reported amounts of assets and liabilities and disclosure of contingent assets and liabilities at the date of financial statements and the reported amounts of revenues and expenses during the reporting period. Actual results could differ from these estimates.

Cash and Cash Equivalents - The Corporation considers all cash investments with an original maturity of three months or less to be cash equivalents.

Accounts Receivable - Accounts receivable arise primarily from amounts billed to members. Management's determination of the need for an allowance for doubtful accounts is based on evaluation of the accounts receivable, past experience, current economic conditions and other risks inherent in the accounts receivable portfolio. Any amounts considered to be uncollectible are written off at the time of such determination. At December 31, 2013 and 2012, management has determined that an allowance for doubtful accounts is not necessary.

Property and Equipment - Property and equipment are stated at cost. Depreciation is computed using the straight-line method over the estimated economic useful lives of the assets ranging from 5-7 years for leasehold improvements and 3 years for computer equipment and software. The costs of major improvements are capitalized, while the costs of maintenance and repairs, which do not improve or extend the lives of the respective assets, are expensed currently. The cost and accumulated depreciation of property and equipment are eliminated from the accounts upon disposal, and any resulting gain or loss is included in the change in net assets of the Corporation. Long-lived assets held and used by the Corporation are reviewed for impairment whenever changes in circumstances indicate the carrying value of an asset may not be recoverable.

Deferred Revenue - Deferred revenue represents amounts billed or collected from members in advance of the periods in which such amounts are earned.

Note 2—Summary of significant accounting policies (continued)

Revenue Recognition - All income is recognized in the period when earned. The Corporation receives a significant portion of its funding directly from the North American Electric Reliability Corporation ("NERC") based on the budget submitted by the Corporation and approved by NERC and the Federal Energy Regulatory Commission ("FERC"). The revenue is received in four equal quarterly installments received at the beginning of each quarter. Based on past history with NERC, the Corporation believes that its revenue risk exposure is limited.

Income Taxes - The Corporation is exempt from federal and state income taxes under Section 501(c)(6) of the Internal Revenue Code ("IRC") and the applicable state statutes. Management believes that the Corporation continues to satisfy the requirements of a tax exempt organization and is not subject to tax. Accordingly, no provision for income taxes has been recorded in the accompanying financial statements.

Management has evaluated the effect of the Financial Accounting Standards Board ("FASB") guidance on accounting for uncertainty in income taxes. The guidance clarifies the accounting for uncertainty in income taxes recognized in an entity's financial statements by prescribing a recognition threshold and measurement attribute for the financial statement recognition and measurement of a tax position taken or expected to be taken in a tax return. The Corporation's policy is to record a liability for any tax position taken that is beneficial to the Corporation, including any related interest and penalties, when it is more likely than not the position taken by management with respect to a transaction or class of transactions will be overturned by a taxing authority upon examination. Management believes there are no such positions at December 31, 2013 or 2012 and, accordingly, no liability has been accrued. The Corporation is no longer subject to tax examinations for years prior to 2010.

Note 3—Property and equipment

Property and equipment includes the following at December 31:

	2013	2012
Leasehold improvements	$ 53,099	$ 53,099
Computer equipment	202,048	177,411
Software	918,535	468,360
	1,173,682	698,870
Less: Accumulated depreciation	(511,204)	(374,058)
Property and equipment, net	$ 662,478	$ 324,812

Depreciation expense was $137,147 and $129,449 for the years ended December 2013 and 2012, respectively.

Note 4—Leases

The Corporation leases office facilities under three operating leases which continue through January 2015. The leases call for monthly payments ranging from $32,000 to $35,000.

Subsequent to year end, the Corporation entered into a new operating lease for office space which commences on April 1, 2014 and continues through March 31, 2025. The lease will provide free rent for the first 10 months of the lease period and annual rent payments ranging from $460,000 to $612,000 thereafter. In connection with the future office space, the Corporation entered into a construction agreement providing for an upfit allowance, whereby the Corporation will be reimbursed for upfit costs up to $814,710.

Note 4—Leases (continued)

Total rent expense for the years ended December 31, 2013 and 2012, was $403,731 and $404,835, respectively.

Future minimum payments on all operating leases are as follows:

Year ending December 31,		
2014	$	410,667
2015		495,442
2016		512,767
2017		524,304
2018		536,101
Thereafter		3,530,777
Total	$	6,010,058

Note 5—Line of credit

The Corporation has a $1,000,000 bank line of credit at an interest rate of prime plus 0.9%, limited to a 5.0% floor, (5.0% at December 31, 2013) for which all outstanding borrowings shall be payable in full at maturity on August 30, 2014. The line is secured by the assets of the Corporation. The line of credit had no outstanding balance at December 31, 2013 and 2012.

Note 6—Benefit plans

401(k) plan - The Corporation sponsors a 401(k) retirement plan covering all eligible employees, as defined. The Corporation makes an annual contribution to the plan equal to 3% of each eligible employee's compensation. In addition, the plan provides that the Corporation may make additional discretionary matching and profit-sharing contributions. During the years ended December 31, 2013 and 2012, contribution expense related to the plan totaled $1,131,588 and $1,029,192, respectively.

Deferred compensation plan - The Corporation established a deferred compensation plan in accordance with Internal Revenue Code Section 457 for certain employees, as defined. The plan provides that eligible employees may make elective salary reduction contributions in accordance with limitations established by the Internal Revenue Code. In addition, the Corporation may make discretionary contributions as provided in the plan. During the years ended December 31, 2013 and 2012, contribution expense related to the plan totaled $21,036 and $21,876, respectively. The asset and liability for deferred compensation of $82,204 and $61,063 at December 31, 2013 and 2012, respectively, is included in prepaid expenses and other current assets and accrued salaries and related benefits in the accompanying statements of financial position.

Note 7—Concentrations of credit risk and uncertainties

The Corporation places its cash and cash equivalents on deposit with a North Carolina financial institution. The Federal Deposit Insurance Company ("FDIC") covers $250,000 for substantially all depository accounts. The Corporation from time to time may have balances in excess of the FDIC insured limits. The Corporation had funds in banks in excess of the federally insured limited of $7,343,667 and $6,960,203 at December 31, 2013 and 2012, respectively.

Note 8—Functional expenses

The following is an allocation of expenses by functional category for the years ended December 31:

	2013	2012
Program expenses:		
Reliability standards	$ 291,074	$ 356,196
Compliance enforcement	6,928,256	5,643,977
Reliability assessment	1,265,510	957,662
Training and education	635,463	643,381
Situtation awareness	557,238	999,826
	9,677,541	8,601,042
Committee and member forums	853,769	544,597
General and administrative expenses:		
General and administrative	4,391,004	3,480,171
Legal and regulatory	27,362	49,805
Information technology	532,388	526,603
Human resources	17,674	50
Accounting and finance	43,563	40,962
	5,011,991	4,097,591
Total	$ 15,543,301	$ 13,243,230

Note 9—Subsequent events

Management has evaluated subsequent events through April 11, 2014, the date the financial statements were issued.

ACCOMPANYING INFORMATION

SERC RELIABILITY CORPORATION
STATUTORY FINANCIAL STATEMENTS

YEAR ENDED DECEMBER 31, 2013

	2013 YTD Actual	2013 YTD Budget	2013 YTD Variance
Funding			
Member assessments	$ 13,829,878	$ 13,829,878	$ -
Penalty sanctions	51,000	51,000	-
Workshops	173,997	246,000	(72,003)
Interest	1,271	10,000	(8,729)
Miscellaneous	238,996	65,000	173,996
Total funding	14,295,142	14,201,878	93,264
Expenses			
Personnel expenses:			
Salaries	9,176,085	9,925,148	(749,063)
Payroll taxes	632,913	595,509	37,404
Employee benefits	896,790	916,100	(19,310)
Savings and retirement	1,169,319	1,353,524	(184,205)
Total personnel expenses	11,875,107	12,790,281	(915,174)
Meeting expenses:			
Meetings	276,839	309,160	(32,321)
Travel	646,398	595,023	51,375
Conference calls	49,760	60,000	(10,240)
Total meeting expenses	972,997	964,183	8,814
Operating expenses:			
Contracts and consultants	1,410,698	1,166,947	243,751
Rent and improvements	403,731	405,407	(1,676)
Office costs	633,768	361,552	272,216
Professional services	107,705	105,900	1,805
Depreciation	137,147	300,389	(163,242)
Miscellaneous	2,148	-	2,148
Total operating expenses	2,695,197	2,340,195	355,002
Total expenses	15,543,301	16,094,659	(551,358)
Change in net assets	$ (1,248,159)	$ (1,892,781)	$ 644,622

SERC RELIABILITY CORPORATION
STATUTORY FINANCIAL STATEMENTS

YEAR ENDED DECEMBER 31, 2012

	2012 YTD Actual	2012 YTD Budget	2012 YTD Variance
Funding			
Member assessments	$ 14,845,275	$ 14,845,275	$ -
Penalty sanctions	434,500	434,500	-
Workshops	226,574	264,670	(38,096)
Interest	7,665	10,000	(2,335)
Miscellaneous	113,822	40,000	73,822
Total funding	15,627,836	15,594,445	33,391
Expenses			
Personnel expenses:			
Salaries	8,003,504	8,908,407	(904,903)
Payroll taxes	561,010	801,758	(240,748)
Employee benefits	665,615	895,883	(230,268)
Savings and retirement	1,060,293	1,207,456	(147,163)
Total personnel expenses	10,290,422	11,813,504	(1,523,082)
Meeting expenses:			
Meetings	341,082	402,078	(60,996)
Travel	581,263	616,591	(35,328)
Conference calls	42,622	96,000	(53,378)
Total meeting expenses	964,967	1,114,669	(149,702)
Operating expenses:			
Contracts and consultants	899,931	1,159,275	(259,344)
Rent and improvements	404,835	444,722	(39,887)
Office costs	402,242	682,875	(280,633)
Professional services	143,214	89,400	53,814
Depreciation	129,449	232,952	(103,503)
Miscellaneous	8,170	-	8,170
Total operating expenses	1,987,841	2,609,224	(621,383)
Total expenses	13,243,230	15,537,397	(2,294,167)
Change in net assets	$ 2,384,606	$ 57,048	$ 2,327,558

SERC RELIABILITY CORPORATION

STATUTORY FINANCIAL STATEMENTS BY FUNCTION

YEAR ENDED DECEMBER 31, 2013

	300 RELIAB STD DEV	400 COMP ENFORCE/ ORG REG & CERT	800 RELIAB ASSES	900 TRAINING & EDUC	1000 SIT AWARE	1100 COMMITTEE & MBR FORUMS	2000 GENERAL ADMIN	2200 LEGAL & REGULATORY	2300 IT	2400 HUMAN RESOURCES	2500 ACCOUNTING & FINANCE	2013 YTD Actual	2013 YTD Budget	2013 YTD Variance
Funding														
Member assessments	$ 698,880	$ 11,150,647	$ 1,937,756	$ 701,400	$ 1,046,920	-	$ (1,705,725)	-	-	-	-	$13,829,878	$ 13,829,878	$ -
Penalty sanctions	2,358	36,796	6,384	2,137	3,325	-	-	-	-	-	-	51,000	51,000	-
Workshops	-	-	-	173,997	-	-	-	-	-	-	-	173,997	246,000	(72,003)
Interest	-	-	-	-	-	-	-	-	-	-	1,271	1,271	10,000	(8,729)
Miscellaneous	87	177,319	-	87	87	87	61,329	-	-	-	-	238,996	65,000	173,996
Total funding	701,325	11,364,762	1,944,140	877,621	1,050,332	87	(1,644,396)	-	-	-	1,271	14,295,142	14,201,878	93,264
Expenses														
Personnel expenses:														
Salaries	226,234	4,556,726	723,751	300,729	380,862	639,983	2,347,800	-	-	-	-	9,176,085	9,925,148	(749,063)
Payroll taxes	17,470	331,116	56,925	20,837	20,980	46,782	138,803	-	-	-	-	632,913	595,509	37,404
Employee benefits	26,540	470,656	93,610	27,231	32,467	57,156	189,130	-	-	-	-	896,790	916,100	(19,310)
Savings and retirement	13,925	636,236	93,427	35,589	61,989	65,562	262,591	-	-	-	-	1,169,319	1,353,524	(184,205)
Total personnel expenses	284,169	5,994,734	967,713	384,386	496,298	809,483	2,938,324	-	-	-	-	11,875,107	12,790,281	(915,174)
Meeting expenses:														
Meetings	302	26,743	28,428	142,043	3,225	11,598	64,500	-	-	-	-	276,839	309,160	(32,321)
Travel	5,804	407,579	69,856	13,986	55,399	28,345	65,429	-	-	-	-	646,398	595,023	51,375
Conference calls	-	-	-	-	-	-	49,760	-	-	-	-	49,760	60,000	(10,240)
Total meeting expenses	6,106	434,322	98,284	156,029	58,624	39,943	179,689	-	-	-	-	972,997	964,183	8,814
Operating expenses:														
Contracts and consultants	-	474,637	194,865	90,077	-	2,756	211,984	-	424,779	10,000	1,600	1,410,698	1,166,947	243,751
Rent and improvements	-	-	-	-	-	-	403,731	-	-	-	-	403,731	405,407	(1,676)
Office costs	799	16,050	4,648	4,971	2,316	1,477	481,725	1,215	107,609	699	12,259	633,768	361,552	272,216
Professional services	-	8,513	-	-	-	-	37,366	26,147	-	6,975	28,704	107,705	105,900	1,805
Depreciation	-	-	-	-	-	-	137,147	-	-	-	-	137,147	300,389	(163,242)
Miscellaneous	-	-	-	-	-	110	1,038	-	-	-	1,000	2,148	-	2,148
Total operating expenses	799	499,200	199,513	95,048	2,316	4,343	1,272,991	27,362	532,388	17,674	43,563	2,695,197	2,340,195	355,002
Total expenses	291,074	6,928,256	1,265,510	635,463	557,238	853,769	4,391,004	27,362	532,388	17,674	43,563	15,543,301	16,094,659	(551,358)
Change in net assets	$ 410,251	$ 4,436,506	$ 678,630	$ 242,158	$ 493,094	$ (853,682)	$ (6,035,400)	$ (27,362)	$ (532,388)	$ (17,674)	$ (42,292)	$ (1,248,159)	$ (1,892,781)	$ 644,622

SERC RELIABILITY CORPORATION

STATUTORY FINANCIAL STATEMENTS BY FUNCTION

YEAR ENDED DECEMBER 31, 2012

	300 RELIAB STD DEV	400 COMP ENFORCE/ ORG REG & CERT	800 RELIAB ASSES	900 TRAINING & EDUC	1000 SIT AWARE	1100 COMMITTEE & MBR FORUMS	2000 GENERAL ADMIN	2200 LEGAL & REGULATORY	2300 IT	2400 HUMAN RESOURCES	2500 ACCOUNTING & FINANCE	2012 YTD Actual	2012 YTD Budget	2012 YTD Variance
Funding														
Member assessments	$ 510,346	$ 10,639,545	$ 1,581,890	$ 570,332	$ 1,543,162	$ -	$ -	$ -	$ -	$ -	$ -	$ 14,845,275	$ 14,845,275	$ -
Penalty sanctions	14,094	318,124	45,906	14,094	42,282	-	-	-	-	-	-	434,500	434,500	-
Workshops	-	-	-	226,574	-	-	-	-	-	-	-	226,574	264,670	(38,096)
Interest	-	-	-	-	-	-	-	-	-	-	7,665	7,665	10,000	(2,335)
Miscellaneous	-	110,604	-	-	-	-	3,218	-	-	-	-	113,822	40,000	73,822
Total funding	524,440	11,068,273	1,627,796	811,000	1,585,444	-	3,218	-	-	-	7,665	15,627,836	15,594,445	33,391
Expenses														
Personnel expenses:														
Salaries	259,658	3,972,211	514,647	249,185	720,321	370,535	1,916,947	-	-	-	-	8,003,504	8,908,407	(904,903)
Payroll taxes	16,079	298,761	42,766	15,936	52,689	24,029	110,750	-	-	-	-	561,010	801,758	(240,748)
Employee benefits	20,639	197,370	108,875	22,991	77,453	23,290	214,997	-	-	-	-	665,615	895,883	(230,268)
Savings and retirement	49,784	612,132	96,200	47,117	89,506	82,545	83,009	-	-	-	-	1,060,293	1,207,456	(147,163)
Total personnel expenses	346,160	5,080,474	762,488	335,229	939,969	500,399	2,325,703	-	-	-	-	10,290,422	11,813,504	(1,523,082)
Meeting expenses:														
Meetings	492	22,384	17,728	224,556	236	7,390	68,296	-	-	-	-	341,082	402,078	(60,996)
Travel	8,777	399,418	23,111	9,341	48,673	29,150	62,793	-	-	-	-	581,263	616,591	(35,328)
Conference calls	-	-	-	-	-	-	42,622	-	-	-	-	42,622	96,000	(53,378)
Total meeting expenses	9,269	421,802	40,839	233,897	48,909	36,540	173,711	-	-	-	-	964,967	1,114,669	(149,702)
Operating expenses:														
Contracts and consultants	-	106,795	149,994	65,338	10,189	6,326	105,521	-	454,722	-	1,046	899,931	1,159,275	(259,344)
Rent and improvements	-	-	-	-	-	-	404,835	-	-	-	-	404,835	444,722	(39,887)
Office costs	405	11,845	3,262	7,602	258	1,223	295,184	125	71,816	-	10,522	402,242	682,875	(280,633)
Professional services	140	22,421	220	609	109	109	40,532	49,680	-	-	29,394	143,214	89,400	53,814
Depreciation	-	-	-	-	-	-	129,449	-	-	-	-	129,449	232,952	(103,503)
Miscellaneous	222	640	859	706	392	-	5,236	-	65	50	-	8,170	-	8,170
Total operating expenses	767	141,701	154,335	74,255	10,948	7,658	980,757	49,805	526,603	50	40,962	1,987,841	2,609,224	(621,383)
Total expenses	356,196	5,643,977	957,662	643,381	999,826	544,597	3,480,171	49,805	526,603	50	40,962	13,243,230	15,537,397	(2,294,167)
Change in net assets	$ 168,244	$ 5,424,296	$ 670,134	$ 167,619	$ 585,618	$ (544,597)	$ (3,476,953)	$ (49,805)	$ (526,603)	$ (50)	$ (33,297)	$ 2,384,606	$ 57,048	$ 2,327,558

ATTACHMENT 7

2013 ACTUAL COST-TO-BUDGET COMPARISON

FOR

SOUTHWEST POWER POOL REGIONAL ENTITY

AND

2013 AUDITED FINANCIAL REPORT

FOR

SOUTHWEST POWER POOL, INC.

SPP Southwest Power Pool
Regional Entity

Deborah K. Currie
Manager of Regulatory Interface and Process Improvement

Southwest Power Pool Regional Entity
201 Worthen Dr.
Little Rock, AR 72223
P 501.688.8228
F 501.482.2025

May 1, 2014

Via Electronic Mail

Michael Walker, Chief Financial Officer
Susan Turpen, Controller
North American Electric Reliability Corporation
3343 Peachtree Road, NE
4th Floor East Tower – Suite 400
Atlanta, GA 30326

Subject: Southwest Power Pool Regional Entity 2013 Actual Cost-to-Budget Comparison

Dear Mr. Walker and Ms. Turpen,

Attached is the Southwest Power Pool, Inc.'s (SPP, Inc.) submission of the SPP Regional Entity's (SPP RE) 2013 Actual Cost-to-Budget Comparison (2013 True Up Filing). For 2013, the SPP RE received approximately $9.5 million in statutory funds and incurred approximately $9.7 million in statutory expense (compared to $11.5 million budget).

The $2.8 thousand funding variance results from interest earned on the cash balance. The SPP RE performs only statutory activities, and therefore no statutory funding was used for non-statutory activities. The net impact on SPP RE's cash position for the year was a $153 thousand negative variance (compared to the budgeted $1.9 million negative variance).

The significant expense variances at the aggregate statutory level are explained below, while the explanations for the expense variances by statutory program area are provided in Attachment 1.

Aggregate Expense Variances

- **Personnel Expenses** (Actual - $4,087K or 16% below budget) – Personnel expenses were less than budget primarily due to four positions (Director of Compliance and Events, two Lead Engineers and a CIP Compliance Specialist) being unfilled as of December 31, 2013. There was also less than expected activity required by shared staff in the Reliability Standards program area due to the completion of the SPP UFLS regional standard.[1]

- **Travel and Meeting Expenses** (Actual - $447K or 24% under budget) –Travel expenses were less than expected primarily due to the unfilled budgeted staff positions.

[1] NERC filed a petition to FERC for approval of SPP's UFLS Regional Standard (PRC-006-01) on April 23, 2013. SPP RE's Board of Trustee's approved the recall of PRC-006-01 on August 8, 2013 and NERC filed a petition with FERC to withdraw the standard on December 11, 2013. By operation of law, the standard was withdrawn as of December 27, 2013.

- **Other Operating Expenses** (Actual - $961K or 44% under budget) – Other operating expenses trailed budget primarily due to the delayed implementation of the BES exception process.

- **SPP, Inc. Indirect Expense** (Actual - $4,187K or 4% under budget) – SPP, Inc. Indirect Expenses were less than budget due to actual FTEs being lower than budgeted and a slight decrease in the actual 2013 Indirect Expenses. Indirect Expenses are discussed in greater detail in the discussion that follows.

- **Total Expenses** (Actual $9.7 million or 16% under budget) – Although SPP RE ended the year under budget, SPP RE completed its intended activities for 2013. Although SPP RE is under budget, SPP RE has completed its required activities principally as a result of the increased experience of the RE direct staff, a higher level of Registered Entity compliance, particularly in the Operations and Planning area, resulting in a declining number of incoming violations, and enhanced efficiencies in internal SPP RE processes.

  Specifically, SPP RE performed 42 audits, performed 3 spot checks, processed 271 technical feasibility exceptions, identified 189 possible violations, processed 175 violations, reviewed 180 mitigation plans, and examined 22 reportable events. In addition, SPP RE conducted various outreach activities, participated in the facility ratings alert program, and published winter, summer, and long-term reliability assessments.

SPP, Inc. Shared Staff and Indirect Support Staff

The SPP governing documents, approved by NERC and FERC, allow for the use of SPP, Inc. staff not directly assigned to the SPP RE in the performance or support of some of the responsibilities that are performed by the SPP RE. There are two groups of SPP, Inc. staff that support the SPP RE. First, there is a group that performs some of the primary duties delegated to the SPP RE referred to as "shared staff." Shared staff consists of a portion of the SPP RTO engineering staff that performs the technical studies that form the basis for the SPP Regional Assessments published by NERC. Second, there is another group that supplies administrative services to the SPP RE such as accounting, computer support, human resources support, building services support, etc. referred to as "indirect support staff." In general, indirect support staff does not directly charge time and expenses to the SPP RE but are billed through an administrative charge referred to as "SPP, Inc. Indirect Overhead Expense Rate." Neither group participates in compliance or enforcement decisions of the SPP RE.

Shared staff members charge time and expenses directly to the SPP RE accounts and their hours are included in the official total full time equivalent headcount of the SPP RE for the purposes of reporting to NERC and FERC. Shared staff members record specific hours worked in the performance or support of the SPP RE's statutory functions in SPP, Inc's time tracking system. These hours are posted by the shared staff members and reviewed and approved by their specific manager or supervisor. The SPP RE Manager of Finance and Process Improvement as well as the SPP RE General Manager review the hours posted by the shared staff members. This procedure results in actual hours spent by shared staff on SPP RE statutory functions being charged directly to the particular SPP RE direct function at the shared staff member's compensation rate. These direct charges are included in the SPP RE's Business Plan and

Budget. For 2013, shared staff charged 4,739 hours, or 2.52 FTEs based on SPP's standard assumption that total number of hours in a year is 1,880, to the SPP RE. 2013 budgeted shared staff FTEs were 4.0.

With respect to the costs of indirect support staff (SPP, Inc. Indirect Expenses), these costs are assessed to the SPP RE based on a fixed rate per hour per FTE. The fixed rate is calculated by dividing the total costs for SPP, Inc. support services by the total hours worked by non-overhead personnel. The fixed rate is then multiplied by the hours charged by the shared staff and SPP RE direct staff to determine the total amount of SPP, Inc. Indirect Expenses that are assessed to the SPP RE. The SPP, Inc. Indirect Expenses assessed to the SPP RE are included in the SPP RE's Business Plan and Budget. The SPP, Inc. support costs included in the calculations are reviewed in detail to help ensure that SPP RTO specific costs are excluded from the calculation.

Due to the timing of the budget schedule, the estimated overhead rate used to develop the 2013 budget was the actual Indirect Overhead Rate for 2011, which was $67.35/hour. The actual 2013 Indirect Overhead Rate was $74.26/hour. The development of the $67.35/hour rate that was used in the development of the 2013 budget and the $74.26/hour rate embedded in the actual 2013 costs are shown in Attachments 2 and 3, respectively.

If you have any questions related to the submitted materials please feel free to call me at 501.688.8228 or email me at dcurrie.re@spp.org.

Sincerely,

Deborah K. Currie

Southwest Power Pool
Regional Entity
Statement of Activities
From 1/1/2013 through 12/31/2013

Total Statutory	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)
Funding			
ERO Funding			
Assessments	8,530,054	8,530,054	-
Penalty Sanctions	995,020	995,020	-
Total ERO Funding	**$ 9,525,074**	**$ 9,525,074**	**$ -**
Federal Grants	-	-	-
Membership Fees	-	-	-
Testing	-	-	-
Services & Software	-	-	-
Workshop Fees	-	-	-
Interest	2,818	-	2,818
Miscellaneous	-	-	-
Total Funding (A)	**$ 9,527,892**	**$ 9,525,074**	**$ 2,818**
Expenses			
Personnel Expenses			
Salaries	3,425,528	4,072,621	(647,093)
Payroll Taxes	229,225	311,555	(82,330)
Employee Benefits	293,743	312,164	(18,421)
Savings & Retirement	138,143	162,905	(24,762)
Total Personnel Expenses	**$ 4,086,639**	**$ 4,859,245**	**$ (772,606)**
Meeting Expenses			
Meetings	81,602	86,500	(4,898)
Travel	365,676	499,000	(133,324)
Conference Calls	-	-	-
Total Meeting Expenses	**$ 447,278**	**$ 585,500**	**$ (138,222)**
Operating Expenses			
Consultants & Contracts	651,204	1,383,150	(731,946)
Rent & Improvements	-	-	-
Office Costs	12,310	2,500	9,810
Professional Services	297,197	316,100	(18,903)
Miscellaneous	-	-	-
Depreciation	-	-	-
Total Operating Expenses	**$ 960,711**	**$ 1,701,750**	**$ (741,039)**
Total Direct Expenses	**$ 5,494,628**	**$ 7,146,495**	**$ (1,651,867)**
SPP Inc. Indirect Expenses	**$ 4,186,854**	**$ 4,368,323**	**$ (181,469)**
SPP RE Indirect Expenses [1]	**$ 0**	**$ -**	**$ 0**
Total Indirect Expenses	**$ 4,186,854**	**$ 4,368,323**	**$ (181,469)**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**
Total Expenses (B)	**$ 9,681,482**	**$ 11,514,818**	**$ (1,833,336)**
Change in Assets (A - B)	**(153,590)**	**(1,989,744)**	**1,836,154**
Fixed Assets			
Depreciation	-	-	-
Computer & Software CapEx	-	-	-
Furniture & Fixtures CapEx	-	-	-
Equipment CapEx	-	-	-
Leasehold Improvements	-	-	-
Incr(Dec) in Fixed Assets	**-**	**-**	**-**
Allocation of Fixed Assets	-	-	-
Total Inc(Dec) in Fixed Assets (C)	**-**	**-**	**-**
TOTAL BUDGET (B + C)	**$ 9,681,482**	**$ 11,514,818**	**$ (1,833,336)**
Change in Working Capital (A-B-C)	**$ (153,590)**	**$ (1,989,744)**	**$ 1,836,154**
FTEs (2)	**30.00**	**34.50**	**(4.50)**

(1) SPP RE Indirect Expenses which represent direct expenses for SPP RE Administrative Services, are included in direct expenses.

(2) Actual FTE equal RE Direct Staff FTEs (number of days employed at RE during 2013 divided by 365) plus Shared Staff FTEs (2013 billed hours divided by 1880)

Southwest Power Pool
Regional Entity
Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013

RELIABILITY STANDARDS	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	351,841	351,841	-	0.00%	
Penalty Sanctions	39,801	39,801	-	0.00%	
Total ERO Funding	$ 391,642	$ 391,641	$ -	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	$ 391,642	$ 391,641	$ -	0.00%	
Expenses					
Personnel Expenses					
Salaries	44,611	154,835	(110,224)	-71.19%	Personnel Expenses, including taxes and benefits, trailed budget primarily due to the completion of SPP's Regional UFLS Standard. NERC filed a petition with FERC for approval of the standard on April 23, 2013.
Payroll Taxes	2,976	11,845	(8,869)	-74.88%	
Employee Benefits	3,625	9,390	(5,765)	-61.40%	
Savings & Retirement	1,813	6,193	(4,380)	-70.73%	
Total Personnel Expenses	$ 53,025	$ 182,263	$ (129,238)	-70.91%	
Meeting Expenses					
Meetings	-	-	-		
Travel	-	5,000	(5,000)	-100.00%	Meeting expenses trailed buget due to the completion of the Regional UFLS standard and subsequent filing in April 2013.
Conference Calls	-	-	-		
Total Meeting Expenses	$ -	$ 5,000	$ (5,000)	-100.00%	
Operating Expenses					
Consultants & Contracts	-	-	-		
Rent & Improvements	-	-	-		
Office Costs	-	-	-		
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	$ -	$ -	$ -		
Total Direct Expenses	$ 53,025	$ 187,263	$ (134,238)	-71.68%	
SPP Inc. Indirect Expenses	94,934	158,273	(63,339)	-40.02%	SPP Inc. Indirect Expenses trailed budget due to the actual FTEs being lower than the budgeted FTEs. SPP RE Inc. Indirect Expenses trailed budget due to a smaller percentage being allocated to this program area based on the relative share of functional program direct expenses.
SPP RE Indirect Expenses	17,548	46,105	(28,557)	-61.94%	
Total Indirect Expenses	$ 112,482	$ 204,378	$ (91,896)	-44.96%	
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses (B)	$ 165,507	$ 391,641	$ (226,134)	-57.74%	
Change in Assets (A - B)	$ 226,135	$ -	$ 226,134		
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	$ -	$ -	$ -		
TOTAL BUDGET (B + C)	$ 165,507	$ 391,641	$ (226,134)	-57.74%	
Change in Working Capital (A-B-C)	$ 226,135	$ -	$ 226,134		
FTE's	0.68	1.25	(0.57)	-45.60%	FTES were lower than budgeted FTEs due to less than expected activity by Shared Staff and RE Direct Staff because of the completion of the UFLS standard in April 2013.

Southwest Power Pool
Regional Entity
Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013

COMPLIANCE OPERATIONS, ENFORCEMENT and ORGANIZATION REGISTRATION (includes Critical Infrastructure Protection)	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	7,455,643	7,455,643	-	0.00%	
Penalty Sanctions	708,454	708,454		0.00%	
Total ERO Funding	$ 8,164,097	$ 8,164,097	$ -	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	$ 8,164,097	$ 8,164,097	$ -	**0.00%**	
Expenses					
Personnel Expenses					
Salaries	2,309,533	2,594,600	(285,067)	-10.99%	Personnel Expenses, including taxes and benefits, trailed budget primarily due to unfilled budgeted positions. As of December 31, 2013, four positions (Direct of Compliance and Events, two Lead Engineers and a CIP Compliance Specialist) were unfilled. The Director is shared between the Compliance Program and the Reliability Assessment Program. The two Engineer positions are in the Reliability Assessment program.
Payroll Taxes	151,857	198,487	(46,630)	-23.49%	
Employee Benefits	204,278	207,142	(2,864)	-1.38%	
Savings & Retirement	92,642	103,784	(11,142)	-10.74%	
Total Personnel Expenses	$ 2,758,310	$ 3,104,013	$ (345,703)	**-11.14%**	
Meeting Expenses					
Meetings	48,798	6,500	42,298	651%	Meeting Expenses exceeded budget due to the number of compliance and enforcement meetings held relative to those budgeted.
Travel	283,814	310,000	(26,186)	-8.45%	
Conference Calls	-	-	-		
Total Meeting Expenses	$ 332,612	$ 316,500	$ 16,112	**5.09%**	
Operating Expenses					
Consultants & Contracts	651,205	870,000	(218,795)	-25.15%	Consultant and Contractor Expenses trailed budget due to a reduction in the use of these services because of the increased experience of Direct Staff and the delay in the implementation date of the BES definition.
Rent & Improvements		-	-		
Office Costs	7,275	-	7,275		
Professional Services	66	-	66		
Miscellaneous		-	-		
Depreciation		-	-		
Total Operating Expenses	$ 658,546	$ 870,000	$ (211,454)	**-24.31%**	
Total Direct Expenses	$ 3,749,468	$ 4,290,513	$ (541,045)	**-12.61%**	
SPP Inc. Indirect Expenses	2,807,434	2,817,251	(9,817)	-0.35%	SPP RE Indirect Expenses allocated to this program area exceeded budget due to a larger percentage being allocated to this program area based on the relative share of functional program direct expenses.
SPP RE Indirect Expenses	1,240,817	1,056,333	184,484	17.46%	
Total Indirect Expenses	$ 4,048,251	$ 3,873,584	$ 174,667	**4.51%**	
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses (B)	$ 7,797,719	$ 8,164,097	$ (366,378)	**-4.49%**	
Change in Assets (A - B)	$ 366,378	$ -	$ 366,378		
Fixed Assets					
Depreciation	0.00	0.00	0.00		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	$ -	$ -	$ -		
TOTAL BUDGET (B + C)	$ 7,797,719	$ 8,164,097	$ (366,378)	**-4.49%**	
Change in Working Capital (A-B-C)	$ 366,378	$ -	$ 366,378		
FTE's	20.12	22.25	(2.13)	-9.57%	FTEs were lower than budget due to the unfilled budgeted positions.

Southwest Power Pool
Regional Entity
Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013

RELIABILITY ASSESSMENTS and PERFORMANCE ANALYSIS	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	2,399,251	2,399,251	-	0.00%	
Penalty Sanctions	206,964	206,964	-	0.00%	
Total ERO Funding	$ 2,606,215	$ 2,606,215	$ -	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	$ 2,606,215	$ 2,606,215	$ -	**0.00%**	
Expenses					
Personnel Expenses					Personnel Expenses, including taxes and benefits, trailed budget primarily due to the unfilled budgeted positions. As of December 31, 2013, four positions (Director of Compliance and Events, two Lead Engineers and a CIP Compliance Specialist) were unfilled. The Director is shared between the Compliance Program and the Reliability Assessment Program. The two Engineer positions are in the Reliability Assessment program.
Salaries	488,568	692,278	(203,710)	-29.43%	
Payroll Taxes	37,026	52,959	(15,933)	-30.09%	
Employee Benefits	32,925	51,828	(18,903)	-36.47%	
Savings & Retirement	19,723	27,691	(7,968)	-28.77%	
Total Personnel Expenses	$ 578,242	$ 824,756	$ (246,514)	**-29.89%**	
Meeting Expenses					Travel Expenses trailed budget primarily due to the unfilled budgeted positions and the promotion of the Manager of Regulatory Interface and Process Improvement from Direct Staff in the RAPA program area.
Meetings	-	-	-		
Travel	23,765	108,000	(84,235)	-78.00%	
Conference Calls	-	-	-		
Total Meeting Expenses	$ 23,765	$ 108,000	$ (84,235)	**-78.00%**	
Operating Expenses					Consultant and Contract Expenses trailed budget primarily due to the delay in the implementation of the BES definition.
Consultants & Contracts		498,150	(498,150)	-100.00%	
Rent & Improvements	-	-	-		
Office Costs	80	-	80		
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	$ 80	$ 498,150	$ (498,070)	**-99.98%**	
Total Direct Expenses	$ 602,087	$ 1,430,906	$ (828,819)	**-57.92%**	
SPP Inc. Indirect Expenses	558,520	823,017	(264,497)	-32.14%	SPP Inc. Indirect Expenses trailed budget due to the actual FTEs being lower than the budgeted FTEs. SPP RE Inc. Indirect Expenses trailed budget due to a smaller percentage being allocated to this program area based on the relative share of functional program direct expenses.
SPP RE Indirect Expenses	199,250	352,292	(153,042)	-43.44%	
Total Indirect Expenses	$ 757,770	$ 1,175,309	$ (417,539)	**-35.53%**	
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses (B)	$ 1,359,857	$ 2,606,215	$ (1,246,358)	**-47.82%**	
Change in Assets (A - B)	$ 1,246,358	$ -	$ 1,246,358		
Fixed Assets					
Depreciation	0.00	0.00	0.00		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	$ -	$ -	$ -		
TOTAL BUDGET (B + C)	$ 1,359,857	$ 2,606,215	$ (1,246,358)	**-47.82%**	
Change in Working Capital (A-B-C)	$ 1,246,358	$ -	$ 1,246,358		
FTE's	4.00	6.50	(2.50)	**-38.45%**	FTEs were lower than budget due to the unfilled budgeted positions.

Southwest Power Pool
Regional Entity
Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013

TRAINING, EDUCATION and OPERATOR CERTIFICATION	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	185,750	185,750	-	0.00%	
Penalty Sanctions	31,841	31,841		0.00%	
Total ERO Funding	$ 217,591	$ 217,591	$ -	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	$ 217,591	$ 217,591	$ -	**0.00%**	
Expenses					
Personnel Expenses					
Salaries	80,603	-	80,603		To maintain salary confidentiality, Personnel Expenses for the Outreach and Standards Coordinator are budgeted in the Compliance Program.
Payroll Taxes	6,166	-	6,166		
Employee Benefits	4,851	-	4,851		
Savings & Retirement	3,224	-	3,224		
Total Personnel Expenses	$ 94,844	$ -	$ 94,844		
Meeting Expenses					
Meetings	22,419	55,000	(32,581)	-59.24%	Meeting & Travel Expenses trailed budget due to the number of meetings held at the SPP Corporate Campus. Travel Expenses for the Outeach and Standards Coordinator are in the Gen & Admin program area.
Travel		13,000	(13,000)	-100.00%	
Conference Calls	-	-	-		
Total Meeting Expenses	$ 22,419	$ 68,000	$ (45,581)	**-67.03%**	
Operating Expenses					
Consultants & Contracts		-	-		Professional Services Expenses trailed budget because SPP RE's video series expenses were lower than projected.
Rent & Improvements	-	-	-		
Office Costs	-	-	-		
Professional Services	3,315	5,000	(1,685)	-33.70%	
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	$ 3,315	$ 5,000	$ (1,685)	**-33.70%**	
Total Direct Expenses	$ 120,578	$ 73,000	$ 47,578	**65.18%**	
SPP Inc. Indirect Expenses	104,707	126,618	(21,911)	-17.31%	SPP Inc. Indirect Expenses trailed budget due to the actual FTEs being lower than budgeted FTEs. SPP RE Indirect Expenses allocated to this program area exceeded budget due to the larger percentage being allocated to this program area based on the relative share of functional program direct expenses.
SPP RE Indirect Expenses	39,903	17,973	21,930	122.02%	
Total Indirect Expenses	$ 144,610	$ 144,591	$ 19	**0.01%**	
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses (B)	$ 265,188	$ 217,591	$ 47,597	**21.87%**	
Change in Assets (A - B)	$ (47,597)	$ -	$ (47,597)		
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	$ -	$ -	$ -		
TOTAL BUDGET (B + C)	$ 265,188	$ 217,591	$ 47,597	**21.87%**	
Change in Working Capital (A-B-C)	$ (47,597)	$ -	$ (47,597)		
FTE's	0.75	1.00	(0.25)	**-25.00%**	FTEs were lower than budget due to a reassignment of personnel to other program areas.

Southwest Power Pool
Regional Entity
Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013

SITUATION AWARENESS and INFRASTRUCTURE SECURITY	2013 Actual	2013 Budget	2013 Variance from Budget		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	127,313	127,313	-	0.00%	
Penalty Sanctions	7,960	7,960		0.00%	
Total ERO Funding	$ 135,273	$ 135,273	$ -	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	$ 135,273	$ 135,273	$ -	**0.00%**	
Expenses					
Personnel Expenses					
Salaries	37,792	72,790	(34,998)	-48.08%	Personnel Expenses, including taxes and benefits, trailed budget due to the promotion of the Manager of Regulatory Interface and Process Improvement from Direct Staff in the RAPA program area performing SAIS activities.
Payroll Taxes	2,891	5,568	(2,677)	-48.08%	
Employee Benefits	1,617	1,878	(261)	-13.90%	
Savings & Retirement	1,512	2,912	(1,400)	-48.08%	
Total Personnel Expenses	$ 43,812	$ 83,148	$ (39,336)	**-47.31%**	
Meeting Expenses					
Meetings	-	-	-		
Travel	-	-	-		
Conference Calls	-	-	-		
Total Meeting Expenses	$ -	$ -	$ -		
Operating Expenses					
Consultants & Contracts		-	-		
Rent & Improvements	-	-	-		
Office Costs	-	-	-		
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	$ -	$ -	$ -		
Total Direct Expenses	$ 43,812	$ 83,148	$ (39,336)	**-47.31%**	
SPP Inc. Indirect Expenses	34,902	31,655	3,247	10.26%	SPP RE Inc. Indirect Expenses trailed budget due to a smaller percentage being allocated to this program area based on the relative share of functional program direct expenses.
SPP RE Indirect Expenses	14,499	20,471	(5,972)	-29.17%	
Total Indirect Expenses	$ 49,401	$ 52,126	$ (2,725)	**-5.23%**	
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses (B)	$ 93,213	$ 135,274	$ (42,061)	**-31.09%**	
Change in Assets (A - B)	$ 42,060	$ -	$ 42,061		
Fixed Assets					
Depreciation	0.00	0.00	0.00		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	$ -	$ -	$ -		
TOTAL BUDGET (B + C)	$ 93,213	$ 135,274	$ (42,061)	**-31.09%**	
Change in Working Capital (A-B-C)	$ 42,060	$ -	$ 42,061		
FTE's	0.25	0.25	-	**0.00%**	

Southwest Power Pool
Regional Entity
Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013

MEMBER FORUMS

	2013 Actual	2013 Budget	Variance from Budget Over(Under	Comments (Explain variances > +/- 10% and >$10,000)
Funding				
ERO Funding				
Assessments			-	
Penalty Sanctions				
Total ERO Funding	$ -	$ -	$ -	
Federal Grants		-	-	-
Membership Fees		-	-	-
Testing		-	-	-
Services & Software		-	-	-
Workshop Fees		-	-	-
Interest		-	-	-
Miscellaneous		-	-	-
Total Funding (A)		-	-	-
Expenses				
Personnel Expenses				
Salaries		-	-	-
Payroll Taxes		-	-	-
Employee Benefits		-	-	-
Savings & Retirement		-	-	-
Total Personnel Expenses		-	-	-
Meeting Expenses				
Meetings		-	-	-
Travel		-	-	-
Conference Calls		-	-	-
Total Meeting Expenses		-	-	-
Operating Expenses				
Consultants & Contracts		-	-	
Rent & Improvements		-	-	
Office Costs		-	-	
Professional Services		-	-	
Miscellaneous		-	-	
Depreciation		-	-	
Total Operating Expenses		-	-	-
Indirect Expenses		-	-	-
Other Non-Operating Expenses		-	-	-
Total Expenses (B)		-	-	-
Change in Assets (A - B)		-	-	-
Fixed Assets				
Depreciation		-	-	-
Computer & Software CapEx		-	-	-
Furniture & Fixtures CapEx		-	-	-
Equipment CapEx		-	-	-
Leasehold Improvements		-	-	-
Incr(Dec) in Fixed Assets		-	-	-
Allocation of Fixed Assets		-	-	-
Total Inc(Dec) in Fixed Assets (C)		-	-	-
TOTAL BUDGET (B + C)		-	-	-
Change in Working Capital (A-B-		-	-	-
FTE's		-	-	-

Southwest Power Pool
Regional Entity
Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013

GENERAL and ADMINISTRATIVE	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and >$10,000)
Funding					
ERO Funding					
Assessments	(1,989,744)	(1,989,744)	-	0.00%	
Penalty Sanctions					
Total ERO Funding	$ (1,989,744)	$ (1,989,744)	$ -	0.00%	
Federal Grants	-	-	-		
Membership Fees	-	-	-		
Testing	-	-	-		
Services & Software	-	-	-		
Workshop Fees	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding (A)	$ (1,989,744)	$ (1,989,744)	$ -	**0.00%**	
Expenses					
Personnel Expenses					
Salaries	464,421	558,118	(93,697)	-16.79%	Personnel Expenses, including taxes and benefits, primarily trailed budget due to the delay in filling the Manager of Regulatory Interface and Process Improvement position until October 2013.
Payroll Taxes	28,309	42,696	(14,387)	-33.70%	
Employee Benefits	46,447	41,926	4,521	10.78%	
Savings & Retirement	19,229	22,325	(3,096)	-13.87%	
Total Personnel Expenses	$ 558,406	$ 665,065	$ (106,659)	**-16.04%**	
Meeting Expenses					
Meetings	10,385	25,000	(14,615)	-58.46%	Meeting Expenses trailed budget primarily due to the number of meetings held at the SPP Corporate Campus.
Travel	58,097	63,000	(4,903)	-7.78%	
Conference Calls	-	-	-		
Total Meeting Expenses	$ 68,482	$ 88,000	$ (19,518)	**-22.18%**	
Operating Expenses					
Consultants & Contracts	-	15,000	(15,000)	-100.00%	Consultant & Contract Expense and Professional Services trailed budget primarily due to a reduced need to engage these services. Office costs exceeded budget due to the need to purchase some additional equipment for use at the Compliance Workshops.
Rent & Improvements	-	-	-		
Office Costs	4,955	2,500	2,455	98.20%	
Professional Services	139,366	161,100	(21,734)	-13.49%	
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	$ 144,321	$ 178,600	$ (34,279)	**-19.19%**	
Total Direct Expenses	$ 771,209	$ 931,665	$ (160,456)	**-17.22%**	
SPP Inc. Indirect Expenses	586,357	411,509	174,848	42.49%	SPP Inc. Indirect Expenses exceeded budget due to the actual FTEs being higher than the budgeted FTEs.
SPP RE Indirect Expenses	(1,357,566)	(1,343,173)	(14,392)	1.07%	
Total Indirect Expenses	$ (771,209)	$ (931,665)	$ 160,456	**-17.22%**	
Other Non-Operating Expenses	$ -	$ -	$ -		
Total Expenses (B)	$ -	$ -	$ -		
Change in Assets (A - B)	$ (1,989,744)	$ (1,989,744)	$ -	**0.00%**	
Fixed Assets					
Depreciation	0.00	0.00	0.00		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Incr(Dec) in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	-	-	-		
Total Inc(Dec) in Fixed Assets (C)	$ -	$ -	$ -		
TOTAL BUDGET (B + C)	$ -	$ -	$ -		
Change in Working Capital (A-B-C)	$ (1,989,744)	$ (1,989,744)	$ -	0.00%	
FTE's	**4.20**	**3.25**	**0.95**	0.00%	FTEs were higher than budget due to the reassignment of personnel to this program area.

Southwest Power Pool
Regional Entity
Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013

LEGAL and REGULATORY	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)	Comments (Explain variances > +/- 10% and >$10,000)
Funding				
ERO Funding				
Assessments		-	-	
Penalty Sanctions		-		
Total ERO Funding	$ -	$ -	$ -	
Federal Grants	-	-	-	
Membership Fees	-	-	-	
Testing	-	-	-	
Services & Software	-	-	-	
Workshop Fees	-	-	-	
Interest	-	-	-	
Miscellaneous	-	-	-	
Total Funding (A)	-	-	-	
Expenses				
Personnel Expenses				
Salaries	-	-	-	
Payroll Taxes	-	-	-	
Employee Benefits	-	-	-	
Savings & Retirement	-	-	-	
Total Personnel Expenses	-	-	-	
Meeting Expenses				
Meetings	-	-	-	
Travel	-	-	-	
Conference Calls	-	-	-	
Total Meeting Expenses	-	-	-	
Operating Expenses				
Consultants & Contracts	-	-	-	
Rent & Improvements	-	-	-	
Office Costs	-	-	-	
Professional Services	154,450	150,000	4,450	2.97%
Miscellaneous	-	-	-	
Depreciation	-	-	-	
Total Operating Expenses	**154,450**	**150,000**	**4,450**	**2.97%**
Total Direct Expenses	**154,450**	**150,000**	**4,450**	
SPP Inc. Indirect Expenses	-	-	-	
SPP RE Indirect Expenses	(154,450)	(150,000)	(4,450)	
Total Indirect Expenses	$ **(154,450)**	$ **(150,000)**	$ **(4,450)**	**2.97%**
Other Non-Operating Expenses	-	-	-	
Total Expenses (B)	-	-	-	
Change in Assets (A - B)	-	-	-	
Fixed Assets				
Depreciation	0.00	0.00	0.00	
Computer & Software CapEx	-	-	-	
Furniture & Fixtures CapEx	-	-	-	
Equipment CapEx	-	-	-	
Leasehold Improvements	-	-	-	
Incr(Dec) in Fixed Assets	-	-	-	
Allocation of Fixed Assets	-	-	-	
Total Inc(Dec) in Fixed Assets (C)	-	-	-	
TOTAL BUDGET (B + C)	-	-	-	
Change in Working Capital (A-B-C)	-	-	-	
FTE's	-	-	-	

Southwest Power Pool
Regional Entity
Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013

INFORMATION TECHNOLOGY	**2013 Actual**	**2013 Budget**	**2013 Variance from Budget Over(Under)**	Comments (Explain variances > +/- 10% and >$10,000)
Funding				
ERO Funding				The costs for IT services to support all RE programs are
Assessments			-	accounted for within the SPP , Inc. Indirect expenses.
Penalty Sanctions				
Total ERO Funding	$ -	$ -	$ -	
Federal Grants	-		-	-
Membership Fees	-		-	-
Testing	-		-	-
Services & Software	-		-	-
Workshop Fees	-		-	-
Interest	-		-	-
Miscellaneous	-		-	-
Total Funding (A)	$ -	$ -	$ -	
Expenses				
Personnel Expenses				
Salaries	-		-	-
Payroll Taxes	-		-	-
Employee Benefits	-		-	-
Savings & Retirement	-		-	-
Total Personnel Expenses	$ -	$ -	$ -	
Meeting Expenses				
Meetings	-		-	-
Travel	-		-	-
Conference Calls	-		-	-
Total Meeting Expenses	$ -	$ -	$ -	
Operating Expenses				
Consultants & Contracts	-		-	-
Rent & Improvements	-		-	-
Office Costs	-		-	-
Professional Services	-		-	-
Miscellaneous	-		-	-
Depreciation	-		-	-
Total Operating Expenses	$ -	$ -	$ -	
Total Direct Expenses	$ -	$ -	$ -	
SPP Inc. Indirect Expenses	-		-	-
SPP RE Indirect Expenses			-	-
Total Indirect Expenses	$ -	$ -	$ -	
Other Non-Operating Expenses	$ -	$ -	$ -	
Total Expenses (B)	$ -	$ -	$ -	
Change in Assets (A - B)	$ -	$ -	$ -	
Fixed Assets				
Depreciation	0.00	0.00	0.00	
Computer & Software CapEx	-		-	-
Furniture & Fixtures CapEx	-		-	-
Equipment CapEx	-		-	-
Leasehold Improvements	-		-	-
Incr(Dec) in Fixed Assets	$ -	$ -	$ -	
Allocation of Fixed Assets	-		-	-
Total Inc(Dec) in Fixed Assets (C)	$ -	$ -	$ -	
TOTAL BUDGET (B + C)	$ -	$ -	$ -	
Change in Working Capital (A-B-C)	$ -	$ -	$ -	
FTE's	-		-	

Southwest Power Pool
Regional Entity
Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013

HUMAN RESOURCES	2013 Actual	2013 Budget	Variance from Budget Over(Under)	Comments (Explain variances > +/- 10% and >$10,000)
Funding				
ERO Funding				The costs for HR services to support all RE programs ar
Assessments			-	accounted for within the SPP , Inc. Indirect expenses.
Penalty Sanctions				
Total ERO Funding	$ -	$ -	$ -	
Federal Grants	-	-	-	
Membership Fees	-	-	-	
Testing	-	-	-	
Services & Software	-	-	-	
Workshop Fees	-	-	-	
Interest	-	-	-	
Miscellaneous	-	-	-	
Total Funding (A)	$ -	$ -	$ -	
Expenses				
Personnel Expenses				
Salaries	-	-	-	
Payroll Taxes	-	-	-	
Employee Benefits	-	-	-	
Savings & Retirement	-	-	-	
Total Personnel Expense	$ -	$ -	$ -	
Meeting Expenses				
Meetings	-	-	-	
Travel	-	-	-	
Conference Calls	-	-	-	
Total Meeting Expenses	$ -	$ -	$ -	
Operating Expenses				
Consultants & Contra	-	-	-	
Rent & Improvement	-	-	-	
Office Costs	-	-	-	
Professional Services	-	-	-	
Miscellaneous	-	-	-	
Depreciation	-	-	-	
Total Operating Expense	$ -	$ -	$ -	
Total Direct Expenses	$ -	$ -	$ -	
Indirect Expenses	$ -	$ -	$ -	
Other Non-Operating Ex	$ -	$ -	$ -	
Total Expenses (B)	$ -	$ -	$ -	
Change in Assets (A - B)	$ -	$ -	$ -	
Fixed Assets				
Depreciation	0.00	0.00	0.00	
Computer & Software	-	-	-	
Furniture & Fixtures C	-	-	-	
Equipment CapEx	-	-	-	
Leasehold Improveme	-	-	-	
Incr(Dec) in Fixed Assets	$ -	$ -	$ -	
Allocation of Fixed Ass	-	-	-	
Total Inc(Dec) in Fixed As	$ -	$ -	$ -	
TOTAL BUDGET (B + C)	$ -	$ -	$ -	
Change in Working Capita	$ -	$ -	$ -	
FTE's	-	-	-	

Southwest Power Pool
Regional Entity
Statement of Activities and Capital Expenditures
01/01/2013 - 12/31/2013

ACCOUNTING and FINANCE	2013 Actual	2013 Budget	2013 Variance from Budget Over(Under)	Comments (Explain variances > +/- 10% and >$10,000)
Funding				
ERO Funding			-	The costs for Financial services to support all RE programs are accounted for within the SPP , Inc. Indirect expenses.
Assessments				
Penalty Sanctions				
Total ERO Funding	$ -	$ -	$ -	
Federal Grants		-	-	-
Membership Fees		-	-	-
Testing		-	-	-
Services & Software		-	-	-
Workshop Fees		-	-	-
Interest		-	-	-
Miscellaneous		-	-	-
Total Funding (A)	$ -	$ -	$ -	
Expenses				
Personnel Expenses				
Salaries		-	-	-
Payroll Taxes		-	-	-
Employee Benefits		-	-	-
Savings & Retirement		-	-	-
Total Personnel Expenses	$ -	$ -	$ -	
Meeting Expenses				
Meetings		-	-	-
Travel		-	-	-
Conference Calls		-	-	
Total Meeting Expenses	$ -	$ -	$ -	
Operating Expenses				
Consultants & Contracts		-	-	
Rent & Improvements		-	-	
Office Costs		-	-	
Professional Services		-	-	
Miscellaneous		-	-	
Depreciation		-	-	
Total Operating Expenses	$ -	$ -	$ -	
Indirect Expenses	$ -	$ -	$ -	
Other Non-Operating Expenses		-	-	-
Total Expenses (B)		-	-	-
Change in Assets (A - B)		-	-	-
Fixed Assets				
Depreciation		0.00	0.00	0.00
Computer & Software CapEx		-	-	-
Furniture & Fixtures CapEx		-	-	-
Equipment CapEx		-	-	-
Leasehold Improvements		-	-	-
Incr(Dec) in Fixed Assets	$ -	$ -	$ -	
Allocation of Fixed Assets		-	-	-
Total Inc(Dec) in Fixed Assets (C)	$ -	$ -	$ -	
TOTAL BUDGET (B + C)	$ -	$ -	$ -	
Change in Working Capital (A-B-C)	$ -	$ -	$ -	

Attachment 2

CALCULATION OF THE SPP INC. INDIRECT EXPENSE RATE[1]

Support Groups[2]		**Overhead Costs to Allocate**	
Administration	$	13,512,703	*
Officers		5,186,792	**
Accounting		1,126,218	
SPP Compliance- Physical Security		191,153	
Human Resources		2,161,869	
Customer Services		560,123	
Legal		1,254,391	
Communications		320,881	
Information Technology		13,795,479	
Total Costs	**$**	**38,109,609**	**A**

Non-Support Resource Groups		
Ending 2011 Headcounts		301
Average Work Hours/FTE in 2011		1880
# of Work Hours in 2011		**565,880** **B**
2011 Indirect Overhead Expense Rate (A/B)	**$**	**67.35**
Times Budgeted SPP RE FTEs		**34.50**
Times Average Work Hours/FTE		**1,880**
Budgeted SPP Inc. Indirect Costs	**$**	**4,368,321**

[1]Due to the timing of the budget process/schedule, the estimated overhead rate for 2013 is based on actual 2011 costs. Any variance between the estimated overhead rate and the actual 2013 overhead rate will be included in the annual 2013 Business Plan and

[2] The services provided by these support groups are separate and distinct from the services provided by SPP RE direct staff and consultants and contractors.

* Does not include FERC Pass-Thru Fees and depreciation of market and transmission assets.
** Does not include costs for executives performing delegated functions.

Increase in SPP, Inc. OH Costs due to Change in FTEs

Attachment 3

CALCULATION OF THE SPP INC. ACTUAL INDIRECT EXPENSE RATE

Support Groups[1]		Overhead Costs to Allocate	
Administration	$	18,800,747	*
Officers		5,121,360	**
Accounting		1,245,053	
Corporate Services		5,101,970	
SPP Compliance - Physical Security		-	
Human resources		-	
Customer Services		-	
Legal		1,470,717	
Communications		378,593	
Information Technology		15,066,273	
Total Costs	**$**	**47,184,713**	**A**
Non-Support Resource Groups			
Ending 2011 Headcounts		338	
Average Work Hours/FTE in 2011		1880	
# of Work Hours in 2011		**635,440**	**B**
2013 Indirect Overhead Expense Rate (A/B)	**$**	**74.26**	
Times ACTUAL SPP RE FTEs		**30.00**	
Times Average Work Hours/FTE		**1,880**	
Budgeted SPP Inc. Indirect Costs	**$**	**4,186,854**	

[1] The services provided by these support groups are separate and distinct from the services provided by SPP RE direct staff and consultants and contractors.

* Does not include FERC Pass-Thru Fees and depreciation of market and transmission assets.
** Does not include costs for executives performing delegated functions.

Southwest Power Pool, Inc.

Independent Auditor's Report and Financial Statements

December 31, 2013 and 2012

BKD LLP
CPAs & Advisors

Southwest Power Pool, Inc.

December 31, 2013 and 2012

Contents

Independent Auditor's Report 1

Financial Statements

Balance Sheets 3

Statements of Operations 4

Statements of Members' Deficit 5

Statements of Cash Flows 6

Notes to Financial Statements 7

BKD LLP
CPAs & Advisors

400 W. Capitol Avenue, Suite 2500 // P.O. Box 3667 // Little Rock, AR 72203-3667
501.372.1040 // fax 501.372.1250 // bkd.com

Independent Auditor's Report

Board of Directors
Southwest Power Pool, Inc.
Little Rock, Arkansas

We have audited the accompanying financial statements of Southwest Power Pool, Inc., which comprise the balance sheets as of December 31, 2013 and 2012, and the related statements of operations, changes in members' deficit and cash flows for the years then ended, and the related notes to the financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Praxity
MEMBER
GLOBAL ALLIANCE OF INDEPENDENT FIRMS

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of Southwest Power Pool, Inc. as of December 31, 2013 and 2012, and the results of its operations and its cash flows for the years then ended in accordance with accounting principles generally accepted in the United States of America.

BKD, LLP

Little Rock, Arkansas
April 7, 2014

Southwest Power Pool, Inc.

Balance Sheets

(In Thousands)

December 31, 2013 and 2012

Assets

	2013	2012
Current Assets		
Cash and cash equivalents	$ 34,874	$ 95,693
Restricted cash deposits	76,713	43,743
Accounts receivable	24,134	17,923
Prepaid expenses and other	6,967	5,412
Total current assets	142,688	162,771
Property and Equipment, at Cost		
Land	4,812	4,812
Building	66,225	67,378
Furniture and fixtures	10,026	9,891
Equipment and machinery	29,364	35,343
Leasehold improvements	-	588
Software	106,003	81,344
Software in development	106,895	76,539
	323,325	275,895
Less accumulated depreciation and amortization	119,065	102,143
	204,260	173,752
Other Assets, Net	4,463	2,997
	$ 351,411	$ 339,520

See Notes to Financial Statements

Liabilities and Members' Deficit

	2013	2012
Current Liabilities		
Accounts payable	$ 15,953	$ 9,831
Customer deposits	76,713	43,913
Current maturities of long-term debt (*Note 3*)	22,998	12,700
Accrued expenses	29,039	28,741
Deferred revenue	5,919	6,286
Total current liabilities	150,622	101,471
Long-term Debt (*Note 3*)	235,260	258,258
Other Long-term Liabilities	6,425	10,519
Members' Deficit	(40,896)	(30,728)
	$ 351,411	$ 339,520

Southwest Power Pool, Inc.

Statements of Operations

(In Thousands)

Years Ended December 31, 2013 and 2012

	2013	2012
Operating Income		
Tariff fees and member assessments	$ 137,811	$ 118,808
Other member services	4,926	29,111
	142,737	147,919
Operating Expenses		
Salaries and benefits	79,661	72,262
Employee travel	1,868	2,245
Administrative	3,967	3,720
Regulatory assessment	14,699	14,977
Meetings	930	983
Communications system	3,666	4,020
Leases	432	1,690
Maintenance	11,300	8,288
Consulting services	16,077	15,160
Depreciation and amortization	19,398	16,590
	151,998	139,935
Operating (Loss) Income	(9,261)	7,984
Other Income (Expense)		
Interest income	223	149
Interest expense	(7,763)	(6,398)
Change in fair market value of interest rate swaps	923	674
Other expense	258	(214)
	(6,359)	(5,789)
(Loss) Income Before Change in Funded Status of Employee Benefit Plans	(15,620)	2,195
Change in Funded Status of Employee Benefit Plans	5,452	(3,501)
Net Loss	$ (10,168)	$ (1,306)

See Notes to Financial Statements

Southwest Power Pool, Inc.

Statements of Members' Deficit

(In Thousands)

Years Ended December 31, 2013 and 2012

	2013	2012
Balance, Beginning of Year	$ (30,728)	$ (29,422)
Net loss	(10,168)	(1,306)
Balance, End of Year	$ (40,896)	$ (30,728)

Southwest Power Pool, Inc.

Statements of Cash Flows

(In Thousands)

Years Ended December 31, 2013 and 2012

	2013	2012
Operating Activities		
Net loss	$ (10,168)	$ (1,306)
Items not requiring cash		
Depreciation and amortization	19,398	16,590
Change in funded status of employee benefit plans	(5,452)	3,501
Loss on disposal of fixed assets	2	264
Change in fair market value of interest rate swaps	(923)	(674)
Changes in assets and liabilities		
Accounts receivable	(6,211)	(2,023)
Prepaid expenses and other	(1,555)	1,224
Other assets	(674)	(180)
Accounts payable	6,122	(7,985)
Accrued expenses	(70)	1,836
Other long-term liabilities	1,230	229
Net cash provided by operating activities	1,699	11,476
Investing Activities		
Acquisition of property and equipment	(49,818)	(78,340)
Net cash used in investing activities	(49,818)	(78,340)
Financing Activities		
Repayments of long-term debt	(12,700)	(11,206)
Issuance of long-term debt	-	100,000
Net cash (used in) provided by financing activities	(12,700)	88,794
(Decrease) Increase in Cash and Cash Equivalents	(60,819)	21,930
Cash and Cash Equivalents, Beginning of Year	95,693	73,763
Cash and Cash Equivalents, End of Year	$ 34,874	$ 95,693
Supplemental Cash Flow Information		
Interest paid (net of interest capitalized of $2,777 and $2,723 in 2013 and 2012, respectively)	$ 7,932	$ 6,261

Southwest Power Pool, Inc.
Notes to Financial Statements
December 31, 2013 and 2012

Note 1: Nature of Operations and Summary of Significant Accounting Policies

Nature of Operations

Southwest Power Pool, Inc. (the Company) is a not-for-profit entity formed in 1941 and incorporated in 1994. The Company is a Federal Energy Regulatory Commission (FERC)-approved regional transmission organization (RTO) serving more than six million ultimate customers across all or parts of nine states. The Company's membership consists of investor-owned utilities, municipal systems, generation and transmission cooperatives, state authorities, independent power producers, contract participants, power marketers and independent transmission companies.

Major services provided by the Company to its members and customers include tariff administration, electric reliability coordination, regional transmission scheduling, energy imbalance service (EIS) market operations and regional transmission expansion planning.

The Company also serves as the Regional Entity (RE) for its region. The primary responsibility of the RE is the enforcement of North American Electric Reliability Corporation (NERC)-approved reliability standards for users, owners and operators of the bulk power system within the region.

Use of Estimates

The preparation of financial statements in conformity with accounting principles generally accepted in the United States of America requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities and disclosure of contingent assets and liabilities at the date of the financial statements and the reported amounts of revenues and expenses during the reporting period. Actual results could differ from those estimates.

Cash and Cash Equivalents and Deposits (in Thousands)

The Company considers all highly liquid interest-earning investments with stated maturities and coupon rate reset dates of no more than three months to be cash equivalents. At December 31, 2013 and 2012, the Company's cash and cash equivalents, including restricted deposits, are invested primarily in money market funds, mutual funds and repurchase agreements. These investments are typically revalued to the market each day and, in the case of repurchase agreements, are collateralized by U.S. government and federal agency securities. The Company's cash and cash equivalents consist primarily of funds accumulated for general operating purposes. Restricted cash deposits consist primarily of customer security deposits, amounts deposited for engineering studies and funds held in escrow for disputed invoices.

Income Taxes

The Company is exempt from income taxes under Section 501c(6) of the Internal Revenue Code and a similar provision of state law. However, the Company is subject to federal income tax on any unrelated business taxable income.

The Company files tax returns in the U.S. federal jurisdiction. With a few exceptions, the Company is no longer subject to U.S. federal examinations by tax authorities for years before 2010.

Accounts Receivable

Accounts receivable are stated at the amount billed to members, customers and others plus any accrued and unpaid interest. The Company provides an allowance for doubtful accounts, when necessary, which is based upon a review of outstanding receivables, historical collection information and existing economic conditions. Accounts that are unpaid after the due date bear interest at a rate set by FERC. Interest continues to accrue until the account is paid or deemed uncollectible.

Property and Equipment (in Thousands)

Property and equipment are recorded at cost and depreciated on a straight-line basis over the estimated useful life of each asset. The estimated useful lives are as follows:

Building	20 years
Building improvements	Shorter of useful life or remaining life of building
Furniture and fixtures	5 years
Vehicles	5 years
Equipment and machinery	3 years
Software	3 years
Leasehold improvements	Shorter of useful life or lease term

The Company capitalizes interest cost incurred on funds used to construct property, plant and equipment. The capitalized interest is recorded as part of the asset to which it relates and is amortized over the asset's estimated useful life. Interest cost capitalized was $2,777 and $2,723 in 2013 and 2012, respectively.

The Company capitalizes development costs, including interest, for internal use software costs. These costs are included in software in development. Management of the Company is of the opinion that all costs capitalized in association with the software in development are fully recoverable over the anticipated life of the asset.

Long-lived Asset Impairment (in Thousands)

The Company evaluates the recoverability of the carrying value of long-lived assets whenever events or circumstances indicate the carrying amount may not be recoverable. If a long-lived asset is tested for recoverability and the undiscounted estimated future cash flows expected to result from the use and eventual disposition of the asset is less than the carrying amount of the asset, the asset cost is adjusted to fair value and an impairment loss is recognized as the amount by which the carrying amount of a long-lived asset exceeds it fair value.

No asset impairment was recognized during the years ended December 31, 2013 and 2012.

Revenue Recognition

Revenues, consisting of member assessments, tariff administrative fees, contract services and miscellaneous revenues are recognized when earned, and expenses are recognized when incurred.

Customer Deposits

Customers may be required to make deposits with the Company prior to the performance of transmission services and engineering studies. These amounts are typically held for the duration of the service and applied to the customer's final invoice. An offsetting liability equal to the deposit balance is recorded in current liabilities. Funds held in escrow related to disputed invoices are also recorded as a customer deposit under current liabilities.

Tariff Fees and Member Assessments (in Thousands)

An administrative charge is applied to all transmission service under the Company's tariff to cover the expenses related to the administration of the tariff. The charge is calculated in accordance with the terms of the Company's Open Access Transmission Tariff. The administrative rate used for the calculation is established by the board of directors.

Members are assessed monthly based on their prior year average 12-month peak demand multiplied by the total hours in a month and by the monthly assessment rate as established by the board. A member's monthly assessment is offset dollar for dollar for qualifying tariff administrative fees collected from a member in any given assessment period.

The Company collects a membership fee from each member annually. The amount of the membership fee is established by the board of directors of the Company. For 2013 and 2012, all members paid a $6 membership fee.

The Company also bills transmission customers and transmission owners a charge under Schedule 12 on all energy delivered under point-to-point transmission service and network integration transmission service. This provides a mechanism for recovering from transmission customers and transmission owners the annual charges the Company pays to FERC. The rate is developed by FERC in the prior calendar year and applied to energy transmitted in the second prior calendar year.

Deferred Revenue

Revenues for contract services received in advance are recognized over the periods to which the revenues relate.

Other Member Services

The Company provides reliability, tariff administration and scheduling for non-members on a contract basis. The Company also provides engineering study services for long-term transmission service and generation interconnection studies.

Withdrawing Members

Members wishing to withdraw their membership from the Company must provide 24 months written notice and are responsible for their portion of the Company's existing obligations as defined in the bylaws, which include unpaid membership fees, any assessments imposed prior to the effective withdrawal date, any costs or expenses imposed upon the Company as a direct consequence of the member's withdrawal, and the member's share of long-term obligations and related interest.

Concentration of Credit Risk

The Company is exposed to credit risk primarily through accounts receivable and uninsured cash balances. During 2013 and 2012, the Company maintained cash balances, including transaction accounts and short-term investment accounts that are not insured by the Federal Deposit Insurance Corporation. The Company's transaction accounts exceeded federal insurance limits by $9,758 at December 31, 2013. The Company's investment accounts were primarily invested in highly liquid short-term investments such as money market funds, mutual funds and repurchase agreements. The Company also requires the financial institutions holding its cash balances to be rated A or better by nationally recognized rating agencies.

Because the Company considers all accounts receivable to be highly probable of collection, an allowance for doubtful accounts is currently not maintained. The Company requires its customers to meet certain minimum standards of financial condition and creditworthiness to receive unsecured credit from the Company. If these standards cannot be met by a counterparty, the Company requires the posting of defined financial security instruments to cover potential liabilities.

Note 2: Line of Credit (In Thousands)

The Company has a $30,000 revolving line of credit expiring in 2016. At December 31, 2013 and 2012, no amounts were borrowed against this line. The agreement has a variable interest rate equal to the London Interbank Offered Rate (LIBOR) plus a credit margin. The Company's line of credit requires compliance with certain financial and non-financial covenants as well as periodic reporting requirements. The Company was in compliance with the covenant and reporting requirements throughout and at December 31, 2013.

Note 3: Long-term Debt and Interest Rate Swaps (in Thousands)

Long-term Debt

	2013	2012
Variable Rate Term Note due 2027 (A)	$ 3,752	$ 3,958
Variable Rate Term Note due 2014 (B)	5,500	11,000
5.45% Senior Notes due 2016 (C)	15,000	21,000
4.82% Series 2010-A Senior Notes due 2042 (D)	29,541	30,000
4.82% Series 2010-B Senior Notes due 2042 (E)	34,465	35,000
3.55% Series 2010-C Senior Notes due 2024 (F)	70,000	70,000
3.00% Series 2012-D-1 Senior Notes due 2024 (G)	50,000	50,000
3.25% Series 2012-D-2 Senior Notes due 2024 (H)	50,000	50,000
	258,258	270,958
Less current maturities	22,998	12,700
	$ 235,260	$ 258,258

(A) Due February 1, 2027; principal and interest are payable quarterly based on a 25-year amortization. Payments commenced on May 1, 2007. The interest rate adjusts monthly based on the London Interbank Offered Rate (LIBOR) plus 0.85%. The note is secured by a first mortgage on the Company's operation facility.

(B) Due December 25, 2014; interest is payable monthly and principal is payable quarterly based on a seven-year amortization. Payments commenced on March 25, 2008. The interest rate adjusts monthly based on the London Interbank Offered Rate (LIBOR) plus 0.30%. The note is unsecured.

(C) Due July 23, 2016; principal and interest are payable quarterly based on a seven-year amortization. Payments commenced on September 30, 2011. The interest rate is fixed at 5.45%. The note is unsecured.

(D) Due December 30, 2042; principal and interest are payable quarterly based on a 32-year amortization. Principal payments commenced on March 30, 2013. The interest rate is fixed at 4.82%. The note is unsecured.

(E) Due December 30, 2042; principal and interest are payable quarterly based on a 32-year amortization. Principal payments commenced on March 30, 2013. The interest rate is fixed at 4.82%. The note is unsecured.

(F) Due March 30, 2024; principal and interest are payable quarterly based on 13-year amortization. Principal payments commence on June 30, 2014. The interest rate is fixed at 3.55%. The note is unsecured.

(G) Due March 30, 2024; principal and interest are payable quarterly based on 10-year amortization. Principal payments commence on June 30, 2014. The interest rate is fixed at 3.00%. The note is unsecured.

(H) Due September 30, 2024; principal and interest are payable quarterly based on 10-year amortization. Principal payments commence on December 30, 2014. The interest rate is fixed at 3.25%. The note is unsecured.

Aggregate annual maturities of long term debt at December 31, 2013, are:

2014	$ 22,998
2015	24,299
2016	21,353
2017	18,410
2018	18,469
Thereafter	152,729
	$ 258,258

Certain of the Company's term notes require compliance with financial and non-financial covenants, as well as periodic reporting requirements. The Company was in compliance with the covenant and reporting requirements throughout and at December 31, 2013.

Variable-to-Fixed Interest Rate Swap

As a strategy to maintain acceptable levels of exposure to the risk of changes in future cash flows due to interest rate fluctuations, the Company entered into an interest rate swap agreement on September 15, 2006, with U.S. Bank National Association. The agreement provides for the Company to receive interest from the counterparty at LIBOR and to pay interest to the counterparty at a fixed rate of 5.51% on notional amounts of $3,723 and $3,927 at December 31, 2013 and 2012, respectively. Under the agreement, the Company pays or receives the net interest amount quarterly, with the quarterly settlements included in interest expense. The swap was established to hedge interest rate risk on its floating rate debt obligation (Loan A).

The Company entered into another interest rate swap agreement on August 23, 2007, with U.S. Bank National Association. The agreement provides for the Company to receive interest from the counterparty at LIBOR and to pay interest to the counterparty at a fixed rate of 5.31% on notional amounts of $5,500 and $11,000 at December 31, 2013 and 2012, respectively. Under the agreement, the Company pays or receives the net interest amount monthly, with the monthly settlements included in interest expense. The swap was established to hedge interest rate risk on its floating rate debt obligation (Loan B).

The table below presents certain information regarding the Company's interest rate swap agreements.

	2013	2012
Fair value of interest rate swap agreements	$ 934	$ 1,857
Balance sheet location of fair value amounts	Other Long-term Liabilities	Other Long-term Liabilities
Gain recognized in statement of operations	$ 923	$ 674
Location of gain recognized in statement of operations	Change in Fair Market Value of Interest Rate Swaps	Change in Fair Market Value of Interest Rate Swaps

Note 4: Operating Leases (In Thousands)

The Company has noncancellable operating leases for certain office equipment which expire at various times through 2015. The lease for office space expired in early 2013. The Company incurred lease expense related to these operating leases of $432 and $1,690 in 2013 and 2012, respectively.

Future minimum lease payments at December 31, 2013, were:

2014	$ 139
2015	69
	$ 208

Note 5: Employee Benefit Plans (in Thousands)

Pension and Other Postretirement Benefit Plans

The Company has a noncontributory defined benefit pension plan covering all employees meeting eligibility requirements. The Company's funding policy is to make the minimum annual contribution that is required by applicable regulations, plus such amounts as the Company may determine to be appropriate from time to time. The Company expects to contribute approximately $3,660 to the plan in 2014.

The Company has a noncontributory defined benefit postretirement health care plan covering eligible retirees, including those retiring between the ages of 55–65 and hired prior to January 1, 1996. Employees hired after June 1, 2006, are not eligible to participate in the defined postretirement health care plan. The Company's funding policy is to make the minimum annual contribution that is required by applicable regulations, plus such amounts as the Company may determine to be appropriate from time to time. The Company expects to contribute approximately $410 to the plan in 2014.

The Company uses a December 31 measurement date for the plans. Information about the plans' funded status is as follows:

	Pension Benefits		Postretirement Health Care Benefits	
	2013	2012	2013	2012
Benefit obligation	$ 44,090	$ 38,014	$ 7,995	$ 7,353
Fair value of plan assets	41,157	31,295	9,657	7,963
Funded status	$ (2,933)	$ (6,719)	$ 1,662	$ 610

Amounts recognized in the balance sheets:

	Pension Benefits		Postretirement Health Care Benefits	
	2013	2012	2013	2012
Noncurrent assets	$ -	$ -	$ 1,662	$ 610
Noncurrent liabilities	(2,933)	(6,719)	-	-
	$ (2,933)	$ (6,719)	$ 1,662	$ 610

Amounts recognized in members' equity not yet recognized as components of net periodic benefit cost as of December 31, 2013, consist of:

	Pension Benefits	Postretirement Health Care Benefits
Net (gain)/loss	$ 5,401	$ (1,664)
Prior service credit	(21)	-
Transition obligation	115	31
	$ 5,495	$ (1,633)

The accumulated benefit obligation for the defined benefit pension plan was $34,673 and $29,577 at December 31, 2013 and 2012, respectively.

Other significant balances and costs are:

	Pension Benefits		Postretirement Health Care Benefits	
	2013	2012	2013	2012
Employer contributions	$ 4,010	$ 3,892	$ 540	$ 469
Benefits paid	256	177	35	26
Benefit costs	4,625	3,643	542	469

The following amounts have been recognized in the statements of operations for the year ended December 31, 2013:

	Pension Benefits	Postretirement Health Care Benefits
Amounts arising during the period		
Net gain	$ 4,031	$ 1,049
Amounts recognized as components of net periodic benefit cost of the period		
Net loss	352	-
Net prior service credit	1	-
Net transition obligation	16	4

The estimated net loss, prior service cost and transition obligation for the defined benefit pension plan that will be amortized from members' equity into net period benefit cost over the next fiscal year are $58, $1 and $16, respectively. The estimated net gain, prior service cost, and net obligation for the defined benefit postretirement health care plan that will be amortized from members' equity into net periodic benefit cost over the next fiscal year are $37, $0, and $4, respectively.

Weighted-average assumptions used to determine benefit obligations and costs:

	Pension Benefits		Postretirement Health Care Benefits	
	2013	2012	2013	2012
Discount rate benefit obligation	5.5%	5.5%	5.5%	5.5%
Expected return on plan assets	7.0%	7.0%	7.0%	7.0%
Rate of compensation increase	4.0%	4.0%	-	-

The Company has estimated the long-term rate of return on plan assets based primarily on historical returns on plan assets, adjusted for changes in target portfolio allocations and recent changes in long-term interest rates based on publicly available information.

For measurement purposes, a 10% annual rate of increase in the per capita cost of covered health care benefits was assumed for 2013 and 2012. The rate was assumed to decrease gradually to 5% by the year 2019 and remain at that level thereafter.

On December 8, 2003, the *Medicare Prescription Drug, Improvement and Modernization Act of 2003* (the Act) was signed into law. The Act introduces a prescription drug benefit under Medicare Part D, as well as a federal subsidy to sponsors of retiree health care benefit plans that provide benefits at least actuarially equivalent to Medicare Part D. The Company has not determined whether its plan provides benefits that are actuarially equivalent to Medicare Part D.

Financial Accounting Standards Board Staff Position 106-2, *Accounting and Disclosure Requirements Related to the Medicare Prescription Drug, Improvement and Modernization Act of 2003*, subsequently incorporated into FASB Accounting Standards Codification (ASC) 715-60, requires federal subsidies, if any, attributable to past service to be accounted for as an actuarial gain and federal subsidies, if any, attributable to current service to be accounted for as a reduction of net periodic benefit cost. The measures of projected benefit obligation and periodic benefit costs do not reflect any amounts associated with the subsidy because the Company has been unable to conclude whether the benefits provided by the plan are actuarially equivalent to Medicare Part D. The effect of adopting the provisions of ASC 715-60, if and when the Company makes such a determination, is not expected to be material.

The following benefit payments, which reflect expected future service, as appropriate, are expected to be paid as of December 31:

	Pension Benefits	Postretirement Health Care Benefits
2014	$ 452	$ 78
2015	612	128
2016	712	159
2017	841	197
2018	1,045	249
2019–2023	8,380	1,801

The Company's investment strategy is based on an expectation that equity securities will outperform fixed income securities over the long-term. Accordingly, the composition of the Company's plan assets is broadly characterized as a 70/30 allocation between equity and fixed income securities. The strategy utilizes indexed and actively managed mutual fund instruments as well as direct investment in individual equity and fixed income securities. Investments in the plans must adhere to the Investment Policy Statement developed by the Company. The Investment Policy Statement limits investments in foreign securities to 20% of the total fair value of plan assets. The Investment Policy Statement is reviewed annually. At December 31, 2013 and 2012, plan assets by category are as follows:

	Pension Plan Assets		Postretirement Health Care Plan Assets	
	2013	2012	2013	2012
Fixed income securities	17%	14%	24%	29%
Equity securities	76	72	72	65
Cash and equivalents	7	14	4	6
	100%	100%	100%	100%

Pension and Other Postretirement Plan Assets

Following is a description of the valuation methodologies used for the pension and postretirement plan assets measured at fair value on a recurring basis and recognized in the accompanying balance sheets, as well as the general classification of the assets pursuant to the valuation hierarchy.

Where quoted market prices are available in an active market, plan assets are classified within Level 1 of the valuation hierarchy. Level 1 plan assets include cash, money market accounts, mutual funds and common stock. If quoted market prices are not available, then fair values are estimated by using pricing models, quoted prices of plan assets with similar characteristics or discounted cash flows. Level 2 plan assets include foreign company stock, corporate debt obligations, foreign corporate debt obligations, government securities and foreign government securities. In certain cases where Level 1 or Level 2 inputs are not available, plan assets are classified within Level 3 of the hierarchy. At December 31, 2013 and 2012, the Company does not hold any plan assets valued using Level 3 inputs.

The fair values of the Company's pension plan assets at December 31, 2013, by asset category are as follows:

		Fair Value Measurements Using		
Asset Category	Total Fair Value	Quoted Prices in Active Markets for Identical Assets (Level 1)	Significant Other Observable Inputs (Level 2)	Significant Unobservable Inputs (Level 3)
Cash	$ 5	$ 5	$ -	$ -
Money market mutual funds	874	874	-	-
Mutual funds				
Foreign large blend	996	996	-	-
Mid cap value	1,741	1,741	-	-
Mid cap growth	6,699	6,699	-	-
Small cap growth	1,780	1,780	-	-
Large growth	6,172	6,172	-	-
Common stock				
Industrial materials	1,602	1,602	-	-
Consumer goods	1,217	1,217	-	-
Financial Services	474	474	-	-
Energy	2,707	2,707	-	-
Healthcare services	2,297	2,297	-	-
Hardware	728	728	-	-
Business services	211	211	-	-
Foreign company stock				
Industrial materials	878	-	878	-
Hardware	628	-	628	-
Business services	124	-	124	-
Energy	2,822	-	2,822	-
Financial services	327	-	327	-
Corporate debt obligations	5,298	-	5,298	-
Foreign corporate debt obligations	930	-	930	-
Government securities	2,000	-	2,000	-
Foreign government securities	647	-	647	-
Total	$ 41,157	$ 27,503	$ 13,654	$ -

The fair values of the Company's pension plan assets at December 31, 2012, by asset category are as follows:

		Fair Value Measurements Using		
Asset Category	Total Fair Value	Quoted Prices in Active Markets for Identical Assets (Level 1)	Significant Other Observable Inputs (Level 2)	Significant Unobservable Inputs (Level 3)
Cash	$ 5	$ 5	$ -	$ -
Money market mutual funds	657	657	-	-
Mutual funds				
Foreign large blend	734	734	-	-
Mid cap value	1,189	1,189	-	-
Mid cap growth	4,734	4,734	-	-
Small cap growth	1,215	1,215	-	-
Large growth	4,099	4,099	-	-
Common stock				
Industrial materials	1,300	1,300	-	-
Consumer goods	978	978	-	-
Financial Services	550	550	-	-
Energy	1,941	1,941	-	-
Healthcare services	1,566	1,566	-	-
Hardware	21	21	-	-
Business services	293	293	-	-
Foreign company stock				
Industrial materials	666	-	666	-
Hardware	834	-	834	-
Business services	133	-	133	-
Energy	1,956	-	1,956	-
Financial services	289	-	289	-
Corporate debt obligations	2,729	-	2,729	-
Foreign corporate debt obligations	1,134	-	1,134	-
Government securities	3,826	-	3,826	-
Foreign government securities	446	-	446	-
Total	$ 31,295	$ 19,282	$ 12,013	$ -

The fair value of the Company's other postretirement benefit plan assets at December 31, 2013, by asset category are as follows:

		Fair Value Measurements		
Asset Category	Total	Quoted Prices in Active Markets for Identical Assets (Level 1)	Significant Other Observable Inputs (Level 2)	Significant Unobservable Inputs (Level 3)
Cash	$ 6	$ 6	$ -	$ -
Money market mutual funds	382	382	-	-
Mutual funds				
Equities				
Foreign large blend	472	472	-	-
Foreign large growth	436	436	-	-
Large cap blend	658	658	-	-
Mid cap value	373	373	-	-
Mid cap growth	433	433	-	-
Small cap value	412	412	-	-
Real estate	498	498	-	-
Emerging markets	368	368		
Commodities	333	333	-	-
Fixed income				
Bond funds	1,961	1,961		
Inflation protected	323	323	-	-
Common stock			-	-
Industrial materials	351	351	-	-
Consumer goods and services	781	781	-	-
Financial services	467	467	-	-
Energy	261	261	-	-
Healthcare services	384	384	-	-
Hardware	52	52	-	-
Business services	277	277	-	-
Software	80	80	-	-
Telecommunications	108	108	-	-
Media	109	109	-	-
Utilities	94	94	-	-
Foreign company stock				
Business services	38	-	38	-
Total	$ 9,657	$ 9,619	$ 38	$ -

The fair value of the Company's other postretirement benefit plan assets at December 31, 2012, by asset category are as follows:

		Fair Value Measurements		
Asset Category	Total	Quoted Prices in Active Markets for Identical Assets (Level 1)	Significant Other Observable Inputs (Level 2)	Significant Unobservable Inputs (Level 3)
Cash	$ 3	$ 3	$ -	$ -
Money market mutual funds	455	455	-	-
Mutual funds				
Equities				
Foreign large blend	392	392	-	-
Foreign large growth	390	390	-	-
Mid cap growth	615	615	-	-
Small cap value	312	312	-	-
Real estate	367	367	-	-
Emerging markets	214	214	-	
Commodities	292	292	-	-
Fixed income				-
Bond funds	2,028	2,028	-	
Inflation protected	292	292	-	-
Common stock				-
Industrial materials	301	301	-	-
Consumer goods and services	631	631	-	-
Financial services	314	314	-	-
Energy	223	223	-	-
Healthcare services	316	316	-	-
Hardware	41	41	-	-
Business services	194	194	-	-
Software	77	77	-	-
Telecommunications	92	92	-	-
Media	71	71	-	-
Utilities	93	93	-	-
Foreign company stock				
Business services	135	-	135	-
Financial services	64	-	64	-
Energy	51	-	51	-
Total	$ 7,963	$ 7,713	$ 250	$ -

Defined Contribution Plans

The Company has a 401(k) defined contribution plan covering substantially all employees. The Company contributes funds to the plan on behalf of plan participants equal to 75% of the participants' elective deferrals up to 6% of deferred compensation. Contributions to the plan were $2,334 and $2,157 for 2013 and 2012, respectively.

The Company has a 457(b) non-qualified tax-deferred compensation plan. This plan is an unfunded plan maintained for the purpose of providing deferred compensation for a select group of management or highly-compensated employees and, therefore, is intended to be exempt from the participation, vesting, funding and fiduciary requirements of Title I of ERISA. Accumulated contributions and earnings of $1,305 and $968 are recorded in other long-term liabilities at December 31, 2013 and 2012, respectively. The Company also offers a 457(f) non-qualified tax-deferred compensation plan to a select group of executive management. The 457(f) plan is intended to be exempt from the participation, vesting, funding and fiduciary requirements of Title I of ERISA and serves to further supplement benefits lost due to IRS limits on compensation and benefits. Accrued benefits of $1,253 and $975 are recorded in other long-term liabilities for the 457(f) plan participants at December 31, 2013 and 2012, respectively.

Note 6: Related Party Transactions (in Thousands)

General disbursements of the Company are apportioned to members based on the formula described in the bylaws of the Company (see *Note 1*). The Company's receivables from members totaled $17,571 and $9,587 as of December 31, 2013 and 2012, respectively. The Company recognized revenues of $128,486 and $110,707, including assessments and tariff administrative fees, from members for the years ended December 31, 2013 and 2012, respectively.

The Southwest Power Pool Regional State Committee (RSC) was incorporated on April 7, 2004, in the State of Arkansas. The RSC is comprised of commissioners from public service commissions or equivalent, having regulatory authority over Company members. FERC, in its February 20, 2004, order regarding the Company's RTO application, stated, "the RSC should have primary responsibility for determining regional proposals and the transition process for funding of regional transmission enhancements, rate structure for a regional access charge and allocation of transmission rights." The RSC prepares budgets annually for the expected costs of its operations. This budget is submitted to the Company's board of directors for approval. The Company includes in its annual budget funds sufficient to cover 100% of the operating costs of the RSC. During 2013 and 2012, the Company incurred $226 and $455, respectively, in expenses attributable to RSC operations. Management of the Company expects such expenditures for 2014 to be approximately $328.

Note 7: Open Access Transmission and EIS Market Operations (In Thousands)

The Company provides short- and long-term firm and non-firm point-to-point transmission services and network integration transmission service across 15 providers in nine states. The Company is responsible for the billing of the transmission customers for the respective services and the remittance of the subsequent collections to the transmission owner on a monthly basis. Billings for these transmission services are not included in the statements of operations. The Company receives a fee for facilitating the transmission process, which is recorded as tariff fees in the Company's statements of operations. For the years ended December 31, 2013 and 2012, the Company billed transmission customers $1,290,757 and $1,118,542, respectively. For the years ended December 31, 2013 and 2012, the Company remitted to transmission owners $1,171,133 and $1,016,886, respectively. At December 31, 2013 and 2012, the Company was due to collect from customers and remit to owners transmission service charges of $101,106 and $85,613, respectively.

The Company's EIS market is a wholesale market that operates under a tariff approved by FERC and is consistent with the mandate of the FERC Order No. 2000, which requires RTOs to provide real-time energy imbalance services and market monitoring functions. Weekly settlements of market participants' energy transactions are not reflected in the Company's statements of operations since they do not represent revenues or expenses of the Company, as the Company merely acts as an intermediary in the settlement process. In this role, the Company receives and disburses funds to/from market participants on a weekly basis.

Note 8: Commitments and Contingencies (in Thousands)

Litigation and Regulatory Matters

In 2011, a suit was filed against the Company claiming a violation of the Arkansas Minimum Wage Act for overtime hours. While the Company believes it has meritorious defenses against the suit, the ultimate resolution of the matter could result in a loss to the Company. An estimate of loss cannot be made at this time.

The Company is engaged in various regulatory proceedings at both the federal and state levels. The Company is also subject to claims and lawsuits that arise primarily in the ordinary course of business. It is the opinion of management that the disposition or ultimate resolution of such proceedings, claims and lawsuits will not have a material adverse effect on the financial position, results of operations and cash flows of the Company.

Note 9: Disclosures About Fair Value of Financial Instruments (in Thousands)

ASC Topic 820, *Fair Value Measurements*, defines fair value as the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date. Topic 820 also specifies a fair value hierarchy, which requires an entity to maximize the use of observable inputs and minimize the use of unobservable inputs when measuring fair value. The standard describes three levels of inputs that may be used to measure fair value:

Level 1 Quoted prices in active markets for identical assets or liabilities

Level 2 Observable inputs other than Level 1 prices, such as quoted prices for similar assets or liabilities; quoted prices in markets that are not active; or other inputs that are observable or can be corroborated by observable market data for substantially the full term of the assets or liabilities

Level 3 Unobservable inputs that are supported by little or no market activity and are significant to the fair value of the assets or liabilities

Following is a description of the valuation methodologies used for assets and liabilities measured at fair value on a recurring basis and recognized in the accompanying balance sheets, as well as the general classification of such assets and liabilities pursuant to the valuation hierarchy.

Interest Rate Swap Agreements

The fair value is estimated using forward-looking interest rate curves and discounted cash flows that are observable or that can be corroborated by observable market data and, therefore, are classified within Level 2 of the valuation hierarchy. At December 31, 2013 and 2012, the fair value measurement of the interest rate swaps as recognized in the accompanying balance sheets was a liability of $934 and $1,857, respectively.

Cash Equivalents

The fair value of money market mutual funds included in cash equivalents are estimated using quoted prices in active markets for identical assets or liabilities. At December 31, 2013 and 2012, the fair value measurement of the cash equivalents as recognized in the accompanying balance sheets was $13,856 and $13,413, respectively.

The Company has no assets or liabilities measured and recognized in the accompanying balance sheets on a nonrecurring basis.

The following methods were used to estimate the fair value of all other financial instruments recognized in the accompanying balance sheets at amounts other than fair value.

Restricted Cash Deposits

For these short-term instruments, the carrying amount is a reasonable estimate of fair value.

Customer Deposits

The carrying amount is a reasonable estimate of fair value.

Long-term Debt

Fair value is estimated based on the borrowing rates currently available to the Company for bank loans with similar terms and maturities.

The following table presents estimated fair values of the Company's financial instruments at December 31, 2013 and 2012.

	2013		2012	
	Carrying Amount	Fair Value	Carrying Amount	Fair Value
Financial assets				
Cash and cash equivalents	$ 34,874	$ 34,874	$ 95,693	$ 95,693
Restricted cash deposits	$ 76,713	$ 76,713	$ 43,743	$ 43,743
Financial liabilities				
Customer deposits	$ 76,713	$ 76,713	$ 43,913	$ 43,913
Long-term debt	$ 258,258	$ 264,200	$ 270,958	$ 274,518
Swap agreements	$ 934	$ 934	$ 1,857	$ 1,857

Note 10: Subsequent Events (in Thousands)

On March 10, 2014, the Company obtained a $33,000 senior unsecured term note facility. This facility will initially be undrawn but will allow the Company to obtain advances as needed during a two year draw period, after which it will convert into an amortizing term loan with escalating principal payments through 2023. Interest will be payable monthly at a floating rate.

Additionally, on March 21, 2014, the Company issued $37,000 in funding related to the 2014 Series E Senior Note due December 30, 2025. This note bears a 3.80% fixed rate interest with quarterly interest payments commencing on June 30, 2014 and principal payments commencing on March 30, 2024. This note is unsecured.

Subsequent events have been evaluated through the date of the Independent Auditor's Report, which is the date the financial statements were available to be issued.

ATTACHMENT 8

2013 ACTUAL COST-TO-BUDGET COMPARISON

AND

2013 AUDITED FINANCIAL REPORT

FOR

TEXAS RELIABILITY ENTITY, INC.

April 29, 2014

Michael Walker, CFO
Susan Turpen, Controller
North American Electric Reliability Corporation
3343 Peachtree Road, NE Floor East Tower – Suite 400
Atlanta, GA 30326

Subject: Texas Reliability Entity (Texas RE) 2013 Actual Cost-to-Budget Comparison

Dear Mr. Walker and Ms. Turpen,

Texas Reliability Entity (Texas RE) has completed the 2013 True Up Analysis. The budget comparisons are compared to the 2013 Texas RE budget, formally approved by FERC.

Texas RE did not use Statutory funds for Non-statutory purposes. Texas RE's policy is to allocate indirect expenses to programs based on the pro-rata share of FTEs to total program FTEs.

Texas RE maintains a $2,000,000 cash reserve balance according to the policy approved by the Texas RE Board of Directors.

The significant expense variances at the aggregate statutory level are explained below. The explanations for the expense variances by statutory program area are provided in the attached spreadsheet.

INCOME

Total Statutory Income was under budget by $40k or 0.4%.

Membership Fees decreased $2,000 or 9%. Fewer registered entities paid membership dues than budgeted.

No Workshop Fees were collected in 2013 causing a 100% budget variance. Registered Entities hosted the workshops; therefore, no fees were charged to attend.

EXPENSES

Personnel Expenses ($553,797 or 7% below budget)

Salary expense was $145k or 2% less than budget due to FTE vacancies. The vacancies were the result of employee turnover and the timing of hiring replacement employees. Employee benefits is 23% less than budget due to fewer employees participating in offered benefits than anticipated.

Travel and Meeting Expenses ($46k or 11.4% less than budget)

Meeting expenses were 16% less than budget due to the workshops being hosted by registered entities with no costs to Texas RE.

Travel expenses were $44k or 12.5% less than budget. Standards attended fewer meetings than budgeted that required travel while the RAPA program required more travel. Less travel was required in the Compliance audit area.

Conference expenses increased $3,784 or 20% offsetting the reduction in the travel expense.

Other Operating Expenses ($818k or 26.5% less than budget)

Consultants and Contract costs were 16.8% less than budget because the IT staff performed some of the task originally planned for consultants in the Sharepoint project implementation.

The Rent budget did not consider the deferred rent adjustment to make the rent expense straight line over the life of the lease causing the favorable 19.5% budget variance.

Reconfiguring the cubicle space and adding front office signage caused the cost to be 18.4% greater than budget for office cost.

Professional Services are $354,177 less than budget because professional insurance policies were less than anticipated since Texas RE has reached an excellent experience rating. The Enforcement department did not utilize the legal fees budgeted for a potential contested case.

Laptops and computer equipment fully depreciated in 2013 and replacements were not purchased causing the 40% favorable variance in depreciation.

Indirect Expenses ($59K or 26.5% less than budget)

Indirect expense are allocated to functional departments based on FTE count.

Texas RE indirect expenses were less than budget because Non-Statutory costs were charged directly to the Non-Statutory department rather than being charged indirectly.

FIXED ASSETS

Budgeted assets were not acquired in 2013 causing budget to be 19.5% less than anticipated.

Total Budgeted Statutory expenses are under budget $1.4 million or 12.8%.

Although Texas RE ended the year $1.4 million under budget, Texas RE completed its intended activities for 2013.

Texas RE completed 33 Non-CIP audits, 10 CIP audits with CCA's, 21 CIP audits without CCA's, and 12 spot checks.

Texas RE indentified 170 non-compliance matters and completely resolved 322 violations to reduce violation caseload from 255 to 103.

86 category zero events, 7 category one, 2 category 2 and 3 category 1 events were examined.

123 technical feasibility exceptions were processed in 2013.

Texas RE verified mitigation plans or mitigation activities for 62 possible violations.

In 2013, Texas RE processed 18 new entity registrations, 23 entity removals and 9 entity name changes. Also, 2 TOP certifications and 2 reviews associated with a control center relocation was conducted.

If you have any questions on the report or the attached spreadsheet, please call me at the number below.

Thank you.

Judy Foppiano

Judy A. Foppiano, CPA
CFO & Director of Corporate Services
Texas Reliability Entity, Inc.
805 Los Cimas Parkway, Suite 200
Austin, Texas 78746
Judy.foppiano@texasre.org
512.583.4959

Texas Reliability Entity, Inc.
2013 Statutory & Non-Statutory Statement of Activities
Audited

Total Statutory & State (Non-Statutory) Combined

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)
ERO Funding			
Assessments	$ 8,152,520	$ 8,152,520	$ -
Penalty Sanctions	849,000	849,000	-
Total ERO Funding	$ 9,001,520	$ 9,001,520	$ -
Membership Fees	$ 19,250	$ 21,250	$ (2,000)
Testing Fees	1,029,100	1,029,100	-
Workshop Fees	-	32,100	(32,100)
Interest	9,076	13,910	(4,834)
Total Funding	$ 10,058,946	$ 10,097,880	$ (38,934)
Expenses			
Personnel Expenses			
Salaries	$ 6,244,320	$ 6,400,409	$ (156,089)
Payroll Taxes	425,797	569,631	(143,834)
Employee Benefits	732,467	943,487	(211,020)
Savings & Retirement	813,224	898,812	(85,588)
Total Personnel Expenses	$ 8,215,808	$ 8,812,339	$ (596,531)
Meeting & Travel Expenses			
Meetings	$ 32,157	$ 38,316	$ (6,159)
Travel	305,399	359,999	(54,600)
Conference Expenses	22,324	18,540	3,784
Total Meeting & Travel Expenses	$ 359,880	$ 416,855	$ (56,975)
Operating Expenses			
Consultants & Contracts	$ 349,113	$ 433,131	$ (84,018)
Rent & Improvements	465,778	533,930	(68,152)
Office Costs	450,428	374,638	75,790
Professional Services	544,911	905,000	(360,089)
Depreciation	672,285	888,000	(215,715)
Total Operating Expenses	$ 2,482,514	$ 3,134,699	$ (652,185)
Indirect Expenses	-	-	-
Total Expenses	$ 11,058,202	12,363,893.00	(1,305,691.00)
Change in Assets	(999,256)	(2,266,013)	1,266,757
Fixed Assets			
Depreciation	$ (672,285)	$ (888,000)	215,715
Computer & Software CapEx	208,176	410,750	(202,574)
Equipment CapEx	2,523	78,238	(75,715)
Incr(Dec) in Fixed Assets	$ (461,586)	$ (399,012)	$ (62,574)
Allocation of Fixed Assets	$ -	$ -	$ -
Total Inc(Dec) in Fixed Assets	$ (461,586)	$ (399,012)	$ (62,574)
TOTAL BUDGET	$ 10,596,616	$ 11,964,881	$ (1,368,265)
Change in Working Captial	$ (537,670)	$ (1,867,001)	$ 1,329,331
FTE's	61	65	-4

Texas Reliability Entity, Inc.
2013 Statutory Statement of Activities
Audited

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
ERO Funding					
Assessments	$ 8,152,520	$ 8,152,520	$ -	0%	
Penalty Sanctions	849,000	849,000	-	0%	
Total ERO Funding	$ 9,001,520	$ 9,001,521	$ -	0%	
Membership Fees	$ 19,250	$ 21,250	$ (2,000)	-9.4%	
Workshop Fees	-	32,100	(32,100)	-100.0%	No fees were charged for the workshops held in 2013. Registered Entities hosted the workshops; therefore, no need to charge fees to attend
Interest	7,929	13,910	(5,981)	-43.0%	
Total Funding	$ 9,028,699	$ 9,068,781	$ (40,081)	-0.4%	
Expenses					
Personnel Expenses					
Salaries	$ 5,713,409	$ 5,858,856	$ (145,447)	-2.5%	Vacancies and timing of new hires
Payroll Taxes	388,927	523,255	(134,328)	-25.7%	Directly related to staff vacancies
Employee Benefits	669,926	868,322	(198,396)	-22.8%	Directly related to staff vacancies
Savings & Retirement	742,894	818,519	(75,625)	-9.2%	Directly related to staff vacancies
Total Personnel Expenses	$ 7,515,155	$ 8,068,952	$ (553,797)	-6.9%	
Meeting & Travel Expenses					
Meetings	$ 32,157	$ 38,316	$ (6,159)	-16.1%	Workshops hosted by Registered Entities
Travel	304,384	348,000	(43,616)	-12.5%	Standards and Compliance did not require as much travel as budgeted
Conference Expenses	22,324	18,540	3,784	20.4%	
Total Meeting & Travel Expenses	$ 358,865	$ 404,856	$ (45,991)	-11.4%	
Operating Expenses					
Consultants & Contracts	$ 345,280	$ 415,000	$ (69,720)	-16.8%	Contract costs related to implementing the Sharepoint project were not used; the IT staff performed some of the tasks originally planned for the consultant
Rent & Improvements	429,751	533,930	(104,179)	-19.5%	Adjustment for deferred rent not considered in the budget
Office Costs	425,991	359,684	66,307	18.4%	
Professional Services	534,108	888,225	(354,117)	-39.9%	Professional insurance policies were less than anticipated since Texas RE has shown an excellent experience rating over the past three years. The budgeted legal services budgeted in the Enforcement Department for a potential contested case were not utilized in 2013.
Depreciation	532,066	888,000	(355,934)	-40.1%	Costs related to replacement laptops, software and server equipment have not been incurred, resulting in a 40.1% variance for depreciation.
Total Operating Expenses	$ 2,267,196	$ 3,084,839	$ (817,643)	-26.5%	
Indirect Expenses	189,349	(223,856)	413,205	-184.6%	Allocated to functional departments based on FTE count
Total Expenses	$ 10,330,564	11,334,791	(1,004,227)	-8.9%	
Change in Assets	(1,301,865)	(2,266,010)	964,145	-42.5%	
Fixed Assets					
Depreciation	$ (532,066)	$ (888,000)	$ 355,934	-40.1%	
Computer & Software CapEx	208,176	410,750	(202,574)	-49.3%	
Equipment CapEx	2,523	78,238	(75,715)	-96.8%	
Incr(Dec) in Fixed Assets	$ (321,367)	$ (399,012)	$ 77,645	-19.5%	
Allocation of Fixed Assets	$ -	$ -	$ -	0.0%	
Total Inc(Dec) in Fixed Assets	$ (321,367)	$ (399,012)	$ 77,645	-19.5%	
TOTAL BUDGET	$ 10,009,197	$ 10,935,779	$ (926,583)	-8.5%	
Change in Working Captial	$ (980,498)	$ (1,866,998)	$ 886,500	-47.5%	
FTE's	56.2	60.0	-3.8		

Texas Reliability Entity, Inc.
2013 Statement of Activities
Audited

RELIABILITY STANDARDS

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
ERO Funding					
Assessments	$ 406,288	$ 406,288	$ -	0%	
Penalty Sanctions	34,477	34,477	-	0%	
Total ERO Funding	$ 440,765	$ 440,765	$ -	0%	
Membership Fees	$ -	$ 863	$ (863)	-100%	Did not allocate membership fees to programs
Total Funding	$ 440,765	$ 441,628	$ (863.00)	0%	
Expenses					
Personnel Expenses					
Salaries	$ 125,229	$ 217,122	$ (91,893)	-42%	Vacancies, employee turnover & timing of New hires
Payroll Taxes	7,340	19,923	(12,583)	-63%	Directly related to staff vacancies.
Employee Benefits	12,246	26,197	(13,951)	-53%	Directly related to staff vacancies.
Savings & Retirement	16,181	32,191	(16,010)	-50%	Directly related to staff vacancies.
Total Personnel Expenses	$ 160,996	$ 295,433	$ (134,437)	-46%	
Meeting & Travel Expenses					
Meetings	$ 583	$ -	$ 583	100%	
Travel	4,555	10,835	(6,280)	-58%	Less Travel required to attend meetings than budgeted
Total Meeting & Travel Expenses	$ 5,138	$ 10,835	$ (5,697)	-53%	
Operating Expenses					
Consultants & Contracts	$ 7,957	$ 12,276	$ (4,319)	-35%	webVote Service Solution canceled
Office Costs	860	485	375	77%	
Total Operating Expenses	$ 8,817	$ 12,761	$ (3,944)	-31%	
Indirect Expenses	135,517	131,461	4,056	3%	Allocated to functional departments based on FTE count
Total Expenses	$ 310,467	450,490	(140,023)	-31%	
Change in Assets	130,298	(8,862)	139,160	-1570%	
Fixed Assets					
Incr(Dec) in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	$ -	$ (8,862)	$ 8,862	-100%	
Total Inc(Dec) in Fixed Assets	$ -	$ (8,862)	$ 8,862	-100%	
TOTAL BUDGET	$ 310,467	$ 441,628	$ (131,161)	-30%	
Change in Working Captial	$ 130,298	$ -	$ 130,298		
FTE's	1.5	2.0	(0.50)		

Texas Reliability Entity, Inc.
2013 Statement of Activities
Audited

COMPLIANCE OPERATIONS, ENFORCEMENT and ORGANIZATION REGISTRATION

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
ERO Funding					
Assessments	$ 8,079,155	$ 8,079,155	$ -	0%	
Penalty Sanctions	689,543	689,543	-	0%	
Total ERO Funding	$ 8,768,698	$ 8,768,698	$ -	0%	
Membership Fees	$ -	$ 17,259	$ (17,259)	-100%	Did not allocate membership fees to programs
Total Funding	$ 8,768,698	$ 8,785,957	$ (17,259)	0%	
Expenses					
Personnel Expenses					
Salaries	$ 3,494,378	$ 3,854,415	$ (360,037)	-9%	Vacancies, employee turnover & timing of New hires
Payroll Taxes	246,514	343,884	(97,370)	-28%	Directly related to staff vacancies.
Employee Benefits	404,569	589,125	(184,556)	-31%	Directly related to staff vacancies.
Savings & Retirement	463,227	571,470	(108,243)	-19%	Directly related to staff vacancies.
Total Personnel Expenses	$ 4,608,688	$ 5,358,894	$ (750,206)	-14%	
Meeting & Travel Expenses					
Meetings	$ 383	$ -	$ 383	100%	
Travel	166,100	222,964	(56,864)	-26%	Less Travel for audits and meetings
Total Meeting & Travel Expenses	$ 166,483	$ 222,964	$ (56,481)	-25%	
Operating Expenses					
Consultants & Contracts	$ 201,688	$ 274,815	$ (73,128)	-27%	CIP consultant not utilized
Office Costs	10,867	15,562	(4,695)	-30%	Telephone charges lower than budgeted
Professional Services	64,174	311,224	(247,050)	-79%	Outside legal for contested case not utilized
Depreciation	-	331,292	(331,292)	-100%	Depreciation actual charged to G&A
Total Operating Expenses	$ 276,728	$ 932,893	$ (656,165)	-70%	
Indirect Expenses	3,162,052	2,629,226	532,826	20%	Allocated to functional departments based on FTE count
Total Expenses	$ 8,213,951	$ 9,143,977	$ (930,026)	-10%	
Change in Assets	554,747	(358,020)	912,767	-255%	
Fixed Assets					
Depreciation	$ -	$ (331,292)	$ 331,292	-100%	Depreciation actually charged to IT and G&A
Computer & Software CapEx	-	150,537	(150,537)	-100%	Assets budgeted not purchased
Incr(Dec) in Fixed Assets	$ -	$ (180,755)	$ 180,755	-100%	
Allocation of Fixed Assets	$ -	$ (177,265)	$ 177,265	-100%	
Total Inc(Dec) in Fixed Assets	$ -	$ (358,020)	$ 358,020	-100%	
TOTAL BUDGET	$ 8,213,951	$ 8,785,957	$ (572,006)	-7%	
Change in Working Captial	$ 554,747	$ -	$ 554,747		
FTE's	35.0	40.0	-5.0		

Texas Reliability Entity, Inc.
2013 Statement of Activities
Audited

RELIABILITY ASSESSMENTS and PERFORMANCE ANALYSIS

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
ERO Funding					
Assessments	$ 1,047,067	$ 1,047,067	$ -	0%	
Penalty Sanctions	81,883	81,883	-	0%	
Total ERO Funding	$ 1,128,950	$ 1,128,950	$ -	0%	
Membership Fees	$ -	$ 2,049	$ (2,049)	-100%	Did not allocate membership fees to programs
Total Funding	$ 1,128,950	$ 1,131,000	$ (2,049.00)	0%	
Expenses					
Personnel Expenses					
Salaries	$ 628,266	$ 590,909	$ 37,357	6%	
Payroll Taxes	41,725	50,393	(8,668)	-17%	Error in budget allocation to payroll taxes
Employee Benefits	77,687	77,259	428	1%	
Savings & Retirement	84,941	87,610	(2,669)	-3%	
Total Personnel Expenses	$ 832,619	$ 806,171	$ 26,448	3%	
Meeting & Travel Expenses					
Meetings	$ 1,913	$ -	$ 1,913	100%	
Travel	39,616	33,658	5,958	18%	
Total Meeting & Travel Expenses	$ 41,529	$ 33,658	$ 7,871	23%	
Operating Expenses					
Consultants & Contracts	$ 1,050	$ -	$ 1,050	100%	
Office Costs	36,367	-	36,367	100%	PI software maintenance was not budgeted in 2013
Professional Services	300	-	300	100%	
Total Operating Expenses	$ 37,717	$ -	$ 37,717		
Indirect Expenses	406,550	312,221	94,329	30%	Allocated to functional departments based on FTE count
Total Expenses	$ 1,318,415	$ 1,152,050	$ 166,365	14%	
Change in Assets	(189,465)	(21,050)	(168,415)	800%	
Fixed Assets					
Incr(Dec) in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	$ -	$ (21,050)	$ 21,050	-100%	
Total Inc(Dec) in Fixed Assets	$ -	$ (21,050)	$ 21,050	-100%	
TOTAL BUDGET	$ 1,318,415	$ 1,131,000	$ 187,415	17%	
Change in Working Captial	$ (189,465)	$ -	$ (189,465)		
FTE's	4.5	4.75	(0.25)		

Texas Reliability Entity, Inc.
2013 Statement of Activities
Audited

TRAINING, EDUCATION and OPERATOR CERTIFICATION

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
ERO Funding					
Assessments	$ 315,477	$ 315,477	$ -	0%	
Penalty Sanctions	30,168	30,168	-	0%	
Total ERO Funding	$ 345,645	$ 345,645	$ -	0%	
Membership Fees	$ -	$ 755	$ (755)	-100%	Did not allocate membership fees to programs
Workshop Fees	-	32,100	(32,100)	-100%	No fees were charged for the workshops. Registered Entities hosted the workshops; therefore, no need to charge fees to attend.
Total Funding	$ 345,645	$ 378,500	$ (32,855)	-9%	
Expenses					
Personnel Expenses					
Salaries	$ 114,833	$ 172,183	$ (57,351)	-33%	Less than anticipated staff involvement in the workshops
Payroll Taxes	10,128	15,167	(5,039)	-33%	
Employee Benefits	17,728	27,147	(9,418)	-35%	
Savings & Retirement	17,980	25,529	(7,550)	-30%	
Total Personnel Expenses	$ 160,668	$ 240,026	$ (79,357)	-33%	
Meeting & Travel Expenses					
Meetings	$ 14,697	$ 30,900	$ (16,203)	-52%	Registered Entities hosted meetings requiring less cost to Texas RE.
Travel	2,116	300	1,816	605%	
Conference Expenses	11,008	-	11,008	100%	Utilizing online meetings that was not included in the budget
Total Meeting & Travel Expenses	$ 27,821	$ 31,200	$ (3,379)	-11%	
Operating Expenses					
Consultants & Contracts	$ 350	$ -	$ 350	100%	
Office Costs	1,933	-	1,933	100%	
Total Operating Expenses	$ 2,283	$ -	$ 2,283	100%	
Indirect Expenses	158,103	115,029	43,074	37%	Allocated to functional departments based on FTE count
Total Expenses	$ 348,875	$ 386,255	$ (37,379)	-10%	
Change in Assets	(3,230)	(7,755)	4,524	-58%	
Fixed Assets					
Incr(Dec) in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets	$ -	$ (7,755)	$ 7,755	-100%	
Total Inc(Dec) in Fixed Assets	$ -	$ (7,755)	$ 7,755	-100%	
TOTAL BUDGET	$ 348,875	$ 378,500	$ (29,624)	-8%	
Change in Working Captial	$ (3,230)	$ 0	$ (3,231)		
FTE's	1.75	1.75	$ -		

Texas Reliability Entity, Inc.
2013 Statement of Activities
Audited

SITUATION AWARENESS and INFRASTRUCTURE SECURITY

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
ERO Funding					
Assessments	$ 185,443	$ 185,443	$ -	0%	
Penalty Sanctions	12,929	12,929	-	0%	
Total ERO Funding	$ 198,372	$ 198,372	$ -	0%	
Membership Fees	$ -	$ 324	$ (324)	-100%	
Total Funding	$ 198,372	$ 198,696	$ (324.00)	0%	
Expenses					
Personnel Expenses					
Salaries	$ 51,624	$ 111,829	$ (60,205)	-54%	Less time charged to SAIS than anticipated in the budget
Payroll Taxes	3,739	9,921	(6,182)	-62%	Directly related to salary variance
Employee Benefits	5,878	13,128	(7,250)	-55%	Directly related to salary variance
Savings & Retirement	7,594	16,580	(8,986)	-54%	Directly related to salary variance
Total Personnel Expenses	$ 68,834	$ 151,458	$ (82,624)	-55%	
Meeting & Travel Expenses					
Travel	2,314	1,263	1,051	83%	
Total Meeting & Travel Expenses	$ 2,314	$ 1,263	$ 1,051	83%	
Operating Expenses					
Office Costs	-	-	-		
Total Operating Expenses	$ -	$ -	$ -		
Indirect Expenses	67,758	49,298	18,460	37%	
Total Expenses	$ 138,907	$ 202,019	$ (63,112)	-31%	
Change in Assets	59,465	(3,323)	62,788	-1890%	
Fixed Assets					
Incr(Dec) in Fixed Assets	$ -	$ -	$ -		
Allocation of Fixed Assets		$ (3,324)	$ 3,324	-100%	
Total Inc(Dec) in Fixed Assets	$ -	$ (3,324)	$ 3,324	-100%	
TOTAL BUDGET	$ 138,907	$ 198,695	$ (59,788)	-30%	
Change in Working Captial	$ 59,465	$ 1	$ 59,464		
FTE's	0.75	0.75	-		

Texas Reliability Entity, Inc.
2013 Statement of Activities
Audited

GENERAL and ADMINISTRATIVE

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
ERO Funding					
Assessments	$ (1,880,909)	$ (1,880,909)	$ -	0%	
Penalty Sanctions	-	-	-		
Total ERO Funding	$ (1,880,909)	$ (1,880,909)	$ -	0%	
Membership Fees	$ 19,250	$ -	$ 19,250	100%	Budgeted to programs, actual charged to G&A
Interest	7,929	13,910	(5,981)	-43%	
Total Funding	$ (1,853,730)	$ (1,866,999)	$ 13,269	-1%	
Expenses					
Personnel Expenses					
Salaries	$ 257,293	$ 189,676	$ 67,617	36%	Salary expense was recorded to G & A by the Legal team for time spent filling an open position in G & A.
Payroll Taxes	11,887	17,678	(5,791)	-33%	Error in budget allocation to payroll taxes
Employee Benefits	25,273	26,158	(884)	-3%	
Savings & Retirement	23,659	17,890	5,769	32%	More employees participated in the retirment plan than in prior years
Total Personnel Expenses	$ 318,113	$ 251,402	$ 66,712	27%	
Meeting & Travel Expenses					
Meetings	$ 2,798	$ 6,180	$ (3,382)	-55%	
Travel	57,124	54,851	2,273	4%	
Conference Expenses	(776)	-	(776)	-100%	
Total Meeting & Travel Expenses	$ 59,145	$ 61,031	$ (1,886)	-3%	
Operating Expenses					
Consultants & Contracts	$ 23,811	$ 2,981	$ 20,830	699%	Regional Assessments Project not budgeted
Rent & Improvements	423,265	533,930	(110,665)	-21%	Deferred rent not considered in budget for straight line cost.
Office Costs	54,681	31,369	23,312	74%	Office space adjusted and new signage
Professional Services	264,016	325,000	(60,984)	-19%	BOD fees less than anticipated
Depreciation	532,066	193,376	338,690	175%	Depreciation expenses charged to G&A. The overage was offset by under-spending in Compliance
Total Operating Expenses	$ 1,297,839	$ 1,086,656	$ 211,183	19%	
Indirect Expenses	(1,675,097)	(1,399,089)	(276,008)	20%	Allocated to functional departments based on FTE count
Total Expenses	$ -	$ 0	$ (0)	-100%	
Change in Assets	(1,853,730)	(1,866,999)	13,269	-1%	
Fixed Assets					
Depreciation	$ (532,066)	$ (193,376)	(338,690)	175%	
Equipment CapEx	2,523	78,238	(75,715)	-97%	
Incr(Dec) in Fixed Assets	$ (529,543)	$ (115,138)	$ (414,405)	360%	
Allocation of Fixed Assets		$ 115,138	$ (115,138)	-100%	Allocated to functional departments based on FTE count
Total Inc(Dec) in Fixed Assets	$ (529,543)	$ -	$ (529,543)	100%	
TOTAL BUDGET	$ (529,543)	0	$ (529,543)	100%	
Change in Working Captial	$ (1,324,187)	$ (1,866,999)	$ 542,812	-29%	
FTE's	1.75	1.75	-		

Texas Reliability Entity, Inc.
2013 Statement of Activities
Audited

LEGAL and REGULATORY

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
ERO Funding					
Total ERO Funding	$ -	$ -	$ -		
Total Funding	$ -	$ -	$ -		
Expenses					
Personnel Expenses					
Salaries	$ 463,471	$ 307,265	$ 156,206	51%	Due to workload, FTE's charged more hours to Legal than budgeted
Payroll Taxes	28,977	28,524	453	2%	
Employee Benefits	55,623	47,924	7,700	16%	Additional training for legal staff
Savings & Retirement	53,108	25,093	28,015	112%	Employees participation in retirement plan more than anticipated
Total Personnel Expenses	$ 601,179	$ 408,806	$ 192,373	47%	
Meeting & Travel Expenses					
Travel	10,791	11,172	(381)	-3%	
Total Meeting & Travel Expenses	$ 10,791	$ 11,172	$ (381)	-3%	
Operating Expenses					
Consultants & Contracts	$ 3,475	$ 2,211	$ 1,264	57%	
Office Costs	3,635	2,415	1,220	51%	
Professional Services	-	17,577	(17,577)	-100%	Outside legal services not utilized
Total Operating Expenses	$ 7,110	$ 22,203	$ (15,093)	-68%	
Indirect Expenses	(619,080)	(442,181)	(176,900)	40%	
Total Expenses	$ -	$ -	$ -		
Change in Assets	-	-	-		
TOTAL BUDGET	$ -	$ -	$ -	0%	
Change in Working Captial	$ -	$ -	$ -	0%	
FTE's	3.57	3.00	0.57		

Texas Reliability Entity, Inc.
2013 Statement of Activities
Audited

INFORMATION TECHNOLOGY

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
ERO Funding					
Total ERO Funding	$ -	$ -	$ -		
Total Funding	$ -	$ -	$ -		
Expenses					
Personnel Expenses					
Salaries	$ 316,631	$ 215,903	$ 100,728	47%	Additional FTE due to workload
Payroll Taxes	23,456	19,525	3,931	20%	Directly related to Salary variance
Employee Benefits	44,497	34,005	10,492	31%	Directly related to additional FTE and salary expenses
Savings & Retirement	45,178	21,779	23,399	107%	Directly related to additional FTE and salary expenses, employees participation greater than anticipated for retirement plan
Total Personnel Expenses	$ 429,761	$ 291,211	$ 138,550	48%	
Meeting & Travel Expenses					
Meetings	$ 1,511	$ 1,236	$ 275	22%	
Travel	10,832	10,000	832	8%	
Conference Expenses	12,092	18,540	(6,448)	-35%	
Total Meeting & Travel Expenses	$ 24,436	$ 29,776	$ (5,340)	-18%	
Operating Expenses					
Consultants & Contracts	$ 79,407	$ 84,562	$ (5,155)	-6%	
Rent & Improvements	6,486	-	6,486	100%	
Office Costs	287,394	267,721	19,673	7%	
Professional Services	54,777	54,424	353	1%	
Depreciation	-	363,332	(363,332)	-100%	Depreciation charged to G &A, allocated to functional departments
Total Operating Expenses	$ 428,064	$ 770,039	$ (341,975)	-44%	
Indirect Expenses	(882,261)	(1,091,026)	208,765	-19%	
Total Expenses	$ -	$ -	$ -		
Change in Assets	-	-	-		
Fixed Assets					
Depreciation	$ -	$ (363,332)	$ 363,332	-100%	Depreciation charged to G &A, allocated to functional departments
Computer & Software CapEx	208,176	260,213	(52,037)	-20%	
Furniture & Fixture CapEx	-	-	0	0%	
Equipment CapEx	-	-	0	0%	
Leasehold Improvement CapEx	-	-	0	0%	
Incr(Dec) in Fixed Assets	$ 208,176	$ (103,119)	$ 311,295	-302%	
Allocation of Fixed Assets	$ -	$ 103,119	$ (103,119)	-100%	
Total Inc(Dec) in Fixed Assets	$ 208,176	$ -	$ 208,176	0%	
TOTAL BUDGET	$ 208,176	$ -	$ 208,176	0%	
Change in Working Captial	$ (208,176)	$ -	$ (208,176)	0%	
FTE's	3.81	2.50	1.31		

Texas Reliability Entity, Inc.
2013 Statement of Activities
Audited

HUMAN RESOURCES

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
ERO Funding					
Total ERO Funding	$ -	$ -	$ -		
Total Funding	$ -	$ -	$ -		
Expenses					
Personnel Expenses					
Salaries					
Payroll Taxes					
Employee Benefits					
Savings & Retirement					
Total Personnel Expenses	$ -	$ -	$ -	0%	
Meeting & Travel Expenses					
Meetings	$ 9,136	$ -	$ 9,136	100%	Staff meetings and team building events not budgeted
Travel	8,788	1,358	7,430	547%	Travel for job applicants & consultants
Total Meeting & Travel Expenses	$ 17,925	$ 1,358	$ 16,567	1220%	
Operating Expenses					
Consultants & Contracts	$ 24,692	$ 28,617	$ (3,925)	-14%	
Office Costs	3,234	280	2,954	1055%	
Professional Services	55,843	20,000	35,843	179%	Unbudgeted VP recruiting service
Total Operating Expenses	$ 83,769	$ 48,897	$ 34,872	71%	
Indirect Expenses	(101,693)	(50,255)	(51,438)	102%	
Total Expenses	$ -	$ -	$ -		
Change in Assets	-	-	-		
TOTAL BUDGET	$ -	$ -	$ -	0%	
Change in Working Captial	$ -	$ -	$ -	100%	
FTE's	1.0	1.0	0.0		

Texas Reliability Entity, Inc.
2013 Statement of Activities
Audited

ACCOUNTING and FINANCE

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
ERO Funding					
Total ERO Funding	$ -	$ -	$ -		
Total Funding	$ -	$ -	$ -		
Expenses					
Personnel Expenses					
Salaries	$ 254,958	$ 199,554	$ 55,404	28%	Additional FTE
Payroll Taxes	16,675	18,240	(1,565)	-9%	
Employee Benefits	28,980	27,380	1,600	6%	
Savings & Retirement	33,684	20,378	13,306	65%	Employee contributions increased resulting in the matching retirement being greater than budgeted.
Total Personnel Expenses	$ 334,296	$ 265,552	$ 68,744	26%	
Meeting & Travel Expenses					
Meetings	$ 1,135	$ -	$ 1,135		
Travel	2,200	1,598	602	38%	
Total Meeting & Travel Expenses	$ 3,335	$ 1,598	$ 1,737	109%	
Operating Expenses					
Consultants & Contracts	$ 2,850	$ 9,539	$ (6,689)	-70%	Did not use consultant as budgeted, offset by additional FTE
Office Costs	27,019	41,852	(14,833)	-35%	Property taxes less than budgeted
Professional Services	94,998	160,000	(65,002)	-41%	Insurance policies were less than anticipated since TRE has shown an excellent experience rating over the past three years
Total Operating Expenses	$ 124,867	$ 211,391	$ (86,524)	-41%	
Indirect Expenses	(462,498)	(478,541)	16,043	-3%	
Total Expenses	$ -	$ (0)	$ 0	-100%	
Change in Assets	-	0	(0)	-100%	
TOTAL BUDGET	$ -	$ (0)	$ 0	-100%	
Change in Working Captial	$ -	$ 0	$ (0)	-100%	
FTE's	2.52	2.00	0.52		

Texas Reliability Entity, Inc.
2013 Statement of Activities
Audited

STATE (NON-STATUTORY)

Funding	2013 Actual	2013 Budget	Variance from Budget Over(Under)		Comments (Explain variances > +/- 10% and $10,000)
ERO Funding					
Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	$ -	$ -	$ -		
PUCT	$ 1,029,100	$ 1,029,100	$ -	0%	
Interest	1,147	-	1,147	100%	
Total Funding	$ 1,030,247	$ 1,029,100	$ 1,147	0%	
Expenses					
Personnel Expenses					
Salaries	$ 530,912	$ 541,553	$ (10,641)	-2%	
Payroll Taxes	36,870	46,376	(9,506)	-20%	
Employee Benefits	62,541	75,164	(12,623)	-17%	Employee participation in benefits less than anticipated
Savings & Retirement	70,331	80,292	(9,961)	-12%	Employee participation in retirement plan less than anticipated
Total Personnel Expenses	$ 700,653	$ 743,385	$ (42,732)	-6%	
Meeting & Travel Expenses					
Meetings	$ -	$ -	$ -		
Travel	1,015	12,000	(10,985)	-92%	Travel less than anticipated for Protocol group
Conference Expenses	-	-	-		
Total Meeting & Travel Expenses	$ 1,015	$ 12,000	$ (10,985)	-92%	
Operating Expenses					
Consultants & Contracts	$ 3,833	$ 18,130	$ (14,297)	-79%	
Rent & Improvements	36,026	-	36,026		Rent charged directly, no indirect costs
Office Costs	24,438	14,954	9,484	63%	Costs charged directly, no indirect costs
Professional Services	10,804	16,775	(9,054)	-54%	Costs charged directly, no indirect costs
Depreciation	140,219	-	140,219		Costs charged directly, no indirect costs
Total Operating Expenses	$ 215,319	$ 49,859	$ 165,460	326%	
Indirect Expenses	-	223,856	(223,856)	-100%	
Total Expenses	$ 916,988	1,029,100	(112,112)	-11%	
Change in Assets	113,260	-	113,260		
Fixed Assets					
Depreciation	$ (140,219)	$ -	$ (140,219)	0%	
Incr(Dec) in Fixed Assets	$ (140,219)	$ -	$ (140,219)		
Allocation of Fixed Assets	$ -	$ -	$ -	0%	
Total Inc(Dec) in Fixed Assets	$ (140,219)	$ -	$ (140,219)	0%	
TOTAL BUDGET	$ 776,769	$ 1,029,100	$ (252,331)	-25%	
Change in Working Captial	$ 253,479	$ -	$ 253,479	0%	
FTE's	5.0	5.0	0.0		

Texas Reliability Entity, Inc.
Penalty Sanctions
For year ended December 31, 2013

Date Rec'd		Amount	Year to Recognize for BP&B				
			2011	2012	2013	2014	2015
		$ 20,000.00	$ 20,000.00				
		198,600.00		$ 198,600.00			
		150,000.00		150,000.00			
		28,000.00		28,000.00			
		18,000.00		18,000.00			
		3,000.00		3,000.00			
		35,000.00		35,000.00			
		900.00		900.00			
		900.00		900.00			
		900.00		900.00			
		900.00		900.00			
		900.00		900.00			
		2,500.00		2,500.00			
		50,000.00		50,000.00			
		3,000.00		3,000.00			
		12,000.00		12,000.00			
		4,000.00		4,000.00			
		16,000.00		16,000.00			
		9,000.00		9,000.00			
		11,000.00		11,000.00			
		6,000.00		6,000.00			
		1,230.00		1,230.00			
		8,000.00		8,000.00			
		5,000.00		5,000.00			
		3,000.00		3,000.00			
		5,000.00		5,000.00			
		22,000.00			22,000.00		
		2,000.00			2,000.00		
		3,000.00			3,000.00		
		7,000.00			7,000.00		
		107,000.00			107,000.00		
		8,000.00			8,000.00		
		45,000.00			45,000.00		
		13,000.00			13,000.00		
		7,000.00			7,000.00		
		7,000.00			7,000.00		
		5,000.00			5,000.00		
		11,000.00			11,000.00		
		12,000.00			12,000.00		
		384,000.00			384,000.00		
	Subtotal 2011	**$ 1,225,830.00**					
		8,500.00			8,500.00		
		10,000.00			10,000.00		
		18,000.00			18,000.00		
		13,000.00			13,000.00		
		21,000.00			21,000.00		
		9,000.00			9,000.00		
		40,000.00			40,000.00		
		30,000.00			30,000.00		
		32,500.00			32,500.00		
		2,000.00			2,000.00		
		15,000.00			15,000.00		
7/19/2012		1,000.00				1,000.00	
7/31/2012		9,000.00				9,000.00	
8/8/2012		14,333.00				14,333.00	
8/20/2012		8,000.00				8,000.00	
8/20/2012		25,000.00				25,000.00	
8/20/2012		50,000.00				50,000.00	
8/20/2012		50,000.00				50,000.00	
9/17/2012		14,000.00				14,000.00	
10/16/2012		7,000.00				7,000.00	
11/30/2012		7,000.00				7,000.00	
11/30/2012		13,500.00				13,500.00	
12/21/2012		17,000.00				17,000.00	
12/21/2012		13,250.00				13,250.00	
12/21/2012		13,250.00				13,250.00	
12/21/2012		6,500.00				6,500.00	
	Subtotal 2012	**$ 447,833.00**					
1/30/2013		6,000.00				6,000.00	
2/28/2013		51,000.00				51,000.00	
2/28/2013		10,000.00				10,000.00	
3/8/2013		32,000.00				32,000.00	
4/29.2013		30,000.00				30,000.00	
5/10/2013		25,000.00				25,000.00	
6/4/2013		10,000.00				10,000.00	
6/4/2013		7,000.00				7,000.00	
7/10/2013		137,000.00					137,000.00
7/10/2013		200,000.00					200,000.00
9/3/2013		9,000.00					9,000.00
9/6/2013		38,000.00					38,000.00
10/1/2013		12,000.00					12,000.00
10/1/2013		4,800.00					4,800.00
10/1/2013		15,000.00					15,000.00
10/1/2013		17,200.00					17,200.00
10/1/2013		12,000.00					12,000.00
12/19/2013		19,000.00					19,000.00
	Subtotal 2013	**$ 635,000.00**					
		$ 2,308,663.00	**$ 20,000.00**	**$ 572,830.00**	**$ 832,000.00**	**$ 419,833.00**	**$ 464,000.00**

Texas RE 2013 Penalties Reconciliation	12/31/2013	12/31/2012	Change in 2013
Total Cumulative Penalties - GAAP/BKD Audit	$ 2,308,663.00	$ 1,673,663.00	$ 635,000.00
Total Cumulative Penalties - True Up Report	1,424,830.00	592,830.00	832,000.00
	$ 883,833.00	**$ 1,080,833.00**	**$ (197,000.00)**

Texas RE's auditited financial statements include penalties recorded as earned revenue at the time of invoicing, in accordance with GAAP.
Texas RE's true up rerporet includes only those penalties included in the approved budgtet for the calendar year, as shown above.

Texas Reliability Entity, Inc.

Auditor's Report and Financial Statements

December 31, 2013 and 2012

BKD LLP
CPAs & Advisors

Texas Reliability Entity, Inc.

December 31, 2013 and 2012

Contents

Independent Auditor's Report..... 1

Financial Statements

Statements of Financial Position 3

Statements of Activities..... 4

Statements of Cash Flows 5

Notes to Financial Statements 6

Other Information

Schedule of Statutory and Nonstatutory Operating Activities 15

BKD LLP
CPAs & Advisors

14241 Dallas Parkway, Suite 1100 // Dallas, TX 75254-2961
972.702.8262 // fax 972.702.0673 // bkd.com

Independent Auditor's Report

Board of Directors
Texas Reliability Entity, Inc.
Austin, Texas

We have audited the accompanying financial statements of Texas Reliability Entity, Inc. (Texas RE), which comprise the statements of financial position as of December 31, 2013 and 2012, and the related statements of activities and cash flows for the years then ended, and the related notes to the financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Praxity MEMBER GLOBAL ALLIANCE OF INDEPENDENT FIRMS

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of Texas Reliability Entity, Inc. as of December 31, 2013 and 2012, and the changes in its net assets and its cash flows for the years then ended in accordance with accounting principles generally accepted in the United States of America.

Emphasis of Matter

As discussed in *Note 8* to the financial statements in 2013, the entity has elected to change its method of accounting of fines and penalties in 2013. Our opinion is not modified with respect to this matter.

Other Information

Our audit was conducted for the purpose of forming an opinion on the financial statements as a whole. The Schedule of Statutory and Nonstatutory Operating Activities is presented for purposes of additional analysis and is not a required part of the financial statements. Such information has not been subjected to the auditing procedures applied in the audit of the financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

BKD, LLP

Dallas, Texas
April 23, 2014

Texas Reliability Entity, Inc.
Statements of Financial Position
December 31, 2013 and 2012

Assets

	2013	2012 *(Restated - Note 7)*
Current Assets		
Cash	$ 4,697,098	$ 5,400,125
Assets limited to use – cash	887,078	1,083,012
	5,584,176	6,483,137
Accounts receivable	-	3,766
Other current assets	239,140	298,910
Total current assets	5,823,316	6,785,813
Property and Equipment, Net	602,903	1,191,777
Total assets	$ 6,426,219	$ 7,977,590

Liabilities and Net Assets

Current Liabilities		
Accounts payable	$ 154,575	$ 250,812
Accrued liabilities	349,460	568,789
Deferred rent	181,440	203,988
Total current liabilities	685,475	1,023,589
Unrestricted Net Assets		
Undesignated	4,853,666	5,870,989
Regulator designated	887,078	1,083,012
Total unrestricted net assets	5,740,744	6,954,001
Total liabilities and net assets	$ 6,426,219	$ 7,977,590

Texas Reliability Entity, Inc.

Statements of Activities

Years Ended December 31, 2013 and 2012

	2013	2012 (Restated - Note 7)
Revenues, Gains and Other Support		
Statutory revenue	$ 8,806,770	$ 9,972,718
Protocol revenue	1,029,100	999,100
Interest income	9,076	15,945
Total revenues, gains and other support	9,844,946	10,987,763
Expenses		
Salaries and related benefits	8,215,809	7,040,648
Facility and equipment costs	685,911	711,200
Outside services	854,729	1,421,830
Travel and meetings	359,880	323,211
Administrative and other	269,589	251,049
Depreciation	672,285	769,124
Total expenses	11,058,203	10,517,062
Change in Unrestricted Net Assets	(1,213,257)	470,701
Unrestricted Net Assets, Beginning of Year	6,954,001	6,483,300
Unrestricted Net Assets, End of Year	$ 5,740,744	$ 6,954,001

Texas Reliability Entity, Inc.

Statements of Cash Flows

Years Ended December 31, 2013 and 2012

	2013	2012 *(Restated - Note 7)*
Operating Activities		
Change in net assets	$ (1,213,257)	$ 470,701
Item not requiring cash		
Depreciation	672,285	769,124
Changes in		
Accounts receivable	3,766	(794)
Other current assets	59,770	5,922
Accounts payable	(96,237)	198,679
Deferred rent	(22,548)	(14,787)
Accrued liabilities	(219,329)	43,949
Net cash (used in) provided by operating activities	(815,550)	1,472,794
Investing Activities		
Capital expenditures for property and equipment and systems under development	(83,411)	(226,682)
Net cash used in investing activities	(83,411)	(226,682)
Net (Decrease) Increase in Cash	(898,961)	1,246,112
Cash, Beginning of Year	6,483,137	5,237,025
Cash, End of Year	$ 5,584,176	$ 6,483,137

Texas Reliability Entity, Inc.

Notes to Financial Statements

December 31, 2013 and 2012

Note 1: Organization and Operations

Texas Reliability Entity, Inc. (Texas RE) is a Texas nonprofit corporation that is tax exempt under Section 501(c)(3) of the Internal Revenue Code. Texas RE was formed January 1, 2010, to be the Regional Entity for the Electric Reliability Council of Texas, Inc. (ERCOT) region and to preserve and enhance reliability across the ERCOT region by encouraging a culture of compliance among all users, owners and operators of the bulk-power system (BPS). Texas RE, took assignment of all rights, contracts, obligations, assets and liabilities of Texas Regional Entity (which was an independent division of ERCOT, the predecessor Regional Entity), effective midnight on June 30, 2010. Texas RE became the Regional Entity for the ERCOT region on July 1, 2010, pursuant to its Amended and Restated Delegation Agreement with North American Electric Reliability Corporation (NERC), which was approved by the Federal Energy Regulatory Commission (FERC) on May 6, 2010. The Delegation Agreement with NERC was further amended effective January 1, 2011 and October 7, 2011. Texas Regional Entity was the authorized Regional Entity for the ERCOT region from May 2007 through June 30, 2010.

As Regional Entity, Texas RE proposes and facilitates development of new and modified NERC Reliability Standards and Regional Standards (Standards); monitors, assesses, investigates and enforces compliance by registered entities with Standards in the ERCOT region, and oversees the mitigation of any violations. Texas RE is authorized to impose penalties and sanctions for violations, but NERC and FERC must approve determination of all violations and the imposition of all penalties and sanctions. These Regional Entity activities are referred to herein as "statutory" activities.

The ERCOT region is the geographic area located within the state of Texas that operates under the jurisdiction of the Public Utility Commission of Texas (PUCT) and is not synchronously interconnected with any electric utilities operating outside of Texas. The ERCOT region includes approximately 200,000 square miles and 85% of Texas load.

In addition to Texas RE's statutory activities as Regional Entity, Texas RE has a contract with the PUCT and ERCOT to be the Reliability Monitor for the ERCOT region. As Reliability Monitor, Texas RE monitors, investigates and reports to the PUCT regarding compliance with state reliability rules (the reliability-based ERCOT Protocols and Operating Guides), and coordinates and assists PUCT staff with related reliability-related matters. The PUCT is responsible for the enforcement of violations of the state reliability rules. Texas RE's activities under this contract are permitted by NERC and FERC, by Exhibit E to the Delegation Agreement, and these activities are referred to herein as "nonstatutory" activities.

Texas Reliability Entity, Inc.
Notes to Financial Statements
December 31, 2013 and 2012

Membership and Governance

Texas RE has the following six membership sectors under its Bylaws:

- System Coordination and Planning: An entity that is registered with NERC as a Reliability Coordinator (RC), Balancing Authority (BA), Planning Authority (PA), Resource Planner (RP) or Interchange Authority (IA).
- Transmission and Distribution: An entity that is registered with NERC as a Transmission Owner (TO), Transmission Planner (TP), Transmission Service Provider (TSP), Distribution Provider (DP), and/or Transmission Operator (TOP) and is not a Cooperative or Municipal Utility.
- Cooperative Utility: An entity that is (a) a corporation organized under Chapter 161 of the Texas Utilities Code or a predecessor statute to Chapter 161 and operating under that chapter; (b) a corporation organized as an electric cooperative in a state other than Texas that has obtained a certificate of authority to conduct affairs in the state of Texas or (c) a cooperative association organized under Tex. Rev. Civ. Stat. 1396-50.01 or a predecessor to that statute and operating under that statute that is registered with NERC for at least one reliability function.
- Municipal Utility: An entity that owns or controls transmission or distribution facilities, owns or controls dispatchable generating facilities or provides retail electric service and is a municipally owned utility as defined in PURA §11.003 and is registered with NERC for at least one reliability function.
- Generation: An entity that is registered with NERC as a Generator Owner (GO) or Generator Operator (GOP).
- Load-Serving and Marketing: An entity that is registered with NERC as a Load-Serving Entity (LSE), a Purchasing-Selling Entity (PSE) or any newly defined NERC reliability function for demand response.

Membership in Texas RE is voluntary and open to any entity that is a user, owner or operator of the ERCOT region BPS and registered with NERC for at least one reliability function. Eligible registered entities must complete and submit a membership application, pay a nominal annual fee, which may be waived for good cause shown and comply with the Texas RE Bylaws. Any person or entity that has a direct and material interest in the BPS has a right to participate in the Texas RE Standards development process, even if not a Texas RE member.

Texas RE is governed by a hybrid board of directors (the Board), comprised of the following nine directors:

- Texas RE President and Chief Executive Officer
- Four Independent Directors

- Two Member Directors (the Chair and Vice-Chair of the Member Representatives Committee)
- Chair of the PUCT, or another PUCT Commissioner designated by the Chairman, as an ex officio nonvoting member
- Texas Public Counsel, from the Texas Office of Public Utility Counsel, as an ex officio nonvoting member

The Board's primary role is to oversee management of Texas RE, including assuring that Texas RE meets its requirements under the Bylaws and Delegation Agreement, and to elect a Chief Executive Officer to manage and be responsible for the day-to-day ongoing activities of Texas RE. The Board has one subcommittee, the Audit and Governance Committee, which is comprised of the Independent Directors.

Texas RE has two stakeholder committees, the Member Representatives Committee (MRC) and the Reliability Standards Committee (RSC). The MRC includes representatives from members in each of the six membership sectors and provides advice and recommendations to the Board on administrative, financial, reliability-related or any other matters, except for standards development issues, through its elected Chair and Vice-Chair, who serve as directors. The RSC includes representatives from the six industry sectors described above, whether or not members of Texas RE and including any entity with a direct and material interest in the ERCOT region BPS. The RSC facilitates the Regional Standards development process, coordinates the development of Regional Standards and variances with the development of national NERC Standards, and monitors, reviews, and comments on Standards under development and Standards interpretation requests.

Note 2: Summary of Significant Accounting Policies

Use of Estimates

The preparation of financial statements in conformity with accounting principles generally accepted in the United States of America requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities and disclosure of contingent assets and liabilities at the date of the financial statements and the reported amounts of revenues, expenses gains, losses and other changes in net assets during the reporting period. Actual results could differ from those estimates.

Cash

At December 31, 2013, Texas RE's cash accounts exceeded federally insured limits by approximately $5,400,000. Texas RE places its cash with a high quality financial institution, and management believes no significant risks exist with respect to uninsured balances.

Assets Limited to Use

As stipulated by NERC policies, Texas RE records fines and penalties that are required to be used in future operations as assets limited to use. Assets limited to use (maintained in a financial institution) was $887,078 and $1,083,012 at December 31, 2013 and 2012, respectively.

Revenue Recognition

Texas RE funds its statutory operations primarily from assessments NERC collects from load serving entities and pays to Texas RE in four quarterly payments, pursuant to the Delegation Agreement. Four quarterly payments were received by Texas RE, which totaled $8,152,520 and $9,503,866 from NERC during 2013 and 2012, respectively. NERC pays Texas RE at or near the beginning of each quarter. Additionally, Texas RE recognized $19,250 and $21,020 for membership dues and other miscellaneous revenue, and $635,000 and $447,832 from fines and penalties, during 2013 and 2012, respectively. Texas RE did not recognize any revenue from providing workshops in 2013; however, Texas RE recognized $3,330 from providing workshops in 2012. All statutory budgeted expenditures for Texas RE are approved by the Texas RE Board when it approves Texas RE's annual business plan and budget.

Texas RE funds its nonstatutory operations from revenues paid by ERCOT from its PUCT approved system administration fee, pursuant to the Reliability Monitor Agreement. Texas RE received revenue of $1,029,100 and $999,100 from the Reliability Monitor Agreement in 2013 and 2012, respectively, to cover operating expenses incurred by Texas RE. All nonstatutory budgeted expenditures for Texas RE are approved by the Texas RE Board when it approves Texas RE's annual business plan and budget.

Texas RE recognized revenue related to fines and penalties in the period in which they are earned (all appeals have been exhausted).

Related Party Transactions

Texas RE compensates its independent board directors, which is a common practice in the industry in which Texas RE operates. The authority to compensate its Independent Directors is specified in the Bylaws, which were approved by the Texas RE membership. Texas RE Independent Director compensation (totaling approximately $225,000 during 2013 and $190,000 during 2012) is paid monthly. In addition to their compensation, Texas RE independent board members are reimbursed for their actual expenses incurred related to their duties as a Texas RE board member.

Property and Equipment

Property and equipment are stated at cost less accumulated depreciation. Depreciation is charged to expense using the straight-line method over the estimated useful life of each asset. Assets under capital lease obligations and leasehold improvements are depreciated over the shorter of the lease term or their respective estimated useful lives. Repairs and maintenance costs are expensed when incurred.

The estimated useful lives for each major depreciable classification of property and equipment are as follows:

Equipment	5 years
Computer hardware	3 years
Computer software	5 years
Furniture and fixtures	7 years
Leasehold improvements	7.5 years

Long-lived Asset Impairment

Texas RE evaluates the recoverability of the carrying value of long-lived assets whenever events or circumstances indicate the carrying amount may not be recoverable. If a long-lived asset is tested for recoverability and the undiscounted estimated future cash flows expected to result from the use and eventual disposition of the asset is less than the carrying amount of the asset, the asset cost is adjusted to fair value and an impairment loss is recognized as the amount by which the carrying amount of a long-lived asset exceeds it fair value. No asset impairment was recognized during the years ended December 31, 2013 and 2012.

Deferred Rent

In 2010, Texas RE entered into an operating lease agreement, which contains provisions for future increases in rent payments. In accordance with accounting principles generally accepted in the United States of America, Texas RE records monthly rent expense equal to the total of payments due over the lease term divided by the number of months of the lease term. The difference between rent expense recorded and the amount paid is credited or charged to deferred rent.

Income Taxes

Texas RE is exempt from income taxes under Section 501 of the Internal Revenue Code and a similar provision of state law. However, Texas RE is subject to federal income tax on any unrelated business taxable income.

Texas RE files tax returns in the U.S. federal jurisdiction. With a few exceptions, Texas RE is no longer subject to U.S. federal examinations by tax authorities for years before 2010.

Note 3: Expenses by Functional Classification

While the statements of activities presents expenses by natural classification, Texas RE's expenses by functional classification for the years ended December 31 were as follows:

	2013	2012
Program	$ 6,942,188	$ 6,602,467
General and administrative	4,116,015	3,914,595
Total	$ 11,058,203	$ 10,517,062

Certain costs have been allocated among the program and general and management categories based on actual use or estimates made by management.

Note 4: Property and Equipment

Property and equipment at December 31 consists of:

	2013	2012
Equipment	$ 410,886	$ 408,364
Computer hardware	701,980	701,980
Computer software	1,376,992	1,168,815
Furniture	309,512	309,512
Leasehold improvement	206,521	206,521
Work in process	15,000	142,288
Total property and equipment	3,020,891	2,937,480
Less accumulated depreciation	2,417,988	1,745,703
Total property and equipment, net	$ 602,903	$ 1,191,777

Note 5: Line of Credit

On January 29, 2013, Texas RE obtained a $500,000 bank line of credit that expires in 2014. The line is not collateralized by any of Texas RE's assets and is unsecured. Interest rate varies with LIBOR plus 4.265%. At December 31, 2013, there was $0 borrowed against the line.

Note 6: Operating Leases

Texas RE leases office space, datacenter space and equipment under noncancellable agreements recorded as operating leases. Operating lease expenditures for the year ended December 31, 2013, were $395,698. The future rental payments due under operating leases are as follows through December 31, 2013:

2014	$ 547,627
2015	424,652
2016	424,652
2017	424,652
2018	270,000
	$ 2,091,583

Note 7: Employee Benefit Plans

Texas RE employees are sponsored under the Texas Reliability Entity, Inc. 401(k) Savings Plan (Plan) which is subject to the provisions of the Employee Retirement Income Security Act of 1974. The Plan utilizes a third-party administrator to assist in the administration. Employees must be 21 years of age to be eligible to participate. Texas RE matches 75% of the employee's contribution up to 6% of eligible compensation as defined in the plan document. Employees are fully vested for the Texas RE match of 75% after five years. In addition, Texas RE contributes 10% of a participant's eligible compensation as defined in the plan document. Employees are fully vested for the Texas RE contributions of 10% after three years. Employer contributions to the 401(k) plans were $813,224 and $705,777, respectively, in 2013 and 2012.

Note 8: Change in Accounting Principle

During 2013, Texas RE changed its method of recognizing fines and penalties revenue from the period they were available to be used in operations to the period in which they were earned (all appeals have been exhausted). This recognition methodology is the preferred method of NERC. As a result of this retrospective change, the 2012 financial statements have been restated as follows:

Statement of Financial Position

	2013			2012		
	As Computed Previously	As Adjusted	Effect of Change	As Originally Reported	As Adjusted	Effect of Change
Cash	$ 5,584,176	$ 4,697,098	$ (887,078)	$ 6,483,137	$ 5,400,125	$ (1,083,012)
Assets limited to use – cash	-	887,078	887,078	-	1,083,012	1,083,012
Deferred revenue	955,837	-	(955,837)	1,080,833	-	(1,080,833)
Total current liabilities	1,641,312	685,475	(955,837)	2,104,422	1,023,589	(1,080,833)
Unrestricted net assets	4,784,907	5,740,744	955,837	5,873,168	6,954,001	1,080,833

Statement of Activities

	2013			2012		
	As Computed Previously	As Adjusted	Effect of Change	As Originally Reported	As Adjusted	Effect of Change
Statutory revenue	$ 8,931,766	$ 8,806,770	$ 124,996	$10,097,716	$ 9,972,718	$ (124,998)
Change in unrestricted net assets	(1,088,261)	(1,213,257)	(124,996)	595,699	470,701	(124,998)
Unrestricted net assets, beginning of year	5,873,168	6,954,001	1,080,833	5,277,469	6,483,300	1,205,831
Unrestricted net assets, end of year	4,784,907	5,740,744	955,837	5,873,168	6,954,001	1,080,833

Statement of Cash Flows	2013			2012		
	As Computed Previously	As Adjusted	Effect of Change	As Originally Reported	As Adjusted	Effect of Change
Change in net assets	$ (1,088,261)	$ (1,213,257)	$ (124,996)	$ 595,699	$ 470,701	$ (124,998)
Decrease in deferred revenue	(124,996)	-	124,996	(124,998)	-	124,998
Net cash (used in) provided by operating activities	(815,550)	(815,550)	-	1,472,794	1,472,794	-

Note 9: Subsequent Events

Subsequent events have been evaluated through the date of the Independent Auditor's Report, which is the date the financial statements were available to be issued.

Other Information

Texas Reliability Entity, Inc.

Schedule of Statutory and Nonstatutory Operating Activities

Year Ended December 31, 2013

	Statutory	Nonstatutory	Total
Revenues, Gains and Other Support			
Statutory revenue	$ 8,806,770	$ -	$ 8,806,770
Protocol revenue	-	1,029,100	1,029,100
Interest income	7,929	1,147	9,076
Total revenues, gains and other support	8,814,699	1,030,247	9,844,946
Expenses			
Salaries and related benefits	7,515,156	700,653	8,215,809
Facility and equipment costs	649,885	36,026	685,911
Outside services	840,092	14,637	854,729
Travel and meetings	358,865	1,015	359,880
Administrative and other	245,151	24,438	269,589
Depreciation	532,066	140,219	672,285
Total expenses	10,141,215	916,988	11,058,203
Change in Unrestricted Net Assets	(1,326,516)	113,259	(1,213,257)
Unrestricted Net Assets, Beginning of Year, As Restated	6,284,829	669,172	6,954,001
Unrestricted Net Assets, End of Year	$ 4,958,313	$ 782,431	$ 5,740,744

ATTACHMENT 9

2013 ACTUAL COST-TO-BUDGET COMPARISON

AND

2013 AUDITED FINANCIAL REPORT

FOR

WESTERN ELECTRICITY COORDINATING COUNCIL

Jillian Lessner
Director of Finance and Accounting

801-883-6872
jlessner@wecc.biz

May 9, 2014

Mr. Michael Walker
Senior Vice President, Chief Financial and Administrative Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, Georgia 30326

RE: 2013 Statement of Activities and Variance Explanations Based on Audited Financials

Summary

The Western Electricity Coordinating Council's (WECC) audited Statutory total change in working capital for the year ended December 31, 2013 is over budget by $8.46 million with grant activity and $4.50 million over budget without grant activity. The major drivers of WECC's 2013 overrun are related to the bifurcation of the organization, the recommendations of the Reliability Coordination Task Force (RCTF), and timing variances related to the Department of Energy (DOE) grants.

A summary of significant overall variances (greater than $10,000 and 10 percent) is described in this document. For significant program area line-item variances, see the detailed statements of activities.

WECC substantially completed all of its goals and key deliverables as contained in the 2013 Business Plan and Budget.

Allocation of Indirect Costs

Administrative Services costs are allocated to program activities based on a full-time equivalent (FTE) ratio that is consistent with NERC's accounting methodology for allocation of overhead.

Federal Grants

In WECC's 2010 Amended Business Plan and Budget, WECC included revenue and associated costs related to three U.S. Department of Energy grants. FERC determined that the activities performed under the three grants received by WECC qualify as Section 215 activities.

The Western Interconnection Synchrophasor Program (WISP) (budgeted in the Situation Awareness program area) increases reliability by, among other things, enhancing the situation awareness of WECC's Reliability Coordinator Offices.

This Interconnection-wide Synchrophasor system also enables smart grid functionality such as:

- Improved integrated system operations.

- Enhanced, knowledge-based, real-time, advanced-warning systems.
- Reduced energy losses.
- Increased efficiency of asset use.
- Improved market efficiency.
- Increased reliability and efficient integration of intermittent renewable resources.

The Regional Transmission Expansion Planning (RTEP) project, which encompasses all activities funded under this U.S. DOE grant, produces Interconnection-level transmission plans for the Western Interconnection. The RTEP project is a natural expansion of the depth, breadth, and coordination of existing regional and sub-regional planning processes. The plan accomplishes the following:

- Evaluates the long-term regional transmission capacity needs under a comprehensive set of load, resource, and policy scenarios.
- Incorporates the results of a comprehensive examination of reliability impacts, technology costs, and emissions conducted during the project.
- Provides guidance for decision-makers at all levels (project developers, siting authorities, utility regulators, and others).
- Facilitates and accelerates the development of needed transmission infrastructure.

WECC uses a fund-accounting system to ensure that federal grant activities are segregated in accordance with federal cost-accounting standards.

Non-Statutory

WECC has one non-statutory activity, the Western Renewable Energy Generation Information System (WREGIS). WECC uses a fund-accounting system that allows costs to be segregated between statutory and non-statutory activities to ensure that no statutory funding is used for non-statutory activities.

In 2013, WECC allocated indirect costs to its non-statutory activity based on FTEs. Indirect costs include the Board of Directors and its Standing Committees, General and Administrative, Legal, Information Technology, Human Resources, and Finance programs. These costs are allocated to WREGIS based on the ratio of total WREGIS FTEs to total operating program FTEs. This allocation is consistent with the FTE method of allocating overhead costs used by NERC and the other Regional Entities.

Reserves

WECC used working capital reserves to fund its budget overrun.

Variance Explanations (Statutory Activities)

FUNDING

- **Penalty Sanctions** ($1.40 million over budget)
  - Some penalty sanction payments received from Registered Entities between July 1, 2013 and December 31,2013 were recorded as 2013 penalty revenues rather than being held to offset 2015 assessments to offset accrued estimates for potential penalty expenses.
- **Grant Funding** ($6.07 million over budget)
  - Grant expenditures were delayed from 2012, the year in which they were budgeted, to 2013.
  - The variances are timing differences only; total project cost has not changed.
- **Interest Income** ($88,000 under budget)
  - Lower-than-anticipated rates of return on WECC's cash balances.
- **Miscellaneous Income** ($279,000 under budget)
  - Unrealized losses arising from fair market valuation of WECC's investment portfolio.

EXPENSES

- **Salaries** ($2.98 million over budget)
  - Additional Reliability Coordinator personnel were hired as recommended by the RCTF.
  - Additional administrative personnel were hired in preparation for the bifurcation of the Reliability Coordinator function into a separate company.
- **Savings and Retirement** ($210,000 over budget)
  - Savings and Retirement fluctuates with Salaries.
- **Meetings** ($311,000 under budget)
  - Lower-than-anticipated attendance at workshops and training classes.
  - Company-wide cost-saving effort to reduce expenses.
  - Increased use of WebEx services.
- **Travel** ($178,000 under budget)
  - WECC staff attended fewer off-site meetings.
  - More efficient audits requiring fewer days on site.
  - Increased use of webinars.
- **Conference Calls** ($74,000 under budget)
  - Conference call usage was less than expected.
- **Consultants & Contracts** ($8.16 million over budget)
  - Contracts associated with the grants were delayed from 2012, the year in which they were budgeted, to 2013.
  - Unbudgeted search fees for independent directors.
  - The development of reliability enhancement measures.
  - The creation of a Reliability Coordinator trainee program.

- **Office Costs** ($885,000 over budget)
  - WISP software licensing and maintenance expenditures were delayed from 2012, the year in which they were budgeted, to 2013.
- **Professional Services** ($820,000 over budget)
  - Unbudgeted legal fees and independent director compensation related to the bifurcation of the Reliability Coordinator function into a separate company.
- **Miscellaneous** ($1.40 million over budget)
  - Accrued estimates for penalty expenses.
- **Indirect Expenses** ($148,000 under budget)
  - Administrative Services program area expenses were less than budgeted due to efficiency gains.

FIXED ASSETS

- **Computer & Software CapEx** ($824,000 over budget)
  - WISP asset expenditures were delayed from 2012, the year in which they were budgeted.
- **Furniture & Fixtures CapEx** ($28,000 under budget)
  - Furniture & Fixtures expenditures were eliminated.
- **Equipment CapEx** ($87,000 under budget)
  - Equipment CapEx expenditures were eliminated in Administrative Services
- **Leasehold Improvements** ($406,000 over budget)
  - Control Room modifications related to WISP.

Please feel free to contact me if you have any questions.

Thank you,

Jillian Lessner

Director of Finance and Accounting

cc:
Jim Robb, CEO
David Godfrey, VP and Chief Administrative Officer
WECC Finance and Audit Committee
Susan Turpen, NERC Controller

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Total Company Summary

	2013 Actual	2013 Budget	2013 Variance
Funding			
WECC Funding			
WECC Assessments	$ 40,962,547	$ 40,962,547	$ -
Penalty Sanctions	4,366,850	2,966,850	1,400,000
Total ERO Funding	**$ 45,329,397**	**$ 43,929,397**	**$ 1,400,000**
Membership Fees	1,913,930	1,850,000	63,930
Grant Funding	11,989,630	5,915,606	6,074,024
Services & Software	-	-	-
Workshops	809,510	895,300	(85,790)
Interest	252,968	300,000	(47,032)
Miscellaneous	(290,847)	4,000	(294,847)
Total Funding	**$ 60,004,588**	**$ 52,894,303**	**$ 7,110,285**
Expenses			
Personnel Expenses			
Salaries	27,739,739	24,794,700	2,945,039
Payroll Taxes	1,855,388	1,783,654	71,734
Employee Benefits	3,557,309	3,528,492	28,817
Savings & Retirement	1,824,550	1,617,965	206,585
Total Personnel Expenses	**$ 34,976,987**	**$ 31,724,812**	**$ 3,252,175**
Meeting Expenses			
Meetings	686,797	1,014,555	(327,758)
Travel	1,774,188	1,992,001	(217,813)
Conference Calls	98,532	172,992	(74,460)
Total Meeting Expenses	**$ 2,559,517**	**$ 3,179,548**	**$ (620,030)**
Operating Expenses			
Consultants & Contracts	13,991,057	5,850,646	8,140,411
Office Rent	2,156,031	1,975,322	180,709
Office Costs	7,539,488	6,684,085	855,403
Professional Services	1,520,333	742,829	777,504
Miscellaneous	1,400,000	-	1,400,000
Depreciation	4,541,466	4,178,235	363,231
Total Operating Expenses	**$ 31,148,375**	**$ 19,431,117**	**$ 11,717,258**
Total Direct Expenses	**$ 68,684,879**	**$ 54,335,476**	**$ 14,349,403**
Indirect Expenses	(0)	-	-
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**
Total Expenses	**68,684,879**	**54,335,476**	**14,349,403**
Change in Assets	**$ (8,680,291)**	**$ (1,441,174)**	**$ (7,239,118)**
Fixed Assets			
Depreciation	(4,541,466)	(4,178,235)	(363,231)
Computer & Software CapEx	2,077,532	1,253,000	824,532
Furniture & Fixtures CapEx	5,858	34,000	(28,142)
Equipment CapEx	-	87,000	(87,000)
Leasehold Improvements	1,405,555	1,000,000	405,555
Change in Fixed Assets	**$ (1,052,521)**	**$ (1,804,235)**	**$ 751,714**
Allocation of Fixed Assets	-	-	-
Incr(Dec) in Fixed Assets	**$ (1,052,521)**	**$ (1,804,235)**	**$ 751,714**
Total Budget	**67,632,358**	**52,531,241**	**15,101,117**
Change in Working Capital	**$ (7,627,770)**	**$ 363,062**	**$ (7,990,832)**
FTEs	232.97	221.3	11.6

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Statutory Summary

	2013 Actual	2013 Budget	2013 Variance	
Funding				
WECC Funding				
WECC Assessments	$ 40,962,547	40,962,547	$ -	
Penalty Sanctions	4,366,850	2,966,850	1,400,000	32.1%
Total ERO Funding	**$ 45,329,397**	**$ 43,929,397**	**$ 1,400,000**	
Membership Fees	-	-	-	
Grant Funding	11,989,630	5,915,606	6,074,024	50.7%
Services & Software	-	-	-	
Workshops	806,065	885,300	(79,235)	-9.8%
Interest	202,060	290,911	(88,851)	-44.0%
Miscellaneous	(275,136)	3,879	(279,015)	101.4%
Total Funding	**$ 58,052,016**	**$ 51,025,092**	**$ 7,026,923**	
Expenses				
Personnel Expenses				
Salaries	27,427,011	24,445,265	2,981,746	10.9%
Payroll Taxes	1,830,268	1,757,635	72,633	4.0%
Employee Benefits	3,518,494	3,443,468	75,026	2.1%
Savings & Retirement	1,803,814	1,593,505	210,309	11.7%
Total Personnel Expenses	**$ 34,579,587**	**$ 31,239,874**	**$ 3,339,713**	
Meeting Expenses				
Meetings	684,817	996,255	(311,438)	-45.5%
Travel	1,763,454	1,942,001	(178,547)	-10.1%
Conference Calls	98,137	172,492	(74,355)	-75.8%
Total Meeting Expenses	**$ 2,546,407**	**$ 3,110,748**	**$ (564,340)**	
Operating Expenses				
Consultants & Contracts	13,988,622	5,830,998	8,157,624	58.3%
Office Rent	2,156,031	1,975,322	180,709	8.4%
Office Costs	7,099,447	6,214,635	884,811	12.5%
Professional Services	1,547,605	722,829	824,776	53.3%
Miscellaneous	1,400,000	-	1,400,000	
Depreciation	4,541,466	4,176,235	365,231	8.0%
Total Operating Expenses	**$ 30,733,171**	**$ 18,920,019**	**$ 11,813,152**	
Total Direct Expenses	**$ 67,859,165**	**$ 53,270,639**	**$ 14,588,525**	
Indirect Expenses	(295,248)	(443,310)	148,062	-50.1%
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	
Total Expenses	**67,563,917**	**52,827,329**	**14,736,587**	
Change in Assets	**$ (9,511,901)**	**$ (1,802,237)**	**$ (7,709,664)**	
Fixed Assets				
Depreciation	(4,541,466)	(4,176,235)	(365,231)	8.0%
Computer & Software CapEx	2,077,532	1,253,000	824,532	39.7%
Furniture & Fixtures CapEx	5,858	34,000	(28,142)	-480.4%
Equipment CapEx	-	87,000	(87,000)	
Leasehold Improvements	1,405,555	1,000,000	405,555	28.9%
Change in Fixed Assets	**$ (1,052,521)**	**$ (1,802,235)**	**$ 749,714**	-71.2%
Allocation of Fixed Assets	-	-	-	
Incr(Dec) in Fixed Assets	**$ (1,052,521)**	**$ (1,802,235)**	**$ 749,714**	
Total Budget	**66,511,396**	**51,025,092**	**15,486,302**	
Change in Working Capital	**$ (8,459,378)**	**$ -**	**$ (8,459,379)**	
FTEs	227.8	216.3	11.4	

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Reliability Standards

	2013 Actual	2013 Budget	2013 Variance		Explanations of Variances - 10% and $10,000
Funding					
WECC Funding					
WECC Assessments	$ 903,967	$ 903,967	$ -	0.0%	
Penalty Sanctions	64,888	64,888	-	0.0%	
Total ERO Funding	**$ 968,855**	**$ 968,855**	**$ -**		
Membership Fees	-	-	-		
Grant Funding	-	-	-		
Services & Software			-		
Workshops	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding	**$ 968,855**	**$ 968,855**	**$ -**		
Expenses					
Personnel Expenses					
Salaries	420,510	464,771	(44,261)	-9.5%	One position was not filled.
Payroll Taxes	28,638	34,916	(6,278)	-18.0%	
Employee Benefits	28,015	60,155	(32,140)	-53.4%	Underutilization of training and medical benefits.
Savings & Retirement	28,483	40,139	(11,656)	-29.0%	Savings & Retirement fluctuates with Salaries.
Total Personnel Expenses	**$ 505,646**	**$ 599,981**	**$ (94,335)**		
Meeting Expenses					
Meetings	112	14,754	(14,642)	-99.2%	No Drafting Team meetings held.
Travel	28,690	43,000	(14,310)	-33.3%	Lower-than-anticipated attendance at external meetings.
Conference Calls	2,263	11,400	(9,137)	-80.1%	
Total Meeting Expenses	**$ 31,065**	**$ 69,154**	**$ (38,089)**		
Operating Expenses					
Consultants & Contracts	-	-	-		
Office Rent	-	-	-		
Office Costs	6,348	8,641	(2,293)	-26.5%	
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	**$ 6,348**	**$ 8,641**	**$ (2,293)**		
Total Direct Expenses	**$ 543,059**	**$ 677,776**	**$ (134,717)**		
Indirect Expenses	266,793	303,869	(37,076)	-12.2%	Based on standardized Regional Entity FTE ratios and spending in Administrative Services areas.
Other Non-Operating Expenses					
Total Expenses	**809,852**	**981,645**	**(171,792)**		
Change in Assets	**$ 159,003**	**$ (12,790)**	**$ 171,792**		
Fixed Assets					
Depreciation	-		-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Change in Fixed Assets	**$ -**	**$ -**	**$ -**		
Allocation of Fixed Assets	(3,906)	(12,790)	8,884	-69.5%	
Incr(Dec) in Fixed Assets	**$ (3,906)**	**$ (12,790)**	**$ 8,884**		
Total Budget	**805,946**	**968,855**	**(162,908)**		
Change in Working Capital	**$ 162,909**	**$ 0**	**$ 162,908**		
FTEs	2.99	3.5	(0.5)		

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Compliance Monitoring and Enforcement and Organization Registration and Certification

	2013 Actual	2013 Budget	2013 Variance		Explanations of Variances - 10% and $10,000
Funding					
WECC Funding					
WECC Assessments	$ 11,696,264	$ 11,696,264	$ -	0.00%	
Penalty Sanctions	936,241	936,241	-	0.00%	
Total ERO Funding	**$ 12,632,505**	**$ 12,632,505**	**$ -**		
Membership Fees	-	-	-		
Grant Funding	-	-	-		
Services & Software			-		
Workshops	375,335	433,750	(58,415)	-13.47%	CUG/CIPUG workshop attendance was less than predicted.
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding	**$ 13,007,840**	**$ 13,066,255**	**$ (58,415)**		
Expenses					
Personnel Expenses					
Salaries	5,188,489	5,019,223	169,266	3.37%	
Payroll Taxes	375,870	370,015	5,855	1.58%	
Employee Benefits	602,842	757,768	(154,926)	-20.45%	Underutilization of training due to reduced staff levels and increased workload. Underutilization of medical benefits due to lower-than-anticipated staffing levels.
Savings & Retirement	338,088	314,433	23,655	7.52%	
Total Personnel Expenses	**$ 6,505,289**	**$ 6,461,439**	**$ 43,850**		
Meeting Expenses					
Meetings	271,718	452,985	(181,267)	-40.02%	Lower-than-anticipated costs per person at CUG/CIPUG meetings.
Travel	619,113	872,000	(252,887)	-29.00%	More efficient audits requiring fewer days onsite.
Conference Calls	22,349	64,550	(42,201)	-65.38%	Increased use of WebEx; lower-than-anticipated number of conference calls.
Total Meeting Expenses	**$ 913,180**	**$ 1,389,535**	**$ (476,355)**		
Operating Expenses					
Consultants & Contracts	617,189	470,000	147,189	31.32%	Staff augmentation for audits and registrations.
Office Rent	3,889	-	3,889		
Office Costs	372,950	494,423	(121,473)	-24.57%	Lower-than-anticipated WEBCDMS maintenance & Licensing fees.
Professional Services	-	1,000	(1,000)	-100.00%	
Miscellaneous	-	-	-		
Depreciation	68,001	115,500	(47,499)	-41.13%	Depreciation was budgeted based on the prior year budget, not on prior year actual depreciation.
Total Operating Expenses	**$ 1,062,029**	**$ 1,080,923**	**$ (18,894)**		
Total Direct Expenses	**$ 8,480,497**	**$ 8,931,897**	**$ (451,400)**		
Indirect Expenses	4,735,094	4,477,429	257,665	5.75%	Based on standardized Regional Entity FTE ratios and spending in Administrative Services areas.
Other Non-Operating Expenses					
Total Expenses	**13,215,591**	**13,409,326**	**(193,735)**		
Change in Assets	**$ (207,751)**	**$ (343,071)**	**$ 135,320**		
Fixed Assets					
Depreciation	(68,001)	(115,500)	47,499	-41.13%	Depreciation was budgeted based on the prior year budget, not on prior year actual depreciation.
Computer & Software CapEx	-	50,000	(50,000)	-100.00%	No actual software purchases in 2013.
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Change in Fixed Assets	**$ (68,001)**	**$ (65,500)**	**$ (2,501)**		
Allocation of Fixed Assets	(69,321)	(184,545)	115,224	-62.44%	Based on standardized Regional Entity FTE ratios and spending in Administrative Services areas.
Incr(Dec) in Fixed Assets	**$ (137,322)**	**$ (250,045)**	**$ 112,723**		
Total Budget	**13,078,269**	**13,159,281**	**(81,012)**		
Change in Working Capital	**$ (70,429)**	**$ (93,025)**	**$ 22,597**		
FTEs	53.10	50.5	2.6		

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Training and Education

	2013 Actual	2013 Budget	2013 Variance		Explanations of Variances - 10% and $10,000
Funding					
WECC Funding					
WECC Assessments	$ 51,135	$ 51,135	$ -	0.00%	
Penalty Sanctions	27,809	27,809	-	0.00%	
Total ERO Funding	**$ 78,944**	**$ 78,944**	**$ -**		
Membership Fees	-	-	-		
Grant Funding	-	-	-		
Services & Software			-		
Workshops	430,730	451,550	(20,820)	-4.61%	
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding	**$ 509,674**	**$ 530,494**	**$ (20,820)**		
Expenses					
Personnel Expenses					
Salaries	83,415	103,772	(20,357)	-19.62%	One position was not filled.
Payroll Taxes	6,433	7,690	(1,257)	-16.34%	
Employee Benefits					Underutilization of external training and lower-than-budgeted enrollment in insurance plans. Credits for internal participation at operator training classes are posted here and the corresponding expense is posted in the employee's department. These amounts net to zero and internal training participation is unbudgeted.
	(22,262)	21,305	(43,567)	-204.49%	
Savings & Retirement	7,873	7,264	609	8.38%	
Total Personnel Expenses	**$ 75,460**	**$ 140,031**	**$ (64,571)**		
Meeting Expenses					
Meetings	80,122	99,950	(19,828)	-19.84%	Lower-than-budgeted attendance at training sessions and workshops.
Travel	10,023	6,350	3,673	57.85%	
Conference Calls	517	600	(83)	-13.79%	
Total Meeting Expenses	**$ 90,663**	**$ 106,900**	**$ (16,237)**		
Operating Expenses					
Consultants & Contracts	62,779	92,500	(29,721)	-32.13%	Consultant did not teach as many sessions as anticipated.
Office Rent	44,800	47,478	(2,678)	-5.64%	
Office Costs	75,904	40,980	34,924	85.22%	Unbudgeted training software maintenance fee.
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	-	-	-		
Total Operating Expenses	**$ 183,484**	**$ 180,958**	**$ 2,526**		
Total Direct Expenses	**$ 349,606**	**$ 427,889**	**$ (78,283)**		
Indirect Expenses	88,931	110,851	(21,920)	-19.77%	Based on standardized Regional Entity FTE ratios and spending in Administrative Services areas.
Other Non-Operating Expenses					
Total Expenses	**438,537**	**538,740**	**(100,203)**		
Change in Assets	**$ 71,137**	**$ (8,246)**	**$ 79,383**		
Fixed Assets					
Depreciation	-	-	-		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Change in Fixed Assets	**$ -**	**$ -**	**$ -**		
Allocation of Fixed Assets	(1,302)	(5,482)	4,180	-76.25%	
Incr(Dec) in Fixed Assets	**$ (1,302)**	**$ (5,482)**	**$ 4,180**		
Total Budget (Expenses plus Inc(Dec) in Fix	**437,235**	**533,258**	**(96,023)**		
Change in Working Capital (Total Funding less Total Budget)	**$ 72,439**	**$ (2,764)**	**$ 75,203**		
FTEs	1.00	1.5	(0.5)		

Western Electricity Coordinating Council
201s Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Reliability Assessment and Performance Analysis

	2013 Actual	2013 Budget	2013 Variance		Explanations of Variances - 10% and $10,000
Funding					
WECC Funding					
WECC Assessments	$ 3,834,675	$ 3,834,675	$ -	0.00%	
Penalty Sanctions	362,755	362,755	-	0.00%	
Total ERO Funding	**$ 4,197,430**	**$ 4,197,430**	**$ -**		
Membership Fees	-	-	-		
Grant Funding	2,804,035	3,129,529	(325,494)	-10.40%	Based on costs incurred related to grant activities.
Services & Software			-		
Workshops	-	-	-		
Interest	-	-	-		
Miscellaneous	1,040	-	1,040		
Total Funding	**$ 7,002,505**	**$ 7,326,959**	**$ (324,454)**		
Expenses					
Personnel Expenses					
Salaries	1,996,940	1,928,608	68,332	3.54%	
Payroll Taxes	151,668	142,733	8,935	6.26%	
Employee Benefits	269,611	237,122	32,489	13.70%	Higher-than-anticipated enrollment in insurance programs.
Savings & Retirement	166,735	133,059	33,676	25.31%	Savings & Retirement fluctuates with Salaries.
Total Personnel Expenses	**$ 2,584,954**	**$ 2,441,522**	**$ 143,432**		
Meeting Expenses					
Meetings	55,950	111,423	(55,473)	-49.79%	Lower-than-budgeted hosting of external meetings.
Travel	112,776	134,900	(22,124)	-16.40%	Reduced travel to external meetings.
Conference Calls	18,111	33,000	(14,889)	-45.12%	Lower-than-anticipated usage of conference calls.
Total Meeting Expenses	**$ 186,838**	**$ 279,323**	**$ (92,485)**		
Operating Expenses					
Consultants & Contracts	1,811,641	2,527,541	(715,900)	-28.32%	Timing of RTEP grant spending and also a modeling project in the planning function was deferred to 2014.
Office Rent	20	-	20		
Office Costs	166,452	61,300	105,152	171.54%	A portion of software maintenance fees were budgeted in Fixed Assets. See offset in Fixed Assets below.
Professional Services	9,809	30,000	(20,191)	-67.30%	No actual Non-Affiliated Director compensation related to RTEP grant meetings.
Miscellaneous	-	-	-		
Depreciation	247,554	68,400	179,154	261.92%	Depreciation was budgeted based on the prior year budget, not on prior year actual depreciation.
Total Operating Expenses	**$ 2,235,476**	**$ 2,687,241**	**$ (451,765)**		
Total Direct Expenses	**$ 5,007,268**	**$ 5,408,086**	**$ (400,819)**		
Indirect Expenses	1,924,235	1,698,777	225,458	13.27%	Based on standardized Regional Entity FTE ratios and spending in Administrative Services areas.
Other Non-Operating Expenses					
Total Expenses	**6,931,503**	**7,106,863**	**(175,361)**		
Change in Assets	**$ 71,003**	**$ 220,096**	**$ (149,093)**		
Fixed Assets					
Depreciation	(247,554)	(68,400)	(179,154)	261.92%	Depreciation was budgeted based on the prior year budget, not on prior year actual depreciation.
Computer & Software CapEx	265,836	360,000	(94,164)	-26.16%	A portion of software maintenancefees were budgeted in Fixed Assets. See offset in Office Costs.
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Change in Fixed Assets	**$ 18,282**	**$ 291,600**	**$ (273,318)**		
Allocation of Fixed Assets	(28,170)	(71,504)	43,334	-60.60%	Based on standardized Regional Entity FTE ratios and spending in Administrative Services areas.
Incr(Dec) in Fixed Assets	**$ (9,888)**	**$ 220,096**	**$ (229,984)**		
Total Budget	**6,921,614**	**7,326,959**	**(405,345)**		
Change in Working Capital	**$ 80,891**	**$ (0)**	**$ 80,891**		
FTEs	21.58	19.6	2.0		

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Situation Awareness and Infrastructure Security

	2013 Actual	2013 Budget	2013 Variance		Explanations of Variances - 10% and $10,000
Funding					
WECC Funding					
WECC Assessments	$ 24,476,506	$ 24,476,506	$ -	0.00%	
Penalty Sanctions	2,975,157	1,575,157	1,400,000	88.88%	Early recognition of revenue to offset estimated penalty expense.
Total ERO Funding	**$ 27,451,663**	**$ 26,051,663**	**$ 1,400,000**		
Membership Fees	-	-	-		
Grant Funding	9,186,952	2,786,076	6,400,876	229.75%	WISP grant funding fluctuates with WISP expenditures. Delayed 2012 spending by subrecipient and cost-share partners resulted in higher-than-budgeted 2013 grant funding.
Services & Software			-		
Workshops	-	-	-		
Interest	-	-	-		
Miscellaneous	(179,266)	-	(179,266)		WISP routers were written off and ownership was transferred to cost-share partners.
Total Funding	**$ 36,459,349**	**$ 28,837,739**	**$ 7,621,610**		
Expenses					
Personnel Expenses					
Salaries	12,982,046	10,500,212	2,481,834	23.64%	Unbudgeted hiring of additional personnel as recommended by the RC Task Force.
Payroll Taxes	866,562	745,846	120,716	16.19%	Payroll Taxes fluctuate with salaries.
Employee Benefits	1,240,400	1,093,420	146,980	13.44%	Employee Benefits fluctuate with headcount.
Savings & Retirement	819,446	647,167	172,279	26.62%	Savings and Retirement fluctuates with salaries.
Total Personnel Expenses	**$ 15,908,454**	**$ 12,986,645**	**$ 2,921,809**		
Meeting Expenses					
Meetings	15,704	-	15,704		Unbudgeted expenditures for the NPCC audit of the RC.
Travel	470,796	437,726	33,070	7.55%	
Conference Calls	23,072	15,920	7,152	44.92%	
Total Meeting Expenses	**$ 509,572**	**$ 453,646**	**$ 55,926**		
Operating Expenses					
Consultants & Contracts	10,264,627	2,422,290	7,842,337	323.76%	2012 budgeted spending by WISP sub-recipient was delayed to 2013.
Office Rent	1,057,733	768,081	289,652	37.71%	Unbudgeted office space to accommodate additional personnel recommended by the RC Task Force.
Office Costs	5,403,291	4,518,304	884,987	19.59%	Primarily due to timing of WISP licensing fees, WISP unbugeted expensed equipment, and higher-than-budgeted license and maintenance fees for WIT, and higher than budgeted license and maintenance fees for the RC.
Professional Services	171,804	5,000	166,804	3336.08%	Unbudgeted fees for the NPCC audit of WECC's RC and IA functions.
Miscellaneous	1,400,000	-	1,400,000		Unbudgeted estimated penalties expenses.
Depreciation	3,849,584	3,315,530	534,054	16.11%	Higher depreciation due to greater-than-budgeted CapEx purchases.
Total Operating Expenses	**$ 22,147,039**	**$ 11,029,205**	**$ 11,117,834**		
Total Direct Expenses	**$ 38,565,065**	**$ 24,469,496**	**$ 14,095,569**		
Indirect Expenses	7,499,576	6,122,257	1,377,319	22.50%	Based on standardized Regional Entity FTE ratios and spending in Administrative Services areas.
Other Non-Operating Expenses	**$ -**				
Total Expenses	**46,064,641**	**30,591,753**	**15,472,888**		
Change in Assets	**$ (9,605,292)**	**$ (1,754,014)**	**$ (7,851,278)**		
Fixed Assets					
Depreciation	(3,849,584)	(3,315,530)	(534,054)	16.11%	Higher depreciation due to greater-than-budgeted CapEx purchases.
Computer & Software CapEx	1,667,176	843,000	824,176	97.77%	Timing related to WISP grant. 2013 software purchases were budgeted in 2012.
Furniture & Fixtures CapEx	5,858	29,000	(23,142)	-79.80%	Less than budgeted Furniture and Fixture purchases in 2013.
Equipment CapEx	-	-	-		
Leasehold Improvements	1,405,555	1,000,000	405,555	40.56%	WISP expenditures for control rooms delayed from 2012 to 2013.
Change in Fixed Assets	**$ (770,995)**	**$ (1,443,530)**	**$ 672,535**		
Allocation of Fixed Assets	(129,109)	(310,484)	181,375	-58.42%	Based on standardized Regional Entity FTE ratios and spending in Administrative Services areas.
Incr(Dec) in Fixed Assets	**$ (900,104)**	**$ (1,754,014)**	**$ 853,910**		
Total Budget	**45,164,537**	**28,837,739**	**16,326,798**		
Change in Working Capital	**$ (8,705,188)**	**$ -**	**$ (8,705,188)**		
FTEs	98.9	85.0	13.9		

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Technical Committees and Member Forums

	2013 Actual	2013 Budget	2013 Variance		Explanations of Variances - 10% and $10,000
Funding					
WECC Funding					
WECC Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	**$ -**	**$ -**	**$ -**		
Membership Fees	-	-	-		
Grant Funding	(1,357)	-	(1,357)		
Services & Software			-		
Workshops	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-			
Total Funding	**$ (1,357)**	**$ -**	**$ (1,357)**		
Expenses					
Personnel Expenses					
Salaries	849,692	902,239	(52,547)	-5.82%	
Payroll Taxes	64,586	67,808	(3,221)	-4.75%	
Employee Benefits	106,789	86,657	20,132	23.23%	Higher-than-budgeted enrollment in insurance programs.
Savings & Retirement	66,555	63,156	3,399	5.38%	
Total Personnel Expenses	**$ 1,087,622**	**$ 1,119,859**	**$ (32,238)**		
Meeting Expenses					
Meetings	265,889	297,448	(31,559)	-10.61%	Lower-than budgeted costs of off-site hotel meeting sites.
Travel	217,400	149,825	67,575	45.10%	Higher-than-anticipated Board Director travel expense incurred related to the bifurcation of WECC.
Conference Calls	13,743	27,400	(13,657)	-49.84%	Lower-than-anticipated usage.
Total Meeting Expenses	**$ 497,032**	**$ 474,673**	**$ 22,359**		
Operating Expenses					
Consultants & Contracts	-	166,667	(166,667)	-100.00%	Data Validation project was deferred to 2014.
Office Rent	-	-	-		
Office Costs	67,955	40,068	27,887	69.60%	Unbudgeted OATI software maintenance and enhancement expenses.
Professional Services	654,424	401,000	253,424	63.20%	Higher-than-budgeted Non-Affiliated Director Compensation due to increased meeting schedules and additional directors in preparation for the bifurcation of WECC.
Miscellaneous	-	-	-		
Depreciation	-	16,000	(16,000)	-100.00%	
Total Operating Expenses	**$ 722,379**	**$ 623,734**	**$ 98,645**		
Total Direct Expenses	**$ 2,307,033**	**$ 2,218,266**	**$ 88,767**		
Indirect Expenses	(2,308,390)	(2,218,266)	(90,124)	4.06%	
Other Non-Operating Expenses					
Total Expenses	**(1,357)**	**0**	**(1,357)**		
Change in Assets	**$ -**	**$ (0)**	**$ 0**		
Fixed Assets					
Depreciation	-	(16,000)	16,000	-100.00%	
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Change in Fixed Assets	**$ -**	**$ (16,000)**	**$ 16,000**		
Allocation of Fixed Assets	-	16,000	(16,000)	-100.00%	Allocated to Statutory Program Areas based on their FTE ratio to total.
Incr(Dec) in Fixed Assets	**$ -**	**$ -**	**$ -**		
Total Budget	**(1,357)**	**0**	**(1,357)**		
Change in Working Capital	**$ 0**	**$ (0)**	**$ 0**		
FTEs	6.6	7.6	(1.0)		

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
General and Administrative

	2013 Actual	2013 Budget	2011 Variance		Explanations of Variances - 10% and $10,000
Funding					
WECC Funding					
WECC Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	**$ -**	**$ -**	**$ -**		
Membership Fees	-	-	-		
Grant Funding	-	-	-		
Services & Software			-		
Workshops	-	-	-		
Interest	196,280	290,911	(94,631)	-32.53%	Lower-than-anticipated rates of return.
Miscellaneous	(97,074)	3,879	(100,953)	-2602.55%	Mark-to-market valuation of WECC's investment portfolio.
Total Funding	**$ 99,206**	**$ 294,790**	**$ (195,584)**		
Expenses					
Personnel Expenses					
Salaries	2,655,532	2,194,293	461,239	21.02%	Unbudgeted expenditures related to the hiring of two new CEOs.
Payroll Taxes	136,847	141,861	(5,014)	-3.53%	
Employee Benefits	277,921	214,991	62,930	29.27%	Higher-than-anticipated participation in the company's insurance programs.
Savings & Retirement	166,874	153,600	13,274	8.64%	
Total Personnel Expenses	**$ 3,237,174**	**$ 2,704,744**	**$ 532,430**		
Meeting Expenses					
Meetings	(11,864)	13,665	(25,529)	-186.82%	Meeting Expense allocation formula resulted in a department level variance and a credit in G&A.
Travel	169,263	168,700	563	0.33%	
Conference Calls	7,866	6,200	1,666	26.87%	
Total Meeting Expenses	**$ 165,265**	**$ 188,565**	**$ (23,300)**		
Operating Expenses					
Consultants & Contracts	265,834	110,000	155,834	141.67%	Unanticipated marketing expenses in Communications and unbudgeted consultants expense in the Procurement department.
Office Rent	1,048,402	1,159,764	(111,362)	-9.60%	
Office Costs	265,668	276,500	(10,832)	-3.92%	
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	245,504	502,179	(256,675)	-51.11%	Depreciation was budgeted based on the prior year budget, not on prior year actual depreciation.
Total Operating Expenses	**$ 1,825,408**	**$ 2,048,443**	**$ (223,035)**		
Total Direct Expenses	**$ 5,227,846**	**$ 4,941,752**	**$ 286,094**		
Indirect Expenses	(5,128,641)	(4,646,962)	(481,679)	10.37%	
Other Non-Operating Expenses					
Total Expenses	**99,206**	**294,790**	**(195,584)**		
Change in Assets	**$ 0**	**$ (0)**	**$ 0**		
Fixed Assets					
Depreciation	(245,504)	(502,179)	256,675	-51.11%	Depreciation was budgeted based on the prior year budget, not on prior year actual depreciation.
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	5,000	(5,000)	-100.00%	
Equipment CapEx	-	6,000	(6,000)	-100.00%	
Leasehold Improvements	-	-	-		
Change in Fixed Assets	**$ (245,504)**	**$ (491,179)**	**$ 245,675**		
Allocation of Fixed Assets	245,504	491,179	(245,675)	-50.02%	Allocated to Statutory Program Areas based on their FTE ratio to total.
Incr(Dec) in Fixed Assets	**$ -**	**$ 0**	**$ (0)**		
Total Budget	**99,206**	**294,790**	**(195,584)**		
Change in Working Capital	**$ 0**	**$ (0)**	**$ 0**		
FTEs	15.6	18.8	(3.2)		

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Legal

	2013 Actual	2013 Budget	2013 Variance		Explanations of Variances - 10% and $10,000
Funding					
WECC Funding					
WECC Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	**$ -**	**$ -**	**$ -**		
Membership Fees	-	-	-		
Grant Funding	-	-	-		
Services & Software			-		
Workshops	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-	-		
Total Funding	**$ -**	**$ -**	**$ -**		
Expenses					
Personnel Expenses					
Salaries	1,378,016	1,730,245	(352,229)	-20.36%	Two positions were not filled and turnover was high.
Payroll Taxes	88,292	126,811	(38,520)	-30.38%	Payroll Taxes fluctuate with Salaries
Employee Benefits	121,355	154,547	(33,192)	-21.48%	Underutilization of training and lower-than-anticipated enrollment in medical benefits.
Savings & Retirement	93,837	120,661	(26,824)	-22.23%	Savings & Retirement fluctuates with Salaries
Total Personnel Expenses	**$ 1,681,500**	**$ 2,132,264**	**$ (450,765)**		
Meeting Expenses					
Meetings	2,425	-	2,425		
Travel	61,386	80,000	(18,614)	-23.27%	Lower-than-anticipated travel to external meetings and open positions.
Conference Calls	2,007	2,500	(493)	-19.72%	
Total Meeting Expenses	**$ 65,819**	**$ 82,500**	**$ (16,681)**		
Operating Expenses					
Consultants & Contracts	82,764	-	82,764		Unbudgeted consultants expenses to support Corporate Compliance activities.
Office Rent	-	-	-		
Office Costs	77,139	50,000	27,139	54.28%	Unanticipated FERC filing fee.
Professional Services	641,781	182,829	458,952	251.03%	Higher-than-budgeted legal fees related to the bifurcation of WECC.
Miscellaneous	-	-	-		
Depreciation	8,489	-	8,489		
Total Operating Expenses	**$ 810,173**	**$ 232,829**	**$ 577,344**		
Total Direct Expenses	**$ 2,557,491**	**$ 2,447,593**	**$ 109,898**		
Indirect Expenses	(2,557,491)	(2,447,593)	(109,898)	4.49%	Allocated to Statutory Program Areas based on their FTE ratio to total.
Other Non-Operating Expenses					
Total Expenses	**-**	**0**	**(0)**		
Change in Assets	**$ -**	**$ (0)**	**$ 0**		
Fixed Assets					
Depreciation	(8,489)	-	(8,489)		
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Change in Fixed Assets	**$ (8,489)**	**$ -**	**$ (8,489)**		
Allocation of Fixed Assets	8,489	-	8,489		
Incr(Dec) in Fixed Assets	**$ -**	**$ -**	**$ -**		
Total Budget	**-**	**0**	**(0)**		
Change in Working Capital	**$ -**	**$ (0)**	**$ 0**		
FTEs	9.76	12.1	(2.3)		

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Information Technology

	2013 Actual	2013 Budget	2013 Variance		Explanations of Variances - 10% and $10,000
Funding					
WECC Funding					
WECC Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	**$ -**	**$ -**	**$ -**		
Membership Fees	-	-	-		
Grant Funding	-	-	-		
Services & Software			-		
Workshops	-	-	-		
Interest	-	-	-		
Miscellaneous	164	-	164		
Total Funding	**$ 164**	**$ -**	**$ 164**		
Expenses					
Personnel Expenses					
Salaries	714,676	829,213	(114,537)	-13.81%	Two positions were not filled.
Payroll Taxes	54,231	62,286	(8,055)	-12.93%	
Employee Benefits	112,078	114,786	(2,708)	-2.36%	
Savings & Retirement	45,061	58,045	(12,984)	-22.37%	Savings & Retirement fluctuates with Salaries.
Total Personnel Expenses	**$ 926,046**	**$ 1,064,330**	**$ (138,284)**		
Meeting Expenses					
Meetings	-	900	(900)	-100.00%	
Travel	9,721	13,000	(3,279)	-25.22%	
Conference Calls	5,956	6,572	(616)	-9.37%	
Total Meeting Expenses	**$ 15,678**	**$ 20,472**	**$ (4,794)**		
Operating Expenses					
Consultants & Contracts	36,106	12,000	24,106	200.88%	Unbudgeted website design costs.
Office Rent	701	-	701		
Office Costs	473,668	587,500	(113,832)	-19.38%	Purchases budgeted here were capitalized. See offset in Fixed Assets.
Professional Services	-	-	-		
Miscellaneous	-	-	-		
Depreciation	111,313	141,927	(30,614)	-21.57%	Depreciation expense was budgeted based on prior year budget, not on prior year actual depreciation.
Total Operating Expenses	**$ 621,788**	**$ 741,427**	**$ (119,639)**		
Total Direct Expenses	**$ 1,563,512**	**$ 1,826,229**	**$ (262,717)**		
Indirect Expenses	(1,563,348)	(1,826,228)	262,880	-14.39%	Allocated to Statutory Program Areas based on their FTE ratio to total.
Other Non-Operating Expenses					
Total Expenses	**164**	**1**	**163**		
Change in Assets	**$ -**	**$ (1)**	**$ 1**		
Fixed Assets					
Depreciation	(111,313)	(141,927)	30,614	-21.57%	Depreciation expense was budgeted based on prior year budget, not on prior year actual depreciation.
Computer & Software CapEx	121,902	-	121,902		Purchases budgeted in Office Costs were capitalizable. See offset in Office Costs.
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	81,000	(81,000)		Planned equipment purchases were cancelled due to the bifurcation of WECC.
Leasehold Improvements	-	-	-		
Change in Fixed Assets	**$ 10,589**	**$ (60,927)**	**$ 71,516**		
Allocation of Fixed Assets	(10,589)	60,927	(71,516)	-117.38%	Allocated to Statutory Program Areas based on their FTE ratio to total.
Incr(Dec) in Fixed Assets	**$ -**	**$ -**	**$ -**		
Total Budget	**164**	**0**	**163**		
Change in Working Capital	**$ -**	**$ (0)**	**$ 1**		
FTEs	8.0	9.0	(1.0)		

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Human Resources

	2013 Actual	2013 Budget	2013 Variance		Explanations of Variances - 10% and $10,000
Funding					
WECC Funding					
WECC Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	**$ -**	**$ -**	**$ -**		
Membership Fees	-	-	-		
Grant Funding	-	-	-		
Services & Software			-		
Workshops	-	-	-		
Interest	-	-	-		
Miscellaneous	-	-			
Total Funding	**$ -**	**$ -**	**$ -**		
Expenses					
Personnel Expenses					
Salaries	782,538	283,445	499,093	176.08%	Unbudgeted recruiting fees for two new CEOs, temporary help due to bifurcation and incremental HR staff for the new entity.
Payroll Taxes	26,330	21,290	5,040	23.67%	
Employee Benefits	721,141	625,824	95,317	15.23%	Higher-than-anticipated utilization of the health reimbursement account insurance program.
Savings & Retirement	45,170	21,841	23,329	106.81%	Savings & Retirement fluctuates with Salaries.
Total Personnel Expenses	**$ 1,575,179**	**$ 952,400**	**$ 622,779**		
Meeting Expenses					
Meetings	4,760	5,130	(370)	-7.21%	
Travel	45,919	26,000	19,919	76.61%	Higher-than-budgeted travel related to bifurcation and union negotiations.
Conference Calls	1,863	3,500	(1,637)	-46.77%	
Total Meeting Expenses	**$ 52,542**	**$ 34,630**	**$ 17,912**		
Operating Expenses					
Consultants & Contracts	840,538	30,000	810,538	2701.79%	Unbudgeted search fees for new Board members for WECC and Peak.
Office Rent	486	-	486		
Office Costs	128,639	88,070	40,569	46.06%	Unbudgeted drug testing and background check costs related to bifurcation of WECC.
Professional Services	13,395	23,000	(9,605)	-41.76%	
Miscellaneous	-	-	-		
Depreciation	692	6,700	(6,008)	-89.68%	
Total Operating Expenses	**$ 983,750**	**$ 147,770**	**$ 835,980**		
Total Direct Expenses	**$ 2,611,471**	**$ 1,134,800**	**$ 1,476,671**		
Indirect Expenses	(2,611,471)	(1,134,800)	(1,476,671)	130.13%	Allocated to Statutory Program Areas based on their FTE ratio to total.
Other Non-Operating Expenses					
Total Expenses	**-**	**(0)**	**0**		
Change in Assets	**$ -**	**$ 0**	**$ (0)**		
Fixed Assets					
Depreciation	(692)	(6,700)	6,008	-89.68%	
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Change in Fixed Assets	**$ (692)**	**$ (6,700)**	**$ 6,008**		
Allocation of Fixed Assets	692	6,700	(6,008)		
Incr(Dec) in Fixed Assets	**$ -**	**$ -**	**$ -**		
Total Budget	**-**	**(0)**	**0**		
Change in Working Capital	**$ -**	**$ 0**	**$ (0)**		
FTEs	4.23	3.1	1.1		

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Finance and Accounting

	2013 Actual	2013 Budget	2013 Variance		Explanations of Variances - 10% and $10,000
Funding					
WECC Funding					
WECC Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	**$ -**	**$ -**	**$ -**		
Membership Fees	-	-	-		
Grant Funding	-	-	-		
Services & Software	-	-	-		
Workshops	-	-	-		
Interest	5,780	-	5,780		
Miscellaneous	-	-			
Total Funding	**$ 5,780**	**$ -**	**$ 5,780**		
Expenses					
Personnel Expenses					
Salaries	375,158	489,243	(114,085)	-23.32%	Turnover and the conversion of a higher level position to a staff level.
Payroll Taxes	30,811	36,377	(5,566)	-15.30%	
Employee Benefits	60,604	76,890	(16,286)	-21.18%	Underutilization of training and lower-than-anticipated enrollment in medical benefits.
Savings & Retirement	25,691	34,142	(8,451)	-24.75%	
Total Personnel Expenses	**$ 492,264**	**$ 636,652**	**$ (144,388)**		
Meeting Expenses					
Meetings	-	-	-		
Travel	18,365	10,500	7,865	74.90%	
Conference Calls	389	850	(461)	-54.24%	
Total Meeting Expenses	**$ 18,754**	**$ 11,350**	**$ 7,404**		
Operating Expenses					
Consultants & Contracts	7,143	-	7,143		
Office Rent	-	-	-		
Office Costs	61,432	48,850	12,582	25.76%	Higher-than-anticipated software license fees for the accounting, fixed asset and new budget systems for Peak Reliability.
Professional Services	56,393	80,000	(23,607)	-29.51%	Lower-than-budgeted fees for audit and tax work.
Miscellaneous	-	-	-		
Depreciation	10,330	10,000	330	3.30%	
Total Operating Expenses	**$ 135,298**	**$ 138,850**	**$ (3,552)**		
Total Direct Expenses	**$ 646,316**	**$ 786,852**	**$ (140,537)**		
Indirect Expenses	(640,536)	(786,852)	146,316	-18.60%	Allocated to Statutory Program Areas based on their FTE ratio to total.
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**		
Total Expenses	**5,780**	**0**	**5,780**		
Change in Assets	**$ -**	**$ (0)**	**$ 0**		
Fixed Assets					
Depreciation	(10,330)	(10,000)	(330)	3.30%	
Computer & Software CapEx	22,618	-	22,618		Unbudgeted accounting and budgeting software for Peak.
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx	-	-	-		
Leasehold Improvements	-	-	-		
Change in Fixed Assets	**$ 12,288**	**$ (10,000)**	**$ 22,288**		
Allocation of Fixed Assets	(12,288)	10,000	(22,288)		Allocated to Statutory Program Areas based on their FTE ratio to total.
Incr(Dec) in Fixed Assets	**$ -**	**$ -**	**$ -**		
Total Budget	**5,780**	**0**	**5,780**		
Change in Working Capital	**$ -**	**$ (0)**	**$ 0**		
FTEs	6.05	5.7	0.3		

Western Electricity Coordinating Council
2013 Statement of Activities, Fixed Asset Expenditures, and Change in Working Capital
Non-Statutory Summary

	2013 Actual	2013 Budget	2013 Variance		
Funding					
WECC Funding					
WECC Assessments	$ -	$ -	$ -		
Penalty Sanctions	-	-	-		
Total ERO Funding	**$ -**	**$ -**	**$ -**		
Membership Fees	1,913,930	1,850,000	63,930	3.46%	
Grant Funding	-	-	-		
Services & Software			-		
Workshops	3,445	10,000	(6,555)	-65.55%	
Interest	50,908	9,089	41,819	460%	WREGIS held larger-than-anticipated levels of cash and cash equivalents which earned greater-than-budgeted interest income.
Miscellaneous	(15,711)	121	(15,832)	-13084%	Mark-to-market fluctuations in WREGIS's investment portfolio.
Total Funding	**$ 1,952,572**	**$ 1,869,210**	**$ 83,362**		
Expenses					
Personnel Expenses					
Salaries	312,728	349,435	(36,707)	-10.50%	Turnover and one unfilled positon during the year.
Payroll Taxes	25,120	26,019	(899)	-3.46%	
Employee Benefits	38,815	85,024	(46,209)	-54.35%	Under-utilization of training and lower-than-anticipated enrollment in medical benefits.
Savings & Retirement	20,737	24,460	(3,723)	-15.22%	
Total Personnel Expenses	**$ 397,400**	**$ 484,938**	**$ (87,538)**		
Meeting Expenses					
Meetings	1,980	18,300	(16,320)	-89.18%	Lower-than-anticipated number of committee meetings.
Travel	10,735	50,000	(39,265)	-78.53%	WREGIS staff conducted fewer than-anticipated off-site audits.
Conference Calls	395	500	(105)	-20.98%	
Total Meeting Expenses	**$ 13,110**	**$ 68,800**	**$ (55,690)**		
Operating Expenses					
Consultants & Contracts	2,435	19,648	(17,213)	-87.61%	Lower-than-budgeted use of consultants for Quickbooks software customization.
Office Rent	-	-	-		
Office Costs	440,041	469,450	(29,409)	-6.26%	
Professional Services	(27,273)	20,000	(47,273)	-236.36%	Unanticipated arbitration credit for prior year legal fees.
Miscellaneous	-	-	-		
Depreciation	-	2,000	(2,000)	-100.00%	
Total Operating Expenses	**$ 415,204**	**$ 511,098**	**$ (95,894)**		
Total Direct Expenses	**$ 825,714**	**$ 1,064,836**	**$ (239,122)**		
Indirect Expenses	295,248	443,310	(148,062)	-33.40%	Allocated to Statutory Program Areas based on their FTE ratio to total.
Other Non-Operating Expenses			**$ -**		
Total Expenses	1,120,962	1,508,146	(387,184)		
Change in Assets	**$ 831,610**	**$ 361,064**	**$ 470,546**		
Fixed Assets					
Depreciation	-	(2,000)	2,000	-100.00%	
Computer & Software CapEx	-	-	-		
Furniture & Fixtures CapEx	-	-	-		
Equipment CapEx					
Leasehold Improvements	-	-	-		
Change in Fixed Assets	**$ -**	**$ (2,000)**	**$ 2,000**	-100.00%	
Allocation of Fixed Assets	-	-	-		
Incr(Dec) in Fixed Assets	**$ -**	**$ (2,000)**	**$ 2,000**	-100.00%	
Total Budget	**1,120,962**	**1,506,146**	**(385,184)**	-25.57%	
Change in Working Capital	**$ 831,610**	**$ 363,064**	**$ 468,546**	129.05%	
FTEs	5.20	5.0	0.2		

Financial Statements and Report of Independent Certified Public Accountants

Western Electricity Coordinating Council

As of and for the years ended
December 31, 2013 and 2012

Contents

	Page
Report of Independent Certified Public Accountants	1
Financial Statements	
Statements of Financial Position	3
Statements of Activities	4
Statements of Cash Flows	5
Notes to Financial Statements	6

Grant Thornton LLP
155 N 400 W, Suite 500
Salt Lake City, Utah 84103

T 801.415.1000
F 801.322.0061
www.GrantThornton.com

REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

Board of Directors
Western Electricity Coordinating Council

We have audited the accompanying financial statements of Western Electricity Coordinating Council, which comprise the statements of financial position as of December 31, 2013 and 2012, the related statements of activities and cash flows for the years then ended, and the related notes to the financial statements.

Management's responsibility for the financial statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's responsibility

Our responsibility is to express an opinion on these financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of Western Electricity Coordinating Council as of December 31, 2013 and 2012, and the results of its operations and its cash flows for the years then ended in accordance with accounting principles generally accepted in the United States of America.

Grant Thornton LLP

Salt Lake City, Utah
May 27, 2014

FINANCIAL STATEMENTS

Western Electricity Coordinating Council

STATEMENTS OF FINANCIAL POSITION

December 31,

	2013	2012
ASSETS		
Cash and cash equivalents	$ 20,737,074	$ 35,219,275
Contractually restricted cash	4,004,026	4,720,916
Certificates of deposit	2,044,097	1,436,598
Investments	2,942,933	5,930,113
Accounts receivable, net of allowance of $33,283 and $42,458 at December 31, 2013 and 2012, respectively	4,099,826	12,908,228
Prepaid expenses and other assets	1,451,697	835,773
Property, equipment, and software, net	11,042,682	11,964,467
Total assets	$ 46,322,335	$ 73,015,370
LIABILITIES AND NET ASSETS		
LIABILITIES		
Accounts payable	$ 5,380,399	$ 7,557,387
Accrued expenses	4,145,493	1,892,947
Deferred revenue	11,679,055	24,381,993
Other liabilities	1,665,866	7,051,156
Total liabilities	22,870,813	40,883,483
UNRESTRICTED NET ASSETS	23,451,522	32,131,887
Total liabilities and net assets	$ 46,322,335	$ 73,015,370

The accompanying notes are an integral part of these financial statements.

Western Electricity Coordinating Council

STATEMENTS OF ACTIVITIES

Years ended December 31,

Operating Revenue	2013	2012
Electric Reliability Organization Funding	$ 45,329,397	$ 39,233,515
Meetings and workshops	809,510	676,865
Western Renewable Energy Generation Information System (WREGIS)	1,913,930	1,489,043
Federal Grants	11,989,630	27,928,644
Other	1,040	32,805
Total operating revenue	60,043,507	69,360,872
Operating Expenses		
Labor	34,976,986	28,150,057
Office and equipment	9,680,774	8,256,436
Depreciation and amortization	4,541,466	3,766,592
Contract labor and consultants	13,991,057	17,538,997
Meetings	2,559,592	2,472,988
Professional services	1,520,333	1,151,537
Excise taxes	14,745	12,764
Other	1,400,000	16,431
Total operating expenses	68,684,953	61,365,802
(Decrease) increase in unrestricted net assets from operations	(8,641,446)	7,995,070
Nonoperating activity		
Interest and dividend income	255,273	305,601
Net unrealized loss on investments	(88,991)	(56,671)
Net realized loss on investments	(205,201)	(52,102)
Net nonoperating activity	(38,919)	196,828
(Decrease) increase in unrestricted net assets	(8,680,365)	8,191,898
Net assets, beginning of year	32,131,887	23,939,989
Net assets, end of year	$ 23,451,522	$ 32,131,887

The accompanying notes are an integral part of these financial statements.

Western Electricity Coordinating Council

STATEMENTS OF CASH FLOWS

Years ended December 31,

	2013	2012
Cash flows from operating activities		
(Decrease) increase in net assets	$ (8,680,365)	$ 8,191,898
Adjustments to reconcile change in net assets		
to cash (used in) provided by operating activities:		
Depreciation and amortization	4,541,466	3,766,592
Unrealized loss on investments	88,991	56,671
Realized loss on investments	205,201	52,102
Loss on the disposal of fixed assets	182,070	-
Decrease (increase) in assets:		
Accounts receivable	8,808,402	(6,185,664)
Prepaid expenses and other assets	(615,924)	(333,287)
(Decrease) increase in liabilities:		
Accounts payable	(1,861,397)	(748,544)
Accrued expenses	2,252,546	92,063
Deferred revenue	(12,702,938)	3,260,323
Other liabilities	(5,385,290)	159,788
Net cash (used in) provided by operating activities	(13,167,237)	8,311,942
Cash flows from investing activities		
Purchase of property, equipment, and software	(4,117,343)	(5,167,758)
Sales (purchases) of investments - net	2,085,489	328,642
Net cash used in investing activities	(2,031,854)	(4,839,116)
Net increase (decrease) in cash and cash equivalents	(15,199,091)	3,472,826
Cash and cash equivalents, beginning of year	39,940,191	36,467,365
Cash and cash equivalents, end of year	$ 24,741,100	$ 39,940,191
Supplemental disclosures of cash flow information		
Cash paid during the year for interest	$ -	$ -
NON-CASH INVESTING AND FINANCING ACTIVITIES		
Property and equipment financed with accounts payable	$ 315,591	$ 529,354

The accompanying notes are an integral part of these financial statements.

Western Electricity Coordinating Council

NOTES TO FINANCIAL STATEMENTS

December 31, 2013 and 2012

NOTE A – SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES

1. Nature of activities

Western Electricity Coordinating Council (WECC) is a not-for-profit organization whose primary mission is to assure a reliable bulk electric power system in the Western Interconnection. WECC's revenues are generated through performance of statutory and non-statutory activities.

WECC performs statutory activities pursuant to the Delegation Agreement effective October 2007 and Amended and Restated Delegation Agreement effective January 2011 with North American Electric Reliability Corporation (NERC). NERC is the Electric Reliability Organization (ERO) certified by the Federal Energy Regulatory Commission (FERC) to establish and enforce reliability standards for the bulk electric system. Statutory activities authorize WECC to develop, monitor, assess, and enforce compliance with NERC reliability standards and regional standards within the United States portion of the geographic boundaries of the Western Interconnection. Statutory revenues are derived from WECC's statutory funding from NERC, which NERC has delegated WECC to collect through assessments to load-servicing entities (LSEs) within the Western Interconnection.

Non-statutory activities include oversight of the operations of a component of WECC "doing business as" Western Renewable Energy Generation Information System (WREGIS). WREGIS is an independent, renewable energy tracking system within WECC's region. WECC funds its non-statutory activities though annual and other activity fees.

2. Financial statement presentation

WECC's financial statements have been prepared on the accrual basis of accounting, in accordance with accounting principles generally accepted in the United States of America (U.S. GAAP). The information regarding its financial position and activities is reported based on the existence or absence of donor-imposed restrictions in three classes of net assets, as applicable: unrestricted net assets, temporarily restricted net assets, and permanently restricted net assets. As of December 31, 2013 and 2012, WECC had only unrestricted net assets.

3. Use of estimates

The preparation of financial statements in conformity with U.S. GAAP requires management to make estimates and assumptions that affect certain reported amounts of assets and liabilities and disclosure of contingent assets and liabilities as of the date of the financial statements and the reported amounts of revenue and expenses during the reporting period. Accordingly, actual results could differ from those estimates.

NOTE A – SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES – CONTINUED

4. Revenue recognition

WECC recognizes revenue from the statutory funding provided by NERC for performing the statutory activities that have been delegated to WECC. The annual assessments are collected by WECC, remitted first to NERC and then are returned to WECC within a few days. WECC generally receives assessment payments in advance of the assessment period, and records it as assessment payable or as deferred revenue after it has been remitted to NERC and returned to WECC. Assessments are recognized as revenue in the year they are intended to fund. Federal grant revenue is generated through WECC's and WECC sub-recipient's performance of services in accordance with federal award agreements on a cost reimbursement basis.

Other types of revenues, such as non-statutory revenue, are recognized when the services or products have been provided.

WECC can incur penalties assessed by its regulators. When the amounts of such penalties become known or reasonably estimable, WECC recognizes penalty revenue (collected from U.S. LSEs) earmarked for a future year to offset the penalty expense. This results in WECC recording an expense and offsetting revenue. Depending on when the amount of the penalty becomes known (whether it is before or after NERC has approved the budget for the subsequent year), WECC's assessments revenue for the subsequent budget year or the year following will be offset by the amount of the penalty. Such penalties are recorded in the income statement as Electric Reliability Organization Funding and Other operating expenses.

5. Cash and cash equivalents

WECC considers all highly liquid financial instruments with an original maturity of three months or less when purchased to be cash equivalents. Cash and cash equivalents consist of bank demand accounts, money market investment accounts, and other investments. WECC's cash deposits are held with financial institutions in the United States that are insured by the Federal Deposit Insurance Corporation (FDIC). Deposits may exceed the federally insured limits at times.

Pursuant to the Delegation Agreement with NERC, cash equivalents contractually restricted as of December 31, 2013 and 2012 were $4,004,026 and $4,720,916, respectively.

6. Certificates of deposit

Certificates of deposits held by WECC that are not classified as debt securities have original maturities greater than three months.

7. Investments

Investments in marketable securities with readily determinable fair values and all investments in debt securities are reported at their fair values in the statements of financial position. Investment income or loss (including realized gains and losses on investments, interest, and dividends) and unrealized gains and losses on investments are included in the change in net assets.

NOTE A – SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES – CONTINUED

8. Accounts receivable

Accounts receivable consists of statutory funding, grants and other fees receivables that have not been collected. Accounts receivable are carried at original invoice amount less an estimate made for doubtful receivables based on a review of all outstanding amounts on an annual basis. Management determines the allowance for doubtful accounts by identifying troubled accounts and by using historical experience applied to an aging of accounts. Accounts receivable are written off when deemed uncollectible. Recoveries of accounts receivable previously written off are recorded when received.

9. Property, equipment, and software

Expenditures for property, equipment, and software that exceed $5,000 on and individual basis are capitalized at cost and are depreciated using the straight-line method over the estimated useful lives of the assets as follows:

Equipment and software	3 years
Furniture and fixtures	5 years

Leasehold improvements are depreciated over the shorter of the lease term or their estimated useful life of 10 years. Minor replacements, maintenance, and repairs which do not increase the useful lives of the property, equipment, and software to which they are related are expensed as incurred.

10. Impairment of long-lived assets

WECC reviews its long-lived assets for impairment whenever events or changes in circumstances indicate that the carrying amount of the assets may be impaired. If it is determined that the estimated undiscounted future cash flows are not sufficient to recover the carrying value of an asset, an impairment loss is recognized in the statement of activities for the difference between the carrying value and the fair value of the asset.

11. Income taxes

WECC has been recognized by the Internal Revenue Service as a not-for-profit corporation as described in Section 501(c)(6) of the Internal Revenue Code and, as such, is not subject to federal or state income taxes on exempt purpose income. WECC recognized no unrelated business income tax benefit in the years ended December 31, 2013 and 2012.

WECC has identified and evaluated its significant tax positions for which the statute of limitations remain open. The open tax years are the years ended December 31, 2009 through December 31, 2013 for federal tax purposes and Utah tax purposes. WECC applied the more likely than not criteria to all tax positions and determined that no material unrecognized tax benefits or liability should be recognized. In addition, there have been no material changes in unrecognized benefits as of December 31, 2013, and it is not expected that there will be a material change in the 12 months following December 31, 2013. WECC did not incur any tax penalties or tax-related interest expenses during the years ended December 31, 2013 and 2012.

NOTE A – SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES – CONTINUED

12. Functional allocation of expenses

The costs of programs and supporting services have been summarized on a functional basis. WECC's expenses are classified as *Statutory Expenses* or *Non-statutory Expenses* as the majority of expenses incurred fulfill the purposes or mission for which WECC exists. Furthermore, the statutory expenses are classified according to the statutory functions WECC performs pursuant to the Delegation Agreement with NERC. All direct costs are charged to the functional area to which they pertain. Indirect costs are charged to programs and supporting services based on estimates made by management, taking into account the nature of the expense and how it relates to the functional area.

NOTE B – FAIR VALUE MEASUREMENTS

WECC's financial instruments, including cash equivalents, accounts receivable, accounts payable, and accrued liabilities, are carried at cost which approximates their fair value due to the short-term nature of these instruments.

Fair value is defined as the amount that would be received for the sale of an asset or be paid to transfer a liability in an orderly transaction between market participants at the measurement date. In determining fair value, WECC uses various valuation approaches within a hierarchy for inputs used in measuring fair value that maximizes the use of observable inputs and minimizes the use of unobservable inputs by requiring that the most observable inputs be used when available. Observable inputs are inputs that market participants would use in pricing the asset or liability developed based on market data obtained from sources independent of WECC. Unobservable inputs are inputs that reflect WECC's estimates about the assumptions market participants would use in pricing the asset or liability developed based on the best information available in the circumstances. The following hierarchy prioritizes the inputs according to valuation methodologies used to measure fair value:

Level 1: Inputs are quoted prices (unadjusted) in active markets that are accessible for identical assets or liabilities as of the measurement date. Valuation of these products does not entail a significant degree of judgment since it is based on quote prices readily available in an active market. The types of instruments generally included in this category include listed equity securities.

Level 2: Inputs are observable for the asset or liability (either directly or indirectly) as of the measurement date, but are other than quoted prices in active markets as in Level 1. The types of instruments generally included in this category include unlisted derivative financial instruments and fixed income investments.

Level 3: Inputs are unobservable for the instrument and include situations where there is little, if any, market activity for the instrument. The inputs into the determination of fair value require significant judgment or estimation by the reporting entity. The types of instruments generally included in this category include privately held investments, partnership interests and similar interests, and beneficial interests in trusts held by others.

NOTE B – FAIR VALUE MEASUREMENTS – CONTINUED

In certain cases, the inputs used to measure fair value may fall into different levels of the fair value hierarchy. In such cases, for disclosure purposes the level in the fair value hierarchy within which the fair value measurement falls in its entirety is determined based on the lowest level input that is significant to the fair value measurement in its entirety. Fair value is a market-based measure considered from the perspective of a market participant rather than an entity-specific measure. Therefore, even when market assumptions are not readily available, WECC's own assumptions are set to reflect those that WECC believes a market participant would use in pricing the asset or liability at the measurement date.

Assets and liabilities measured at fair value on a recurring basis are summarized as follows:

	Fair Value Measurements as of December 31, 2013			
Description	Level 1	Level 2	Level 3	Total
Cash equivalents:				
Money market funds	$ 12,690,456	$ -	$ -	$ 12,690,456
Investments:				
Corporate bonds	-	502,754	-	502,754
Government agency bonds	-	2,440,179	-	2,440,179
	-	2,942,933	-	2,942,933
	$ 12,690,456	$ 2,942,933	$ -	$ 15,633,389

	Fair Value Measurements as of December 31, 2012			
Description	Level 1	Level 2	Level 3	Total
Cash equivalents:				
Money market funds	$ 35,340,465	$ -	$ -	$ 35,340,465
Commercial paper	-	89,941	-	89,941
	35,340,465	89,941	-	35,430,406
Investments:				
Commercial paper	-	2,138,625	-	2,138,625
Corporate bonds	-	1,128,748	-	1,128,748
Government agency bonds	-	2,501,506	-	2,501,506
Foreign bonds	-	161,234	-	161,234
	-	5,930,113	-	5,930,113
	$ 35,340,465	$ 6,020,054	$ -	$ 41,360,519

Money market funds are valued using observable prices in the active market. Commercial paper, corporate bonds, government agency bonds, and foreign bonds are valued using observable quoted prices of similar securities.

NOTE C – INVESTMENTS

Investments stated at fair value consisted of the following as of December 31:

	2013	2012
Government agency bonds	$ 2,440,179	$ 2,501,506
Corporate bonds	502,754	1,128,748
Commercial paper	-	2,138,625
Foreign bonds	-	161,234
	$ 2,942,933	$ 5,930,113

NOTE D – PROPERTY, EQUIPMENT, AND SOFTWARE

Property, equipment, and software consisted of the following as of December 31:

	2013	2012
Equipment	$ 12,284,835	$ 10,787,879
Software	9,542,253	6,774,760
Leasehold improvements	6,145,304	5,632,787
Furniture and fixtures	695,513	689,655
	28,667,905	23,885,081
Less accumulated depreciation and amortization	(18,972,742)	(14,562,013)
Construction in progress	1,347,519	2,641,399
Property, equipment and software - net	$ 11,042,682	$ 11,964,467

Depreciation and amortization expense for the years ended December 31, 2013 and 2012 was $4,541,466 and $3,766,592, respectively.

Assets purchased with grant funds are secured by a lien on the assets. For the years ended December 31, 2013 and 2012 such assets totaled $7,196,746 and $7,215,063, respectively, net of accumulated depreciation.

NOTE E – ACCOUNTS PAYABLE

Accounts payable consisted of the following as of December 31:

	2013	2012
Assessment payables	$ 4,296,396	$ 4,469,827
Trade payables	1,082,204	2,986,287
Other payables	1,799	101,273
	$ 5,380,399	$ 7,557,387

NOTE F – ACCRUED EXPENSES AND OTHER LIABILITIES

Accrued expenses consisted of the following as of December 31:

	2013	2012
Accrued wages and paid time off	$ 2,279,629	$ 1,672,000
Other accrued expenses	1,654,242	220,947
Accrued employee benefits expense	211,622	140,352
	$ 4,145,493	$ 1,892,947

Other liabilities consisted of the following as of December 31:

	2013	2012
Deferred rents	$ 1,665,866	$ 1,793,598
Subrecipient payable	-	5,257,558
	$ 1,665,866	$ 7,051,156

NOTE G – UNRESTRICTED NET ASSETS

WECC reports information regarding statutory and non-statutory related earnings to the Federal Energy Regulatory Commission in accordance with its Delegation Agreement with NERC dated October 16, 2007 as amended and restated January 1, 2011. As of December 31, the breakdown of such earnings included in unrestricted net assets consisted of the following:

	2013	2012
Non-statutory earnings	$ 8,642,963	$ 7,811,415
Statutory earnings	14,808,559	24,320,472
	$ 23,451,522	$ 32,131,887

NOTE H – COMMITMENTS AND CONTINGENCIES

1. Operating lease commitments

WECC has entered into non-cancelable operating leases for office space and office equipment. Future minimum lease payments under non-cancelable operating leases with terms of one year or more are as follows:

Year Ending December 31:		Amount
2014	$	2,092,821
2015		2,116,135
2016		2,156,515
2017		2,213,848
2018		2,185,758
Thereafter		2,277,703
	$	13,042,781

Total rent expense under non-cancelable operating leases was $2,034,309 and $1,828,431 for the years ended December 31, 2013 and 2012, respectively.

2. Sub-recipient grant

WECC committed up to a total of $22 million in federal grant awards to a sub-recipient. WECC records a payable in sub-recipient payable for payments due for the sub-recipient's performance of services in accordance with federal award agreements on a cost reimbursement basis. As of December 31, 2013 there was no remaining commitment related to this grant.

3. Other matters

WECC may incur a future loss from a monetary penalty assessed by its regulators. The amount of the potential monetary penalty associated with this action is uncertain. During 2013, WECC accrued its reasonable estimate of the expected penalty. Ultimate resolution of this matter could result in a loss that is less than or in excess of the amount accrued.

NOTE I – RETIREMENT PLAN

Employee benefit plan

WECC has a 401(k) Retirement Savings Plan (Plan) for eligible employees. The Plan requires WECC to make matching contributions equal to 50% of the first 6% of eligible compensation of the participating employees' contributions to the Plan. WECC may also make, at its discretion, supplemental contributions for eligible employees. Plan expense reflected in the accompanying statements of activities was $1,802,545 and $1,427,114 for the years ended December 31, 2013 and 2012, respectively.

NOTE J – FUNCTIONAL EXPENSES

The detail of functional expenses for the years ended December 31, are as follows:

Program services	2013	2012
Statutory services	$ 56,316,225	$ 51,997,258
Non-statutory services	927,738	936,470
	57,243,963	52,933,728
Support Services		
Management and general	11,440,990	8,432,074
	$ 68,684,953	$ 61,365,802

NOTE K – SUBSEQUENT EVENTS

WECC has evaluated events occurring between the end of its most recent fiscal year and May 27, 2014, the date the financial statements were available to be issued.

On October 10, 2013, WECC incorporated Peak Reliability (Peak), a not-for-profit organization headquartered in Vancouver, Washington, in preparation for the legal separation of its regional entity function from its reliability coordinator function. On January 1, 2014, Peak began operating as a wholly-owned subsidiary of WECC and assumed WECC's reliability coordinator function. On February 12, 2014, WECC received formal FERC approval of the sub-delegation of WECC's reliability coordinator function to Peak. Subsequent to this date, Peak began to operate independently of WECC (as an unconsolidated entity). Additionally, WECC subsequently transferred to Peak WECC's right, title and interest in all assets directly related to the reliability coordinator function, as well as related liabilities. The assets transferred consisted primarily of fixed assets with a total net book value of approximately $9.4 million and cash and other assets totaling approximately $6.7 million. The liabilities transferred consisted primarily of deferred rent and accrued employee compensation costs and totaled approximately $1.1 million.

ATTACHMENT 10

METRICS CONCERNING ADMINISTRATIVE COSTS IN 2013 NERC AND REGIONAL ENTITY BUDGETS AND ACTUAL COSTS

Analysis of Administrative (Indirect) Costs
2013 Actual and Budget

2013 ACTUAL SPEND

	Total Statutory Expenses & Capital Expenditures	Total Statutory Direct Expenses & Capital Expenditures	Total Statutory Indirect Expenses & Capital Expenditures	% Statutory Indirect to Total Statutory	Statutory Direct Spend per Spend on Indirect
NERC	$ 54,714,887	$ 30,571,766	$ 24,143,121	44.13%	$ 1.27
FRCC	5,864,298	5,249,163	615,135	10.49%	8.53
MRO	8,574,820	5,185,929	3,388,891	39.52%	1.53
NPCC	11,275,494	7,240,821	4,034,673	35.78%	1.79
RFC	17,545,584	11,493,152	6,052,432	34.50%	1.90
SERC	15,880,967	9,677,541	6,203,426	39.06%	1.56
SPP RE	9,681,482	4,568,970	5,112,512	52.81%	0.89
Texas RE	9,536,748	6,400,635	3,136,113	32.88%	2.04
WECC	66,511,396	52,124,780	14,386,616	21.63%	3.62
TOTAL/Average	$ 199,585,676	$ 132,512,757	$ 67,072,919	33.61%	$ 1.98

2013 BUDGET SPEND

	Total Statutory Expenses & Capital Expenditures	Total Statutory Direct Expenses & Capital Expenditures	Total Statutory Indirect Expenses & Capital Expenditures	% Statutory Indirect to Total Statutory	Statutory Direct Spend per Spend on Indirect
NERC	$ 54,286,255	$ 30,909,400	$ 23,376,855	43.06%	$ 1.32
FRCC	$ 6,531,782	$ 5,861,218	$ 670,564	10.27%	8.74
MRO	$ 9,283,539	$ 5,558,189	$ 3,725,350	40.13%	1.49
NPCC	$ 13,879,226	$ 8,969,958	$ 4,909,268	35.37%	1.83
RFC	$ 17,426,838	$ 12,443,206	$ 4,983,632	28.60%	2.50
SERC	$ 15,907,603	$ 10,433,393	$ 5,474,210	34.41%	1.91
SPP RE	$ 11,514,817	$ 6,064,830	$ 5,449,987	47.33%	1.11
Texas RE	$ 10,935,780	$ 7,916,802	$ 3,018,978	27.61%	2.62
WECC	$ 51,025,093	$ 38,697,715	$ 12,327,378	24.16%	3.14
TOTAL/Average	$ 190,790,933	$ 126,854,711	$ 63,936,222	33.51%	$ 1.98

2013 ACTUAL FTEs

	Total Statutory FTEs	Total Statutory Direct FTEs	Total Statutory Indirect FTEs	Indirect FTE as % of Total FTE	# Direct to Indirect Statutory FTEs
NERC	174.75	120.86	53.89	30.84%	2.24
FRCC	28.99	25.92	3.07	10.59%	8.44
MRO	37.91	28.51	9.40	24.80%	3.03
NPCC	35.22	26.22	9.00	25.55%	2.91
RFC	69.80	53.70	16.10	23.07%	3.34
SERC	69.89	51.06	18.83	26.94%	2.71
SPP RE	30.00	25.80	4.20	14.00%	6.14
Texas RE	56.15	43.50	12.65	22.53%	3.44
WECC	227.81	177.57	50.24	22.05%	3.53
TOTAL/Average	730.52	553.14	177.38	24.28%	3.12

2013 BUDGET FTEs

	Total Statutory FTEs	Total Statutory Direct FTEs	Total Statutory Indirect FTEs	Indirect FTE as % of Total FTE	# Direct to Indirect Statutory FTEs
NERC	186.25	133.50	52.75	28.32%	2.53
FRCC	30.12	26.37	3.75	12.45%	7.03
MRO	37.75	27.75	10.00	26.49%	2.78
NPCC	35.86	26.86	9.00	25.10%	2.98
RFC	73.00	57.20	15.80	21.64%	3.62
SERC	77.45	57.52	19.93	25.73%	2.89
SPP RE	34.50	31.25	3.25	9.42%	9.62
Texas RE	60.00	49.25	10.75	17.92%	4.58
WECC	216.30	160.10	56.20	25.98%	2.85
TOTAL/Average	751.23	569.80	181.43	24.15%	3.14

2013 ACTUAL SPEND per FTE

	Total Statutory	Total Statutory Direct	Total Statutory Indirect	Statutory Indirect Spend per Total FTE
NERC	$ 313,104	$ 252,952	$ 448,007	$ 138,158
FRCC	202,287	202,514	200,370	21,219
MRO	226,189	181,899	360,520	89,393
NPCC	320,145	276,156	448,297	114,556
RFC	251,369	214,025	375,927	86,711
SERC	227,228	189,533	329,444	88,760
SPP RE	322,716	177,092	1,217,265	170,417
Texas RE	169,844	147,141	247,914	55,852
WECC	291,960	293,545	286,358	63,152
TOTAL/Average	$ 273,210	$ 239,565	$ 378,131	$ 91,815

2013 BUDGETED SPEND per FTE

	Total Statutory	Total Statutory Direct	Total Statutory Indirect	Statutory Indirect Spend per Total FTE
NERC	$ 291,470	$ 231,531	$ 443,163	$ 125,513
FRCC	216,859	222,268	178,817	22,263
MRO	245,922	200,295	372,535	98,685
NPCC	387,039	333,952	545,474	136,901
RFC	238,724	217,539	315,420	68,269
SERC	205,392	181,387	274,672	70,681
SPP RE	333,763	194,075	1,676,919	157,971
Texas RE	182,263	160,747	280,835	50,316
WECC	235,900	241,710	219,348	56,992
TOTAL/Average	$ 253,971	$ 222,630	$ 352,402	$ 85,109

The accompanying narrative in this filing is essential to understanding the financial information on this schedule

Analysis of Administrative (Indirect) Costs
2011, 2012 and 2013 Actual

2011 ACTUAL SPEND

	Total Statutory Expenses & Capital Expenditures	Total Statutory Direct Expenses & Capital Expenditures	Total Statutory Indirect Expenses & Capital Expenditures	% Statutory Indirect to Total Statutory	Statutory Direct Spend per Spend on Indirect
NERC	$ 51,331,461	$ 29,699,184	$ 21,632,277	42.14%	$ 1.37
FRCC	5,177,020	4,476,298	700,722	13.54%	6.39
MRO	7,385,721	4,593,792	2,791,929	37.80%	1.65
NPCC	11,754,576	9,256,662	2,497,914	21.25%	3.71
RFC	15,158,286	10,361,567	4,796,719	31.64%	2.16
SERC	11,438,066	7,155,166	4,282,900	37.44%	1.67
SPP RE	8,397,845	4,116,846	4,280,999	50.98%	0.96
Texas RE	8,179,402	5,289,369	2,890,033	35.33%	1.83
WECC	57,554,596	46,643,617	10,910,979	18.96%	4.27
TOTAL/Average	$ 176,376,973	$ 121,592,501	$ 54,784,472	31.06%	$ 2.22
3-Year Average					

2012 ACTUAL SPEND

	Total Statutory Expenses & Capital Expenditures	Total Statutory Direct Expenses & Capital Expenditures	Total Statutory Indirect Expenses & Capital Expenditures	% Statutory Indirect to Total Statutory	Statutory Direct Spend per Spend on Indirect
NERC	$ 51,200,212	$ 30,071,355	$ 21,128,857	41.27%	$ 1.42
FRCC	5,519,156	4,918,683	600,473	10.88%	8.19
MRO	8,819,027	4,607,445	4,211,582	47.76%	1.09
NPCC	12,916,639	10,619,055	2,297,584	17.79%	4.62
RFC	16,014,703	10,712,245	5,302,458	33.11%	2.02
SERC	13,271,927	8,658,435	4,613,492	34.76%	1.88
SPP RE	9,552,118	4,400,658	5,151,460	53.93%	0.85
Texas RE	9,031,959	5,991,084	3,040,875	33.67%	1.97
WECC	62,137,704	51,286,671	10,851,033	17.46%	4.73
TOTAL/Average	$ 188,463,445	$ 131,265,631	$ 57,197,814	30.35%	$ 2.29
3-Year Average					

2013 ACTUAL SPEND

	Total Statutory Expenses & Capital Expenditures	Total Statutory Direct Expenses & Capital Expenditures	Total Statutory Indirect Expenses & Capital Expenditures	% Statutory Indirect to Total Statutory	Statutory Direct Spend per Spend on Indirect
NERC	$ 54,714,887	$ 30,571,766	$ 24,143,121	44.13%	$ 1.27
FRCC	5,864,298	5,249,163	615,135	10.49%	8.53
MRO	8,574,820	5,185,929	3,388,891	39.52%	1.53
NPCC	11,275,494	7,240,821	4,034,673	35.78%	1.79
RFC	17,545,584	11,493,152	6,052,432	34.50%	1.90
SERC	15,880,967	9,677,541	6,203,426	39.06%	1.56
SPP RE	9,681,482	4,568,970	5,112,512	52.81%	0.89
Texas RE	9,536,748	6,400,635	3,136,113	32.88%	2.04
WECC	66,511,396	52,124,780	14,386,616	21.63%	3.62
TOTAL/Average	$ 199,585,676	$ 132,512,757	$ 67,072,919	33.61%	$ 1.98
3-Year Average				31.72%	$ 2.15

2011 ACTUAL FTEs

	Total Statutory FTEs	Total Statutory Direct FTEs	Total Statutory Indirect FTEs	Indirect FTE as % of Total FTE	# Direct to Indirect Statutory FTEs
NERC	140.25	101.04	39.21	27.96%	2.58
FRCC	25.48	21.15	4.33	16.99%	4.88
MRO	32.97	24.47	8.50	25.78%	2.88
NPCC	29.83	23.08	6.75	22.63%	3.42
RFC	62.05	48.77	13.28	21.40%	3.67
SERC	56.70	43.95	12.75	22.49%	3.45
SPP RE	26.38	22.51	3.87	14.67%	5.82
Texas RE	42.70	31.60	11.10	26.00%	2.85
WECC	188.70	146.80	41.90	22.20%	3.50
TOTAL/Average	605.06	463.37	141.69	23.42%	3.27
3-Year Average					

2012 ACTUAL FTEs

	Total Statutory FTEs	Total Statutory Direct FTEs	Total Statutory Indirect FTEs	Indirect FTE as % of Total FTE	# Direct to Indirect Statutory FTEs
NERC	167.83	116.03	51.80	30.86%	2.24
FRCC	25.42	21.22	4.20	16.52%	5.05
MRO	35.44	25.14	10.30	29.06%	2.44
NPCC	33.34	25.42	7.92	23.76%	3.21
RFC	65.46	49.58	15.88	24.26%	3.12
SERC	68.70	52.95	15.75	22.93%	3.36
SPP RE	29.77	26.27	3.50	11.76%	7.51
Texas RE	51.29	38.79	12.50	24.37%	3.10
WECC	199.93	154.88	45.05	22.53%	3.44
TOTAL/Average	677.18	510.28	166.90	24.65%	3.06
3-Year Average					

2013 ACTUAL FTEs

	Total Statutory FTEs	Total Statutory Direct FTEs	Total Statutory Indirect FTEs	Indirect FTE as % of Total FTE	# Direct to Indirect Statutory FTEs
NERC	174.75	120.86	53.89	30.84%	2.24
FRCC	28.99	25.92	3.07	10.59%	8.44
MRO	37.91	28.51	9.40	24.80%	3.03
NPCC	35.22	26.22	9.00	25.55%	2.91
RFC	69.80	53.70	16.10	23.07%	3.34
SERC	69.89	51.06	18.83	26.94%	2.71
SPP RE	30.00	25.80	4.20	14.00%	6.14
Texas RE	56.15	43.50	12.65	22.53%	3.44
WECC	227.81	177.57	50.24	22.05%	3.53
TOTAL/Average	730.52	553.14	177.38	24.28%	3.12
3-Year Average				24.14%	3.14

2011 ACTUAL SPEND per FTE

	Total Statutory	Total Statutory Direct	Total Statutory Indirect	Statutory Indirect Spend per Total FTE
NERC	$ 366,000	$ 293,935	$ 551,703	$ 154,241
FRCC	203,180	211,645	161,830	27,501
MRO	224,013	187,732	328,462	84,681
NPCC	394,052	401,069	370,061	83,738
RFC	244,291	212,458	361,199	77,304
SERC	201,730	162,802	335,914	75,536
SPP RE	318,341	182,890	1,106,201	162,282
Texas RE	191,555	167,385	260,363	67,682
WECC	305,006	317,736	260,405	57,822
TOTAL/Average	$ 291,503	$ 262,409	$ 386,650	$ 90,544
3-Year Average				

2012 ACTUAL SPEND per FTE

	Total Statutory	Total Statutory Direct	Total Statutory Indirect	Statutory Indirect Spend per Total FTE
NERC	$ 305,072	$ 259,169	$ 407,893	$ 125,894
FRCC	217,119	231,795	142,970	23,622
MRO	248,844	183,271	408,891	118,837
NPCC	387,422	417,744	290,099	68,914
RFC	244,649	216,060	333,908	81,003
SERC	193,187	163,521	292,920	67,154
SPP RE	320,864	167,516	1,471,846	173,042
Texas RE	176,096	154,449	243,270	59,288
WECC	310,797	331,138	240,866	54,274
TOTAL/Average	$ 278,306	$ 257,242	$ 342,707	$ 84,465
3-Year Average				

2013 ACTUAL SPEND per FTE

	Total Statutory	Total Statutory Direct	Total Statutory Indirect	Statutory Indirect Spend per Total FTE
NERC	$ 313,104	$ 252,952	$ 448,007	$ 138,158
FRCC	202,287	202,514	200,370	21,219
MRO	226,189	181,899	360,520	89,393
NPCC	320,145	276,156	448,297	114,556
RFC	251,369	214,025	375,927	86,711
SERC	227,228	189,533	329,444	88,760
SPP RE	322,716	177,092	1,217,265	170,417
Texas RE	169,844	147,141	247,914	55,852
WECC	291,960	293,545	286,358	63,152
TOTAL/Average	$ 273,210	$ 239,565	$ 378,131	$ 91,815
3-Year Average	$ 281,007	$ 253,072	$ 369,163	$ 88,941

The accompanying narrative in this filing is essential to understanding the financial information on this schedule

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

MOTION TO DISCONTINUE COMPLIANCE OBLIGATION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO PARAGRAPH 629 OF ORDER NO. 693

In its March 16, 2007 Order,[1] the Federal Energy Regulatory Commission ("FERC" or the "Commission") directed the North American Electric Reliability Corporation ("NERC" or "ERO") to provide a quarterly informational filing regarding the timeframe to restore power to the auxiliary power systems of U.S. nuclear power plants following a blackout as determined during simulations and drills of system restoration plans. Pursuant to Rule 212 of the Commission's Rules of Practice and Procedure, 18 C.F. R. § 385.212 (2012), NERC hereby submits this motion requesting that the Commission discontinue NERC's obligations to (i) collect data and (ii) provide quarterly informational filings pursuant to the Commission's directive in Paragraph 629 of Order No. 693.

The purpose of conducting the data collection has been superseded by the development of Reliability Standard NUC-001-2 (Nuclear Plant Interface Coordination) and Reliability Standard EOP-005-2 (System Restoration from Blackstart Resources),

[1] *Mandatory Reliability Standards for the Bulk-Power System*, 118 FERC ¶ 61,218, FERC Stats. & Regs. ¶ 31,242, P 629 (Order No. 693), *Order on reh'g, Mandatory Reliability Standards for the Bulk-Power System*, 120 FERC ¶ 61,053 (Order No. 693-A) (2007).

which were approved by the Commission on January 21, 2010[2] and March 17, 2011[3], respectively. Further, after twenty-five quarters of data collection and reporting, NERC and the Commission now have a set of data points for each U.S. nuclear power plant.[4]

Finally, because the development of quarterly reports requires the outlay of substantial resources by Transmission Operators who collect and forward the information to the Regional Entity, by the Regional Entity which accumulates and assembles the data, and by NERC which combines the information into the filings and generate reports, NERC is seeking to redirect these industry, regional, and NERC resources to other reliability-related activities that impact the Bulk-Power System.

I. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[5]

[2] *North American Electric Reliability Corporation*, 130 FERC ¶ 61,051 (2010).

[3] *System Restoration Reliability Standards*, Order No. 749, 134 FERC ¶ 61,215 (2011).

[4] Upon Board of Trustees approval, NERC began to collect nuclear data from U.S. Transmission Operators during the fourth quarter of 2007 and has continued to collect and report the data to the Commission on a quarterly basis.

[5] Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of 18 C.F.R. § 385.203(b) to permit the inclusion of more than two people on the service list.

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

Charles A. Berardesco*****
Senior Vice President, General Counsel and
Corporate Secretary
Holly A. Hawkins*****
Associate General Counsel
Brady A. Walker*****
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
brady.walker@nerc.net

II. BACKGROUND

In Order No. 693, in response to comments offered by the U.S. Nuclear Regulatory Commission ("NRC") during the Notice of Proposed Rulemaking process, the Commission expressed its concern regarding the role and priority that nuclear power plants should have in Bulk-Power System restoration plans.[6] The NRC comments suggested that Reliability Standard EOP-005-1 include: (1) a requirement to record the amount of time required to restore power to the auxiliary power systems of nuclear power plants; (2) a provision requiring the affected transmission operators give high priority to restoration of off-site power to nuclear power plants even if a nuclear power plant is being powered from the nuclear power plant's onsite power supply, and (3) a provision stating that restoration shall not violate nuclear power plant minimum voltage and frequency requirements.[7] The Commission addressed the concern in its discussion of

[6] Order No. 693 at P 629.
[7] *See* NRC Dec. 28, 2006 Comments, Docket No. RM06-16-000 at 3-4.

Reliability Standard EOP-005-1 (System Restoration Plans). In Paragraph 629 of Order No. 693, the Commission issued the following directive:

> [t]he Commission directs the ERO to gather data, pursuant to § 39.5(f) of the Commission's regulations, from simulations and drills of system restoration on the time it takes to restore power to the auxiliary power systems of nuclear power plants under its data gathering authority and report that information to the Commission on a quarterly basis.

NERC, in its role as the ERO and in accordance with 18 C.F.R. § 39.2(d) (2012), is required to provide information as necessary to the Commission in order to implement section 215 of the Federal Power Act. That same regulation obligates users, owners, and operators of the Bulk-Power System to provide the ERO with information in support of this same objective. As noted above, NERC began collecting data in the fourth quarter of 2007 pursuant to the directive in Order No. 693 and has done so for twenty-five consecutive quarters.

III. MOTION TO DISCONTINUE PARAGRAPH 629 COMPLIANCE OBLIGATION

NERC respectfully requests the discontinuance of the compliance obligation under Paragraph 629 for three reasons, each of which is addressed below. First, since the issuance of Order No. 693 in March 2007, NERC has addressed the issues raised by the NRC in Order No. 693 through the development and approval of Reliability Standards NUC-001-2 and EOP-005-2. These Reliability Standards create a broader approach, and specifically address the off-site power capability concerns of the NRC. Second, the Commission and NERC have collected extensive sets of data on each of the nuclear plants in response to the directive in Paragraph 629. Lastly, because the purpose behind the data collection is now being accomplished by the much broader Reliability Standards

mentioned above, NERC can more efficiently utilize the time and resources of NERC, Regional Entities, and Transmission Operators to accomplish other reliability efforts.

A. Development of Two Reliability Standards with Broader Approach

1. Reliability Standard NUC-001-2

Since the issuance of Order No. 693 in March 2007, Reliability Standard NUC-001-2.1 (Nuclear Plant Interface Coordination) has been approved by the Commission, and contains explicit Requirements that address the off-site power concerns expressed by the NRC. Specifically, Reliability Standard NUC-001-2 requires a Nuclear Plant Generator Operator to coordinate operations and planning with Transmission Entities providing services relating to nuclear plant operating and off-site power delivery requirements. Reliability Standard NUC-001-2 also requires Nuclear Plant Generator Operators and Transmission Entities to implement interface agreements setting forth expectations and procedures for coordinating operations to meet the nuclear plant licensing requirements and System Operating Limits affecting nuclear plant operations.

As an example of how Reliability Standard NUC-001-2.1 provides a broader approach to the Commission directive in Order No. 693, currently-effective Requirement R9.2.2 of Reliability Standard NUC-001-2 requires Nuclear Plant Generator Operators to identify facilities, components, and configuration restrictions that are essential for meeting the Nuclear Interface Plant Requirements ("NPIRs"). Requirement R9.3.4 includes provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entities lose the ability to assess the capability of the electric system to meet the NPIRs. These provisions also include the obligation to notify the Nuclear Plant Generator Operator of this information within a specified time frame.

Additionally, Requirement R9.3.5 of Reliability Standard NUC-001-2 includes provisions for considering, during the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power. Requirement R4 provides that the applicable Transmission Entities shall incorporate the NPIRs into their operating analyses of the Bulk-Electric System, operate the Bulk-Electric System to meet the NPIRs, and inform the Nuclear Plant Generator Operator when the ability to assess the operation of the Bulk-Electric System is lost.

2. Reliability Standard EOP-005-2

In addition to the approval of Reliability Standard NUC-001-2, the Commission stated in its approval of Reliability Standard EOP-005-2 in Order No. 749 that Reliability Standard EOP-005-2 effectively addresses the Commission's directive in Order No. 693 to develop timeframes for training and review of restoration plan requirements to simulate contingencies and prepare operators for anticipated and unforeseen events.[8] The purpose of Reliability Standard EOP-005-2 is to ensure plans, facilities, and personnel are prepared to enable system restoration from Blackstart Resources, and to ensure that reliability is maintained during restoration and priority is placed on restoring the Interconnection. Requirement R1.2 of Reliability Standard EOP-005-2 provides that the Transmission Operator shall have a Reliability Coordinator-approved restoration plan that includes "[a] description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration."

[8] *See System Restoration Reliability Standards*, Order No. 749, 134 FERC ¶ 61,215 at P 17. *See also System Restoration Reliability Standards*, Notice of Proposed Rulemaking, 133 FERC ¶ 61,161 at P 19 (2010).

Requirements R3 and R4 set forth time frames for review of restoration plans. Frequency of testing Blackstart Resources is addressed in Requirement R9, and Requirement R6 requires each transmission operator to verify every five years through analysis of actual events, testing, or steady state and dynamic simulations that the restoration plan accomplishes its intended function. Requirements R10, R11 and R17 address training requirements.

B. Existing Nuclear Data Points

NERC has collected data from U.S. Transmission Operators pursuant to its obligation under Paragraph 629 of Order No. 693 since the fourth quarter of 2007. This information, which is collected by U.S. Transmission Operators, submitted to Regional Entities, then delivered to NERC for submission the Commission, includes a comprehensive collection of nuclear data including the following: identification of the reporting entity; name of the exercise, drill or simulation; date of the exercise, drill or simulation; name of the nuclear plant; unit designation; identification of the off-site power source; time duration measured from the time off-site power sources are lost to the time of restoration of the first off-site power source; and discussion of scenario assumptions or constraints impacting the restoration of the first off-site power source to the nuclear power plant. Because the information collected by NERC and reported to the Commission over the previous twenty-five quarters has been thorough and complete, NERC and the Commission have an extensive collection of accurate data points with regard to nuclear plants in the Commission's jurisdiction.

C. Unnecessary Utilization of Resources

The quarterly reports submitted to the Commission require a substantial expenditure of time, effort, and other valuable resources by Transmission Operators,

Regional Entities, NERC, and the industry as a whole. These are resources that could be utilized to accomplish more important reliability-related activities designed to improve the resiliency of the Bulk Power System. As described above, Transmission Operators, Regional Entities, and NERC have independent responsibilities related to the reporting requirements prescribed by Order No. 693. For example, Transmission Operators conduct a series of drills and exercises to collect information regarding the service restoration times for auxiliary power systems of nuclear power plants, and forward that information to their respective Regional Entities. Upon receipt of this information, the Regional Entities coordinate the collection of the requested data from its members and prepare a composite presentation. This is data which must then be validated by the Transmission Operators prior to submittal to NERC. Once NERC has received these data sets, NERC officials combine the information into cognizable filings and generate reports for final submission to the Commission.

As explained above, these filings and reports submitted to the Commission by NERC contain redundant and, in many cases, less robust, data than is provided to the Commission through Reliability Standards NUC-001-2.1 and EOP-005-2. Because the information provided to NERC and the Commission by these Reliability Standards is more than enough to satisfy the Commission's directive in Paragraph 629 of Order No. 693 and because NERC and the Commission already have extensive data related to U.S. nuclear power plants, NERC requests the ability to utilize these valuable resources in a more effective manner.

IV. CONCLUSION

In summary, on the basis that the more explicit Requirements contained in Reliability Standards NUC-001-2 and EOP-005-2 specifically address the off-site power

capability concerns of the NRC and establish timeframes for training and review of restoration plan requirements, and because NERC and the Commission have collected a series of data points regarding existing nuclear plants over the course of the last twenty-five quarters, NERC requests that the Commission discontinue NERC's obligation to collect and report this data, a Commission directive contained in Paragraph 629 of Order No. 693, and allow NERC to redirect the resources required by these obligations to other reliability-related matters.

Respectfully submitted,

/s/ Brady A. Walker
Brady A. Walker
Counsel for North American Electric Reliability Corporation

CERTIFICATE OF SERVICE

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

Dated at Washington, District of Columbia this 30th day of May, 2014.

/s/ Brady A. Walker
Brady A. Walker
Counsel for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD CIP-014-1

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

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Associate General Counsel
Shamai Elstein
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

May 23, 2014

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 2
II. NOTICES AND COMMUNICATIONS 7
III. BACKGROUND 7
A. Regulatory Framework 7
B. NERC Reliability Standards Development Procedure 8
C. The Physical Security Order 9
D. Procedural History of Proposed Reliability Standard CIP-014-1 13
IV. JUSTIFICATION FOR APPROVAL 15
A. Purpose and Overview of the Proposed Reliability Standard 15
B. Scope and Applicability of the Proposed Reliability Standard 17
C. Requirements in the Proposed Reliability Standard 29
D. Protection of Sensitive or Confidential Information 51
E. Enforceability of the Proposed Reliability Standards 53
V. EFFECTIVE DATE 54
VI. CONCLUSION 56

Exhibit A Proposed Reliability Standard
Exhibit B Implementation Plan
Exhibit C Order No. 672 Criteria
Exhibit D Consideration of Directives
Exhibit E Analysis of Violation Risk Factors and Violation Security Levels
Exhibit F Summary of Development History and Record of Development
Exhibit G Standard Drafting Team Roster

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD CIP-014-1

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA"),[1] Section 39.5 of the regulations of the Federal Energy Regulatory Commission ("FERC" or "Commission"),[2] and the Commission's March 7, 2014 order issued in Docket No. RD14-6-000,[3] the North American Electric Reliability Corporation ("NERC")[4] hereby submits for Commission approval proposed Reliability Standard CIP-014-1 – Physical Security. NERC requests that the Commission approve the proposed Reliability Standard (Exhibit A) as just, reasonable, not unduly discriminatory, or preferential, and in the public interest.[5] NERC also requests approval of (i) the associated Implementation Plan (Exhibit B), and (ii) the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibits A and E), as detailed in this Petition.

As required by Section 39.5(a) of the Commission's regulations,[6] this Petition presents the technical basis and purpose of proposed Reliability Standard CIP-014-1, a summary of its

---

1 16 U.S.C. § 824o (2006).

2 18 C.F.R. § 39.5 (2014).

3 *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014) (the "Physical Security Order").

4 The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006).

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

6 18 C.F.R. § 39.5(a) (2013).

development history (Exhibit F) and a demonstration that the proposed Reliability Standard meets the criteria identified by the Commission in Order No. 672[7] (Exhibit C). The NERC Board of Trustees adopted proposed Reliability Standard CIP-014-1 and the associated Implementation Plan on May 13, 2014.

I. EXECUTIVE SUMMARY

The Bulk-Power System is one of North America's most critical infrastructures and is uniquely critical as other infrastructure sectors depend on electric power. The reliability and security of the Bulk-Power System is fundamental to national security, economic development, and public health and safety. A major disruption in electric service due to extreme weather, equipment failure, a cybersecurity incident, or a physical attack could have far-reaching effects. Owners and operators of the Bulk-Power System must therefore institute measures to protect against and mitigate the impact of both conventional risks (e.g., extreme weather and equipment failures) and emerging security risks, such as physical attacks intended to damage or disable critical elements of the Bulk-Power System. As the Commission recognized in the Physical Security Order, "[p]hysical attacks to critical Bulk-Power System facilities can adversely impact the reliable operation of the Bulk-Power System, resulting in instability, uncontrolled separation, or cascading failures."[8] The purpose of the proposed Reliability Standard is to enhance physical security measures for the most critical Bulk-Power System facilities and thereby lessen the overall vulnerability of the Bulk-Power System to physical attacks.[9]

---

[7] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, at P 262, 321-37, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[8] Physical Security Order at P 5.

[9] NERC's Reliability Standards already includes numerous Reliability Standards addressing both conventional risks and cybersecurity risks. Consistent with the Physical Security Order, the proposed Reliability Standard focuses on bolstering mandatory requirements addressing physical security risks.

The Commission's Physical Security Order provides a framework for a mandatory Reliability Standard that will represent a significant step forward in securing North America's most critical Bulk-Power System facilities. Proposed Reliability Standard CIP-014-1 requires Transmission Owners and Transmission Operators to protect those critical Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Consistent with the Physical Security Order, the proposed Reliability Standard requires Transmission Owners to take the following steps to address the risks that physical attacks pose to the reliable operation of the Bulk-Power System:

1) Perform a risk assessment of their systems to identify (i) their critical Transmission stations and Transmission substations, and (ii) the primary control centers that operationally (i.e., physically) control the identified Transmission stations and Transmission substations.

2) Evaluate the potential threats and vulnerabilities of a physical attack to the facilities identified in the risk assessment.

3) Develop and implement a security plan, based on the evaluation of threats and vulnerabilities, designed to protect against and mitigate the impact of physical attacks that may compromise the operability or recovery of the identified critical facilities.

Further, the proposed Reliability Standard requires Transmission Operators that operate primary control centers that operationally control any of the Transmission stations or substations identified by the Transmission Owner to also:

1) evaluate the potential threats and vulnerabilities of a physical attack to such primary control centers; and

2) develop and implement a security plan, based on the evaluation of threats and vulnerabilities, designed to protect against and mitigate the impact of physical attacks that may compromise the operability or recovery of such primary control centers.

Additionally, proposed Reliability Standard CIP-014-1 includes requirements for: (i) the protection of sensitive or confidential information from public disclosure; (ii) third party

verification of the identification of critical facilities as well as third party review of the evaluation of threats and vulnerabilities and the security plans; and (iii) the periodic reevaluation and revision of the identification of critical facilities, the evaluation of threats and vulnerabilities, and the security plans to help ensure their continued effectiveness.

The proposed Reliability Standard continues NERC's longstanding efforts to provide for the reliability and security of the Bulk-Power System. Even before the advent of mandatory Reliability Standards, NERC made grid security a priority, working with industry participants to address both physical and cyber security threats to critical assets. NERC currently addresses physical security through a combination of reliability tools, including security guidelines, training exercises, alerts, and mandatory standards. NERC's ongoing activities to addresses physical security issues include the following:

- NERC's Electricity Sector Information Sharing and Analysis Center ("ES-ISAC") monitors and analyzes Bulk-Power System events. The ES-ISAC then issues alerts through a secure portal to inform industry of physical and cyber threats, and to advise mitigation actions.
- NERC has security guidelines covering physical security response, best practices, and substation security.[10]
- Mandatory Reliability Standards that address certain aspects of physical security, including Reliability Standard EOP-004-2, which requires registered entities to report to NERC and law enforcement any physical damage to or destruction of a facility or threats to damage or destroy a facility, and Reliability Standard CIP-006-5, which includes requirements for the management of physical access to BES Cyber Systems.[11]
- NERC's Critical Infrastructure Protection Committee ("CIPC") was formed to advance the physical and cyber security of the critical electricity infrastructure of North America. Among other things, CIPC issues security guidelines and coordinates and communicates

[10] These guidelines address the following topics: (1) potential risks, (2) best practices that can help mitigate risks, (3) determination of organizational risks and practices appropriate to manage those risks, (4) identification of actions that industry should consider when responding to threat alerts received from the ES-ISAC and other organizations, (5) the scope of actions each organization may implement for its specific response plan, and (6) assessing and categorizing vulnerabilities and risks to critical facilities and functions.

[11] FERC approved Reliability Standard CIP-006-5 and it will becomes effective on April 1, 2016. CIP-006-5 replaces CIP-006-3c, which requires a physical security program for the protection of Critical Cyber Assets.

with organizations responsible for physical and cyber security in all electric industry segments, as well as other critical infrastructure sectors as appropriate.[12]

- NERC hosts grid security exercises, most recently GRIDEX II, to provide training and education opportunities for industry and government participants across North America.
- NERC hosts an annual Grid Security Conference ("GridSecCon") where experts discuss in detail a range of physical security issues.[13]
- NERC regularly participates in energy sector classified briefings both in the United States and Canada.
- NERC regularly works with industry and government partners on security matters through both formal and informal structures.[14]

This multi-pronged approach provides a framework for addressing the dynamic issues of physical and cyber security and helps to ensure a secure and reliable Bulk-Power System for North America. NERC's actions following a physical security incident at a California substation in April 2013 illustrate how NERC uses its multi-pronged approach to inform industry of security incidents and provide guidance on steps to mitigate and protect against future attacks.[15] Immediately after the incident, NERC's ES-ISAC issued an alert to industry to raise awareness of the seriousness and sophistication of the incident. Following this initial alert, NERC continued to work with the owner of the transmission substation to learn about the incident and communicate lessons learned to the industry. Additionally, NERC planned and participated in a 13-city outreach effort across the U.S. and Canada to raise awareness of the incident, inform industry of tactics and tools to

[12] The CIPC has a Physical Security Subcommittee that regularly discusses and analyzes physical security issues for education and awareness among the industry.

[13] NERC provides free physical security training in association with GridSecCon.

[14] For instance, NERC participates in the Electricity Sub-sector Coordinating Council, which provides a forum for communication between public and private sector partners in the Electricity Sub-sector

[15] The April 2013 incident did not result in a power outage. The owner of the substation worked diligently to maintain reliable operations and share lessons learned with government authorities and industry.

mitigate similar security risks, and provide a forum for industry participants to meet with state, local, and federal authorities to discuss physical security concerns in their regions.[16]

Although physical threats to the Bulk-Power System are not new, they are evolving and, as the incident in California illustrates, continue to demand NERC's and the industry's attention. The proposed Reliability Standard will enhance NERC's foundational physical security efforts and help ensure that owners and operators of the Bulk-Power System take the necessary steps to protect the Bulk-Power System from physical attacks. Additionally, as discussed further below, in approving proposed Reliability Standard CIP-014-1, the NERC Board of Trustees instructed NERC management to monitor and assess the implementation of the proposed Reliability Standard and provide regular updates to the Board of Trustees to measure the effectiveness of industry's implementation of the proposed Reliability Standard.

For the reasons discussed herein, NERC respectfully requests that the Commission approve the proposed Reliability Standard as just, reasonable, not unduly discriminatory, or preferential and in the public interest.

[16] This outreach effort involved, among others, NERC's ES-ISAC, the Department of Energy, FERC, the Department of Homeland Security, and the Federal Bureau of Investigation.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[17]

Charles A. Berardesco*
Senior Vice President and General Counsel
Holly A. Hawkins*
Associate General Counsel
Shamai Elstein*
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Valerie Agnew*
Director of Standards Development
Steven Noess*
Associate Director of Standards Development
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560
valerie.agnew@nerc.net
steven.noess@nerc.net

III. BACKGROUND

A. Regulatory Framework

By enacting the Energy Policy Act of 2005,[18] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Nation's Bulk-Power System, and with the duty of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215(b)(1)[19] of the FPA states that all users, owners, and operators of the Bulk-Power System in the United States will be subject to Commission-approved Reliability Standards. Section 215(d)(5)[20] of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability

[17] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203 (2013), to allow the inclusion of more than two persons on the service list in this proceeding.

[18] 16 U.S.C. § 824o (2006).

[19] *Id.* § 824(b)(1).

[20] *Id.* § 824o(d)(5).

Standard. Section 39.5(a)[21] of the Commission's regulations requires the ERO to file for Commission approval each Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to make effective.

The Commission has the regulatory responsibility to approve Reliability Standards that protect the reliability of the Bulk-Power System and to ensure that such Reliability Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest. Pursuant to Section 215(d)(2) of the FPA[22] and Section 39.5(c)[23] of the Commission's regulations, the Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard.

B. NERC Reliability Standards Development Procedure

The proposed Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[24] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[25] In its ERO Certification Order, the Commission found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain of the criteria for approving Reliability

---

21 18 C.F.R. § 39.5(a) (2012).

22 16 U.S.C. § 824o(d)(2).

23 18 C.F.R. § 39.5(c)(1).

24 *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672 at P 334, FERC Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

25 The NERC Rules of Procedure are available at http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx. The NERC Standard Processes Manual is available at http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

Standards. The development process is open to any person or entity with a legitimate interest in the reliability of the Bulk-Power System. NERC considers the comments of all stakeholders, and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard before NERC submits the Reliability Standard to the Commission for approval.

C. The Physical Security Order

On March 7, 2014, the Commission issued the Physical Security Order directing NERC to submit for approval, within 90 days of the order, one or more Reliability Standards to address physical security risks and vulnerabilities of critical facilities on the Bulk-Power System. Although the Commission recognized that NERC and the industry have "engaged in longstanding efforts to address the physical security of its critical facilities,"[26] the Commission maintained that "to carry out section 215 of the FPA and to provide for the reliable operation of the Bulk-Power System," it was necessary to develop a mandatory Reliability Standard to "specifically require entities to take steps to reasonably protect against physical security attacks on the Bulk-Power System."[27]

The Commission stated that the Reliability Standard(s) should require owners and operators of the Bulk-Power System to take a least three steps:

- First, they should be required to "perform a risk assessment of their systems to identify their 'critical facilities.'"[28]
- Second, they should be required to "evaluate the potential threats and vulnerabilities to those identified critical facilities."[29]

---

[26] Physical Security Order at P 12.

[27] *Id*. at P 5.

[28] *Id*. at P 6.

[29] *Id*. at P 8.

- Third and finally, they should be required to "develop and implement a security plan designed to protect against attacks to their critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security."[30]

Additionally, the Commission stated that the proposed Reliability Standard(s) should also include: (1) procedures to ensure confidential treatment of sensitive or confidential information; (2) procedures for a third party to verify the list of identified facilities and allow the verifying entity, as well as the Commission, to add or remove facilities from the list of critical facilities; (3) procedures for a third party to review of the evaluation of threats and vulnerabilities and the security plan; and (4) a requirement that the identification of the critical facilities, the evaluation of the potential threats and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness.

The following is a brief discussion of each of the elements that the Commission stated should be included in any proposed Reliability Standard.

Identification of Critical Facilities: The Commission explained that the purpose of the risk assessment to identify critical facilities is to "ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System."[31] As such, the Commission explained, a "critical facility" for purposes of the Physical Security Order "is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk Power System."[32] The

---

30 Physical Security Order at P 9.

31 *Id*. at P 6.

32 *Id*. at P 6. The Commission recognized that "owners and operators may also take steps to protect facilities necessary to serve critical load on their systems, even if the inoperability or damage to those facilities would not result in instability, uncontrolled separation or cascading failures on the Bulk-Power System." *Id*. at n. 5. However, the Commission continued, the Reliability Standards should have a narrower purpose and apply only to

Commission explained that critical facilities will generally include critical substations and control centers.[33]

The Commission specified that "methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment," but did not require NERC to adopt a specific type of risk assessment, nor did the Commission require that a mandatory number of facilities be identified as critical facilities under the Reliability Standard(s).[34] The Commission stated, however, that it did not expect there to be a large number of critical facilities identified under the any proposed Reliability Standard:

> Under the Reliability Standards, we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard.[35]

Evaluation of Threats and Vulnerabilities: The Commission recognized that "threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target."[36] Thus, the Commission stated, "the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated."[37] The Commission also stated that NERC should consider whether to

---

critical facilities that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. *Id*.

33 Physical Security Order at n. 6.

34 *Id*. at P 6.

35 *Id*. at P 12.

36 *Id*. at P 8.

37 *Id*. at P 8.

require owners and operators to consult with entities with appropriate expertise as part of the evaluation process.[38]

Development and Implementation of a Security Plan: For the third step, the Commission recognized that there is not a "one size fits all" response to protect against physical security threats.[39] The Commission stated, however, that while the proposed Reliability Standard(s) need not "dictate specific steps an entity must take to protect against attacks on the identified facilities," it must "require that owners or operators of identified critical facilities have a plan that results in an adequate level of protection against the potential physical threats and vulnerabilities they face at the identified critical facilities."[40]

The Commission also stated that the Reliability Standard should allow applicable entities to consider elements of resiliency in carrying out these three steps, including system design, operation, and maintenance, and the sophistication of recovery plans and inventory management.[41]

Third Party Verification and Review: The Commission stated that the Reliability Standard should require that "the risk assessment used by an owner or operator to identify critical facilities [] be verified by an entity other than the owner or operator."[42] Additionally, the Physical Security Order provides that any proposed Reliability Standard "should include a procedure for the verifying entity, as well as the Commission, to add or remove facilities from an owner's or operator's list of critical facilities."[43] Similarly, the Commission stated that under the Reliability Standard the "determination of threats and vulnerability and the security plan should also be

---

38 Physical Security Order at P 8.

39 *Id*. at P 2.

40 *Id*. at P 9.

41 *Id.* at P 7.

42 *Id*. at P 11.

43 *Id*. at P 11.

reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise."[44]

Reevaluation and Revision: Given the dynamic nature of the Bulk-Power System and physical security threats, the Physical Security Order provides that any proposed Reliability Standard "should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness."[45]

Confidentiality: Lastly, the Commission stated that the proposed Standard(s) should also include procedures that will ensure confidential treatment of sensitive or confidential information.[46] The Commission noted that compliance with a Reliability Standard including the three steps outlined in the order "could [lead to the development of] sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure."[47]

D. Procedural History of Proposed Reliability Standard CIP-014-1

As further described in Exhibit F hereto, following the issuance of the Physical Security Order, the NERC Standards Committee, working with NERC staff, initiated Project 2014-04 Physical Security to develop a proposed Reliability Standard to satisfy FERC's directive to submit one or more physical security Reliability Standards by June 5, 2014 (i.e., within 90 days of the Physical Security Order). To facilitate meeting the 90-day timeline, the NERC Standards

---

44 Physical Security Order at P 11.

45 *Id*. at P 11.

46 *Id*. at P 10.

47 *Id*. at P 10.

Committee approved waivers to the Standard Processes Manual to shorten the comment and ballot periods for the Standards Authorization Request ("SAR") and draft Reliability Standard.[48] In accordance with a Standard Committee-approved waiver of the Standard Processes Manual, NERC posted the SAR for a seven-day informal comment period from March 21-28, 2014. A NERC-led industry Technical Conference on April 1, 2014 provided an opportunity for the standards drafting team, NERC, and industry participants to discuss issues related to applicability, identification of critical facilities, evaluation of threats and vulnerabilities, development and implementation of physical security plans, and a proposed implementation plan for the proposed Reliability Standard.

On April 10, 2014, following standard drafting team meetings, NERC posted the proposed Reliability Standard for an initial 15-day comment period and 5-day ballot in accordance with the Standard Committee-approved waiver.[49] The initial ballot received a quorum of 88.60% and an approval of 82.07%. After addressing industry comments on the initial draft of the proposed Reliability Standard, NERC posted the proposed Reliability Standard for a final ballot, which received a quorum of 95.53% and approval of 85.61%.

The NERC Board of Trustees adopted proposed Reliability Standard CIP-014-1 and the associated Implementation Plan on May 13, 2014. In approving the proposed Reliability Standard, the NERC Board of Trustees articulated its expectation that NERC management monitor and assess implementation of the proposed Reliability Standard on an ongoing basis, including:

- the number of assets identified as critical under the proposed Reliability Standard;

[48] The Standards Committee approved the waivers in accordance with Section 16 of the Standard Processes Manual.

[49] On April 9, 2014, the Standards Committee authorized the posting of the proposed Reliability Standard for comment and ballot.

- the defining characteristics of the assets identified as critical;
- the scope of security plans (i.e., the types of security and resiliency measures contemplated under the various security plans);
- the timeliness included in the security plans for implementing the security and resiliency measures; and
- industry's progress in implementing the proposed Reliability Standard.

As directed by the NERC Board of Trustees, NERC staff could use this information to provide regular updates to the NERC Board of Trustees, FERC staff, and other applicable regulatory authorities on industry's progress in securing critical Bulk-Power System facilities. NERC staff would monitor implementation in a manner that protects against the public disclosure of any sensitive or confidential information by, among other things, collecting and presenting aggregated information that cannot be attributed to any particular entity or transmission system.

IV. JUSTIFICATION FOR APPROVAL

As discussed below and in Exhibit C, proposed Reliability Standard CIP-014-1 satisfies the Commission's criteria in Order No. 672 and is just, reasonable, not unduly discriminatory or preferential, and in the public interest. The following section provides an explanation of: (1) the purpose of the proposed Reliability Standard; (2) the scope and applicability of the proposed Reliability Standard; (3) each of the requirements in the proposed Reliability Standard, including a discussion of how the requirements fulfil each element of the Physical Security Order and enhance Bulk-Power System security; (4) the protection of sensitive or confidential information under the proposed Reliability Standard; and (5) the enforceability of the proposed Reliability Standard.

A. Purpose and Overview of the Proposed Reliability Standard

The proposed Reliability Standard serves the vital reliability goal of enhancing physical security measures for the most critical Bulk-Power System facilities and lessening the overall

vulnerability of the Bulk-Power System to physical attacks. As the Commission noted, physical attacks on critical elements of the Bulk-Power System could have a significant impact on the reliable operation of the Bulk-Power System, potentially resulting in instability, uncontrolled separation, or Cascading.[50] Although the April 2013 attack on a California substation did not result in a power outage and reliability was maintained throughout the incident,[51] it emphasizes the evolving nature of physical security risks and the need to bolster physical security measures through a combination of NERC's reliability tools, including mandatory Reliability Standards, to provide for a secure and reliable Bulk-Power System for North America.

Proposed Reliability Standard CIP-014-1 will reinforce NERC's and the industry's longstanding efforts to protect the Bulk-Power System from physical attacks. Consistent with the Physical Security Order, the proposed Reliability Standard requires Transmission Owners and Transmission Operators to take steps to address threats and vulnerabilities to the physical security of those Bulk-Power System facilities that present the greatest risk to reliability if damaged or otherwise rendered inoperable. As explained further below, the proposed Reliability Standard contains six requirements designed to protect against and mitigate the impact of physical attacks on certain Transmission stations and Transmission substations, and their associated primary control centers, as follows:

- *Requirement R1* requires applicable Transmission Owners to perform risk assessments on a periodic basis to identify their Transmission stations and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Transmission Owner must then identify the primary control center that operationally controls each of the identified Transmission stations or Transmission substations.

- *Requirement R2* provides that each applicable Transmission Owner shall have an unaffiliated third party with appropriate experience verify the risk assessment performed

[50] Physical Security Order at P 5.

[51] No customers lost service during the incident.

under Requirement R1. The Transmission Owner must either modify its identification of facilities consistent with the verifier's recommendation or document the technical basis for not doing so.

- *Requirement R3* requires the Transmission Owner to notify a Transmission Operator that operationally controls a primary control center identified under Requirement R1 of such identification. This requirement helps ensure that such a Transmission Operator has notice of the identification so that it may timely fulfill its resulting obligations under Requirements R4 and R5 to protect that primary control center.

- *Requirement R4* requires each applicable Transmission Owner and Transmission Operator to conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of its respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1, as verified under Requirement R2.

- *Requirement R5* requires each Transmission Owner and Transmission Operator to develop and implement documented physical security plan that covers each of its respective Transmission stations, Transmission substations, and primary control centers identified in Requirement R1, as verified under Requirement R2.

- *Requirement R6* provides that each Transmission Owner and Transmission Operator subject to Requirements R4 and R5 have an unaffiliated third party with appropriate experience review its Requirement R4 evaluation and Requirement R5 security plan. The Transmission Owner and Transmission Operator must either modify its evaluation and security plan consistent with the recommendation of the reviewer or document its reasons for not doing so.

B. Scope and Applicability of the Proposed Reliability Standard

As outlined above, the objective of proposed Reliability Standard CIP-014-1 is to identify and protect those critical Transmission stations and Transmission substations, and their primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. This scope is consistent with the Commission's directive in the Physical Security Order that the mandatory Reliability Standard focus industry resources on protecting the highest priority facilities on the Bulk-Power System. As discussed above, while the Commission recognized that owners and operators of the Bulk-Power System may also take steps to protect other types of facilities (i.e., "facilities necessary to serve critical load"), the Commission directed NERC to develop one

or more mandatory Reliability Standards that apply to facilities that would have significant or widespread impact on the Bulk-Power System if damaged or rendered inoperable as a result of a physical attack, namely, those "facilities that…could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System."[52]

Provided this direction, NERC and the standard drafting team determined that the appropriate focus of the proposed Reliability Standard is Transmission stations and Transmission substations, which are uniquely essential elements of the Bulk-Power System. They make it possible for electricity to move long distances, connect generation to the grid, serve as critical links or hubs for intersecting power lines, and are vital to the delivery of power to major load centers. Because of this functionality, Transmission stations and Transmission substations are the types of facilities that could meet the criteria for critical facilities set forth in the Physical Security Order. Damage to or the inoperability of certain large Transmission stations or Transmission substations has the potential to result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

The use of the phrase "Transmission stations or Transmission substations" in the applicability section and the requirements of the proposed Reliability Standard clarifies that the Reliability Standard applies to both "Transmission stations" and "Transmission substations," as industry uses those terms. Although these terms are sometimes used interchangeably, some entities consider the term "Transmission substation" to refer specifically to a facility contained within a physical border (e.g., a fence or a wall) that contains one or more autotransformers. In contrast, some entities use the term "Transmission station" to refer specifically to a facility that

[52] Physical Security Order at P 6 and n. 5.

functions as a switching station or switchyard but does not contain autotransformers. The proposed Reliability Standard uses both "Transmission station" and "Transmission substation" to make clear that both types of facilities are subject to the proposed Reliability Standard.

Following its determination that Transmission stations or Transmission substations are the appropriate focus of the proposed Reliability Standard, the standard drafting team recognized that it was also necessary to identify and protect the primary control centers that operationally control any critical Transmission stations or Transmission substations. A primary control center is a control center that the Transmission Owner or Transmission Operator uses as the principal, permanently-manned site to operate a Bulk-Power System facility. A primary control center operationally controls a Transmission station or Transmission substation when the electronic actions from the control center can cause direct physical actions at the identified Transmission station or Transmission substation, such as opening a breaker. If a physical attack damages or otherwise renders such a primary control center inoperable, it could jeopardize the reliable operation of the critical Transmission station and Transmission substation in Real-time because it could remove or severely limit the ability to operate that critical facility remotely to respond to events on the system or otherwise ensure the reliable operation of a critical Bulk-Power System facility. Similarly, if perpetrators of a physical attack seize a primary control center that operationally controls a critical Transmission station or Transmission substation, the attackers could directly operate the critical Transmission station and Transmission substation to cause significant adverse reliability impacts.

Control centers that provide back-up capability and control centers that cannot operationally control a critical Transmission station or Transmission substation do not present similar direct risks to Real-time operations if they are the target of a physical attack. If a physical

attack damages or renders inoperable a backup control center for a critical Transmission station or Transmission substation, it would have no direct reliability impact in Real-time as the entity can continue operating the Transmission station or Transmission substation from its primary control center. Backup control centers are maintained in a dormant, stand-by state. A backup control center is a form of resiliency built into the system and is therefore intentionally redundant. So long as the proposed Reliability Standard requires the Transmission Owner or Transmission Operator to adequately protect its primary control center(s), it need not also require the Transmission Owner or Transmission Operator to protect its backup control center(s). Nothing in the proposed Reliability Standard, however, prohibits a Transmission Owner or Transmission Operator from considering whether to implement security measures at its backup control centers to strengthen the resiliency of its system and the ability to recover from a physical attack.

Similarly, the standard drafting team concluded that a physical attack at a control center of a Reliability Coordinator, for instance, that only has monitoring or oversight capabilities of a critical Transmission station or Transmission substation[53] would not have the direct reliability impact in Real-time contemplated in the Physical Security Order because operators at such control centers do not have the ability to physically operate critical Bulk-Power System facilities. Although certain monitoring and oversight capabilities might be lost as a result of a physical attack on such controls centers, the Transmission Owner or Transmission Operator that operationally controls the critical Transmission station or Transmission substation would be able to continue

[53] Certain Independent System Operators ("ISO") and Regional Transmission Organizations ("RTO"), for instance, operate control centers that monitor the transmission system within their footprint. These control centers, however, have no capability to physically operate those facilities. Rather, the ISO/RTO, in their role as Reliability Coordinator or Transmission Operator, only has the authority to coordinate or direct the action of the entity that actually physically operates the facility at local control centers.

operating its transmission system to prevent widespread instability, uncontrolled separation, or Cascading within an Interconnection.

Importantly, while the proposed Reliability Standard only covers primary control centers that operationally control a critical Transmission station or Transmission substation, the physical security protections required under Reliability Standard CIP-006-5 are applicable to primary and backup control centers of Reliability Coordinators, Balancing Authorities, Transmission Operators and Generation Operators irrespective of their ability to operationally control Bulk-Power System facilities. Reliability Standard CIP-006-5 requires entities to implement physical security measures designed to restrict physical access to locations containing High and Medium Impact BES Cyber Systems. Such locations include primary and backup control centers that perform the functional obligations of Reliability Coordinators, Balancing Authorities, Transmission Operators, and Generation Operators.[54] While the measures implemented under Reliability CIP-006-5 are primarily designed to protect against a cyber attack, these measures also help protect such control centers from physical attack. Additionally, NERC understands that Reliability Coordinators, Balancing Authorities, Transmission Operators, and Generation Operators typically include physical intrusion controls for their control centers, such as barriers and fences, card key access restrictions, and manned-security, and have done so for many years outside the scope of mandatory Reliability Standards. For the reasons stated above, however, the standard drafting team concluded that the scope of the proposed Reliability Standard should only provide additional physical security

[54] Specifically, Reliability Standard CIP-002-5.1 provides that BES Cyber System located at primary and backup control centers that perform the functional obligations of Reliability Coordinators, Balancing Authorities, Transmission Operators and Generation Operators are "High Impact" or "Medium Impact" BES Cyber Systems.

protections to those primary control centers that can physically operate critical Transmission stations and Transmission substations.[55]

The standard drafting team also considered whether the scope of the proposed Reliability Standard should include other types of facilities, such as generation facilities (e.g., a generation plant or a generator collector bus). The standard drafting team concluded that while the loss of a generation facility due to a physical attack may have local reliability effects, the loss of the facility is unlikely to have the widespread, uncontrollable impact that the Commission was concerned about in the Physical Security Order. A generation facility does not have the same critical functionality as certain Transmission stations and Transmission substations due to the limited size of generating plants, the availability of other generation capacity connected to the grid, and planned resilience of the transmission system to react to the loss of a generation facility. For example, as required by NERC's Transmission Planning (TPL) group of Reliability Standards, planning models must account for the loss of a generation facility, and entities must build resiliency into their systems to withstand an N-1 contingency (e.g., the loss of a generator or a generation switchyard). Accordingly, a physical attack that damages a generation facility is highly unlikely to destabilize the system, or cause uncontrolled separation or Cascading within an Interconnection. By limiting the scope of proposed Reliability Standard CIP-014-1 to Transmission stations,

[55] NERC recognizes that certain control centers categorized as "High Impact" or "Medium Impact" under Reliability Standard CIP-002-5.1 would not be subject to the proposed Reliability Standard. This reflects the different nature of cyber security risks and physical security risks at control centers. An asset that presents a heightened risk to the Bulk-Power System from a cyber security perspective may not present the same risk from a physical security perspective and vice versa. A primary cyber security concern for control centers is the corruption of data or information and the potential for operators to take action based on corrupted data or information. This concerns exists at control centers that operationally control Bulk-Power System facilities and those that do not. As such, there is no distinction in CIP-002-5.1 between these controls centers. As discussed above, however, such a distinction is appropriate in the physical security context. As such, the standard drafting team concluded that each type of control centers categorized as "High Impact" or "Medium Impact" under CIP-002-5.1 does not necessarily need the additional protections provided by the proposed Reliability Standard.

Transmission substations and their associated primary control centers, industry will be able to focus resources where it is most essential for maintaining reliable operations.

Furthermore, Transmission Owners must consider the loss of generation in determining which Transmission stations or Transmission substations are critical for purposes of the proposed Reliability Standard. Specifically, any determination of whether a Transmission station or Transmission substation is critical under the proposed Reliability Standard would account for the loss of generation facilities connected to that Transmission station or Transmission substation. As stated in the technical guidance attached to proposed Reliability Standard CIP-014-1, in performing its risk assessment to identify critical Transmission stations and Transmission substations, "[a]n entity could remove all lines, without regard to the voltage level, to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a significant area of the Interconnection." By doing so, a Transmission Owner would account for the loss of any generation connected to that Transmission station or Transmission substation.

As also explained and illustrated via a one-line diagram in the technical guidance attached to the proposed Reliability Standard, a Transmission station or Transmission substation that interconnects generation on the high side of a Generator Step-up transformer is subject to the Requirement R1 risk assessment, provided that the Transmission station or Transmission substation meets the criteria listed in Applicability Section 4.1.1, discussed below. The Requirement R1 risk assessment would then take into account the impact of the loss of a Transmission station or Transmission substation on the high-side of a Generator Step-up transformer that serves as an interconnection point for one or multiple generation resources.

Importantly, nothing in the proposed Reliability Standard precludes an entity from taking steps to protect against and mitigate the impact of physical attacks to generation facilities and control centers outside the scope of the proposed Reliability Standard, or any other Bulk-Power System element that does not meet the criteria of the proposed Reliability Standard. Many Reliability Coordinators, Balancing Authorities, Transmission Operators, Generation Owners, and Generation Operators are already taking steps to protect the physical security of their Bulk-Power System facilities, such as control centers and large generation facilities. NERC will continue to use its various reliability tools (e.g., security guidelines, training exercises, reliability assessments, and alerts) to inform industry of security threats and vulnerabilities and to provide guidance on steps industry participants should take to improve the security of all of their facilities to provide for a secure and reliable Bulk-Power System. Further, as noted above, Reliability Standards EOP-004-2 and CIP-006-5 address certain aspects of physical security.

Given the standard drafting team's determination on the appropriate scope of facilities subject to the proposed Reliability Standard, the proposed Reliability Standard provides requirements applicable to Transmission Owners and Transmission Operators, which are the functional entities that own and/or physically operate Transmission stations, Transmission substations and associated primary controls centers. Applying the proposed Reliability Standard to every registered Transmission Owner, however, would be overly broad, requiring many Transmission Owners to perform a risk assessment under Requirement R1 even though their systems do not include any Transmission stations or Transmission substations that would meet the Commission's criteria for critical facilities specified in the Physical Security Order. As the Commission recognized, "the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System" and many owners and

operators of the Bulk-Power System will not have critical facilities under the Reliability Standard.[56] NERC and the standard drafting team thus sought to establish a bright-line applicability threshold that would be broad enough to capture all Transmission Owners that could potentially have "critical facilities" while excluding Transmission Owners who do not own such facilities.

To that end, Applicability Section 4.1.1 of the proposed Reliability Standard provides that the proposed Reliability Standard applies only to those Transmission Owners that own a Transmission station or Transmission substation that meets the description of Transmission Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4. The Transmission Facilities included in Applicability Section 4.1.1.1 through 4.1.1.4 match the "Medium Impact" Transmission Facilities listed in Attachment 1 of Reliability Standard CIP-002-5.1.[57] The standard drafting team determined that using the criteria for "Medium Impact" Transmission Facilities set forth in Reliability Standard CIP-002-5.1 is an appropriate applicability threshold as the Commission has acknowledged that it is as a technically sound basis for identifying Transmission Facilities, which, if compromised, would present an elevated risk to the Bulk-Power System.[58]

Applicability Section 4.1.1 establishes an overinclusive threshold for defining which Transmission Owners are subject to the proposed Reliability Standard and must perform a risk assessment in accordance with Requirement R1. NERC expects that a number of Transmission Owners required to perform risk assessments under Requirement R1 will not identify any

---

[56] Physical Security Order at P 12.

[57] Specifically, the "Medium Impact" facilities described in Sections 2.4, 2.5, 2.6, and 2.7 of Attachment 1 of CIP-002-5.1.

[58] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160, Order No. 791-A, 146 FERC ¶ 61,188 (2013). As described in CIP-002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits.

Transmission stations or Transmission substations that, if damaged or rendered inoperable as a result of physical attack, pose a risk of widespread instability, uncontrolled separation, or Cascading within an Interconnection. Nevertheless, NERC and the standard drafting team concluded that using the "Medium Impact" criteria was a prudent approach to balancing the need for a Reliability Standard that is broad enough to capture all critical Transmission stations and Transmission substations while narrowing the scope of the Reliability Standard so as not to unnecessarily include entities that do not own or operate such critical facilities. During the development of the proposed Reliability Standard, the standard drafting team considered several other options for bright-line criteria but could not technically justify any higher threshold that would ensure the necessary Transmission stations and Transmission substations would be subject to the proposed Reliability Standard. Further, entities are already identifying whether they have "Medium Impact" facilities for purposes of transitioning to compliance with Reliability Standard CIP-002-5.1. As such, using the "Medium Impact" criteria in the applicability section of the proposed Reliability Standard does not create an additional burden on entities and complements the efforts already underway to comply with the CIP Reliability Standards approved in Order No. 791.

Transmission Operators are also subject to the proposed Reliability Standard (Applicability Section 4.1.2) to ensure that where the Transmission Owner does not operate the primary control center that operationally controls an identified Transmission station or Transmission substation, the Transmission Operator of that control center takes the steps required to protect that control center from physical attack. As discussed below, however, a Transmission Operator only has performance obligations under the proposed Reliability Standard if an applicable Transmission Owner notifies the Transmission Operator under Requirement R3 that the Transmission Operator

operates a primary control center that operationally controls a Transmission station or Transmission substation identified according to Requirement R1 (and verified under Requirement R2).

Finally, the standard drafting team considered whether it was necessary to include functional entities such as Reliability Coordinators or Balancing Authorities that have wide-area view of the Bulk-Power System as applicable entities under the proposed Reliability Standard. Specifically, whether such entities should be obligated to participate in the identification of critical facilities or have any responsibilities with respect to preventing or responding to physical attacks. Ultimately, for the reasons discussed below, the standard drafting team determined that expanding the scope beyond Transmission Owners and Transmission Operators would not provide any additional security benefits.

First, the standard drafting team concluded that the framework established in the proposed Reliability Standard accounts for a wide-area view and makes it unnecessary to include additional functional entities for purposes of identifying critical facilities. As explained further below, Transmission Owners are obligated to study in their risk assessments all of the categories of Transmission Facilities listed in Applicability section 4.1.1, including:

> Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

Accordingly, Transmission Owners are required to analyze Transmission stations and Transmission substations previously identified by Reliability Coordinators, Planning Coordinators, or Transmission Planners as potentially having a critical impact on the Bulk-Power

System.[59] Further, as noted above, the Commission already has acknowledged that the types of facilities listed in the applicability section reflect the subset of Transmission facilities that present an elevated risk to the Bulk-Power System.

Second, as further explained below, Requirement R2 obligates Transmission Owners to select an unaffiliated third party to verify their Requirement R1 risk assessment to help ensure that the identification of critical facilities captured the appropriate facilities. Requirement R2, Part 2.1 requires the verifying entity to be either a registered Planning Coordinator, Transmission Planner, or Reliability Coordinator, or an entity that has transmission planning or analysis experience. Through this verification process, Transmission Owners can work with a third party with a wide-area view of the Bulk-Power System to help identify critical facilities that would have widespread impacts if compromised as a result of a physical attack.

Lastly, the standard drafting team concluded that it was not necessary to extend the applicability of the proposed Reliability Standard to Reliability Coordinators or Balancing Authorities for purposes of imposing responsibilities on such entities with respect to preventing or responding to physical attacks. The standard drafting team determined that any security measures to protect against or mitigate the impact of physical attacks on a particular facility most appropriately fall on the owner or operator of that facility, not another functional entity. Reliability Coordinators and Balancing Authorities, however, continue to have an important role, outside of the proposed Reliability Standard, in helping the system respond to or recover from a physical attack. Other Reliability Standards set forth the duties of functional entities in responding to events on the Bulk-Power System. The Emergency Preparedness and Operations (EOP) group of

[59] Interconnection Reliability Operating Limit are defined in the NERC Glossary as "[a] System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Bulk Electric System."

Reliability Standards, for instance, include requirements for, among other things, emergency operations planning and coordination between the Reliability Coordinators, Balancing Authorities and Transmission Operators.[60] Proposed Reliability Standard CIP-014-1 will complement these Reliability Standards.

C. Requirements in the Proposed Reliability Standard

The following is an explanation of each of the requirements in the proposed Reliability Standard, including a discussion of how each requirement satisfies the elements of the Physical Security Order and enhances the reliability and security of the Bulk-Power System.

Requirement R1 addresses the directive in the Physical Security Order that entities should be required to perform a risk assessment of their systems to identify their critical facilities.[61] It also satisfies the directive for the periodic reevaluation and revision of the identification of critical facilities.[62] Requirement R1 requires Transmission Owners to conduct periodic risk assessment to identify their critical Transmission stations and Transmission substations. Requirement R1 provides:

> **R1.** Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria

---

60 For example, EOP-001-2.1b, Requirements R2 requires each Balancing Authority and Transmission Operator to develop, maintain, and implement a set of plans (i) to mitigate operating emergencies for insufficient generating capacity, (ii) to mitigate operating emergencies on the transmission system, (iii) for load shedding, and (iv) to mitigate operating emergencies. Under EOP-001-2.1b, Requirement R6 each Balancing Authority and Transmission Operator is also required to coordinate its operating plans with other Balancing Authorities and Transmission Operators. Further, Reliability Standard EOP-005-2, Requirement R1 requires the Transmission Operator to have a Reliability Coordinator approve its system restoration plan. Requirement R13 of that standard requires the Transmission Operator to have written agreements or mutually agreed to procedures with Generator Operators with blackstart resources, including testing requirements for those resources. Reliability Standard EOP-006-2 requires the Reliability Coordinator to have a Reliability Coordinator Area restoration plan and to coordinate restoration plans with other Reliability Coordinators and review the restoration plans of Transmission Operators within its Reliability Coordinator Area. The Reliability Coordinator is also required to work with Transmission Operators s, Generation Operators and adjacent Reliability Coordinators to monitor restoration and provide assistance if necessary.

61 Physical Security Order at P 6.

62 *Id*. at P 11.

specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.1 Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or

- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2 The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

The applicability section and Requirement R1 effectively establish a two-step process for identifying critical facilities under the proposed Reliability Standard. First, a Transmission Owner must determine whether it has any Transmission stations or Transmission substations that meet the criteria in Applicability Section 4.1.1. If it does not, the Transmission Owner is not an applicable entity and has no performance obligations under the proposed Reliability Standard. If it does own Transmission stations or Transmission substations described in the applicability section, the Transmission Owner must then assess, in accordance with Requirement R1, whether any of those Transmission stations or Transmission substations, if rendered inoperable or damaged as a result of a physical attack, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

Requirement R1 mandates that the risk assessment "consist of a transmission analysis or transmission analyses" to help ensure that the methods used to identify critical facilities are based on objective analysis, technical expertise, and experienced judgment, consistent with the Commission's directive. The proposed Reliability Standard, however, does not require that a Transmission Owner use a specific method to perform its analysis. Transmission Owners have the ability to use the method that best suits their needs and the characteristics of their system. For example, an entity may perform a power flow analysis, which, depending on the characteristics of its system, could include a stability analysis at a variety of load levels as well as steady state or short circuit analyses under various system conditions and configurations.[63] The standard drafting team concluded that mandating a specific method would not adequately consider regional, topological, and system circumstances. Regardless of the method used to perform the risk assessment, however, Transmission Owners must be able to demonstrate to the verifier under Requirement R2 and the ERO during its compliance monitoring activities that it used an appropriate method to meet its affirmative obligation to identify all critical Transmission stations and Transmission substations under Requirement R1.[64]

As set forth in the Implementation Plan for proposed Reliability Standard CIP-014-1, Transmission Owners must complete their initial risk assessments on or before the effective date of the proposed Reliability Standard. Consistent with the Commission's directive, Requirement R1 also requires the periodic reevaluation and revision of the identification of critical facilities to

---

[63] The guidance section of the proposed Reliability Standard provides entities guidance on ways to perform the transmission analysis to meet the requirements of the standard.

[64] If a Transmission Owner patently fails to develop a method reasonably designed to identify its critical facilities (e.g., the assumptions underlying the study are patently deficient), the ERO could find that the Transmission Owner is non-compliant with Requirement R1 and exercise its enforcement authority against that Transmission Owner, as appropriate. As discussed below, in cases where the Transmission Owner demonstrates that the verifying entity is qualified, unaffiliated with the Transmission Owner, and the scope of their verification is clear, auditors are encouraged to rely on the verifications.

help ensure that the risk assessments remain current with projected conditions and configurations of the Transmission Owner's system. As provided in Requirement R1, Part 1.1, however, the timing of subsequent risk assessments depends on whether the Transmission Owner has previously identified any critical facilities. Specifically, if a Transmission Owner identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection, it must conduct its next risk assessment within 30 calendar months of its previous risk assessment. The standard drafting team concluded that a 30-month period was appropriate given the long lead times required for a Transmission Owner to change its system, whether through construction of new facilities or otherwise, in a manner that would result in additional Transmission stations or Transmission substations meeting the criteria of a critical facility for purposes of the proposed Reliability Standard. Additionally, the 30-month period aligns with the requirement to consider both existing Transmission stations and Transmission substations and those planned to be in service within 24 months.

For a Transmission Owner that did not identify any critical facilities in its previous risk assessment (as verified according to Requirement R2), Requirement R1 requires the Transmission Owner to conduct its next risk assessment within 60 calendar months of its previous risk assessment. The standard drafting team concluded that because such entities are unlikely to see material changes to their systems in the Near-Term Planning Horizon that would result in a new or existing Transmission station or substation becoming critical, a 60-month period for completing subsequent risk assessments was appropriate.

Following the identification of any critical Transmission stations and Transmission substations, Part 1.2 requires the Transmission Owner to identify the primary control center that operationally controls each identified Transmission station and Transmission substation. As noted above, it is important to protect such primary control centers from a physical attack to help ensure that they are not damaged, rendered inoperable or misoperated in a way that could cause significant adverse reliability impacts.

Requirement R2 addresses the Commission directive that the Reliability Standard should (i) require that an entity other than the owner or operator verify the risk assessment, and (ii) include a procedure for the verifying entity to add or remove facilities from an owner's or operator's list of critical facilities.[65] Requirement R2 provides:

> **R2.** Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1.
>
> **2.1.** Each Transmission Owner shall select an unaffiliated verifying entity that is either:
>
> - A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
>
> - An entity that has transmission planning or analysis experience.
>
> **2.2.** The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.
>
> **2.3.** If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each

[65] Physical Security Order at P 11.

recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or

- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

The purpose of the verification requirement is to have a third party with requisite expertise provide an independent assessment of the Transmission Owner's identification of critical facilities. As noted above, physical attacks on certain Transmission stations and Transmission substations could have a significant adverse impact on the reliable operation of the Bulk-Power System. Requirement R2 therefore builds in a layer of independence to help ensure that the Transmission Owner identifies and protects all critical Transmission stations and Transmission substations on its system. The third-party verification will also help provide additional assurance, consistent with the Physical Security Order, that the "methodologies to determine these facilities [are] based on objective analysis, technical expertise, and experienced judgment."[66]

To meet the intent of this element of the Physical Security Order, Requirement R2 requires that the verifying entity meet certain criteria. First, the verifying entity must be an "unaffiliated third party." For purposes of this Reliability Standard, the term "unaffiliated" means that the selected verifying entity cannot be a corporate affiliate (i.e., the verifying entity cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission

[66] *See* Physical Security Order at P 6.

Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.[67]

Additionally, the verifying entity must be a registered Planning Coordinator, Transmission Planner, or Reliability Coordinator, or another entity that has transmission planning or analysis experience. In all cases, but particularly if the Transmission Owner does not select a registered Planning Coordinator, Transmission Planner, or Reliability Coordinator, the Transmission Owner must demonstrate that the selected verifier has the requisite expertise to perform the verification. The guidance section of the proposed Reliability Standard includes a discussion of characteristics that Transmission Owners should consider when selecting a verifying entity, including: (1) experience in power system studies and planning; (2) understanding of the NERC MOD standards, TPL standards, and facility ratings as they pertain to planning studies; and (3) familiarity with the Interconnection within which the Transmission Owner is located. In cases where the Transmission Owner shows that the verifying entity is qualified, unaffiliated with the Transmission Owner, and the scope of their verification is clear, auditors are encouraged to rely on the verifications. In cases where the verifying entity lacks the qualifications specified in Requirement R2, the verifier is not sufficiently independent, or where the scope of the verification is unclear, it is expected that auditors will apply increased audit testing of Requirements R1.

Requirement R2 also provides that the "verification may occur concurrent with or after the risk assessment performed under Requirement R1." This provision is designed to provide the Transmission Owner the flexibility to work with the verifying entity throughout the risk

[67] The prohibition on Transmission Owners using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could collaborate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently. The intent of Requirement R2 is to have an entity other than the owner or operator of the facility be involved in the risk assessment process and have an opportunity to provide input, rather than to simply have an after-the-fact verification. Accordingly, Requirement R2 allows entities to have a two-step process, where the Transmission Owner performs the risk assessment and subsequently has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the risk assessment.

Consistent with the Commission's directive, Requirement R2 includes a process for the verifying entity to recommend the addition or removal of facilities from a Transmission Owner's list of identified facilities. Part 2.2 specifies that the verification "may include recommendations for the addition or deletion of a Transmission station or Transmission substation." Part 2.3 then requires the Transmission Owner to address those recommendations in one of two ways. The Transmission Owner must either: (i) modify its identification under Requirement R1 consistent with the verifier's recommendation(s); or (ii) document the technical basis for not modifying the identification in accordance with the recommendation. Requiring documentation of the technical basis for not modifying the identification in accordance with the recommendation will help ensure that a Transmission Owner meaningfully considers the verifier's recommendations and follows those recommendations unless it can technically justify its reasons for not doing so. To comply with Part 2.3, the technical justification must be sound and based on acceptable approaches to conducting transmission analyses. During its compliance monitoring activities, the ERO will

review that documentation in assessing the Transmission Owner's compliance with the proposed Reliability Standard.

Because the Commission has existing authority to enforce NERC Reliability Standards, the proposed Reliability Standard does not also include a procedure for the Commission to add or remove a facility from a Transmission Owner's list of identified facilities.[68] As provided in Section 215(e)(3) of the FPA and Section 39.7(f) of the Commission's regulations, the Commission has the authority, on its own motion, to enforce NERC Reliability Standards. In exercising that authority, the Commission, like NERC and the Regional Entities, can effectively require Transmission Owners to add or remove facilities if its finds that the Transmission Owner did not comply with its duty under Requirement R1 to identify critical Transmission stations or Transmission substations. As stated above, a Transmission Owner must be able to demonstrate that its method for performing its risk assessment was technically sound and reasonably designed to identify its critical Transmission stations and Transmission substations. If, in the course of assessing an entity's compliance with the proposed Reliability Standard, NERC, a Regional Entity, or FERC finds that the entity's transmission analysis was patently deficient and that the Requirement R2 verification process did not cure those deficiencies, they could use their enforcement authority to compel Transmission Owners to re-perform the risk assessment using assumptions designed to identify the appropriate critical facilities.

Requirement R2 also addresses the timing of the verifications. As provided in Part 2.2, the Transmission Owner is responsible for ensuring that the verifier completes the verification within 90 calendar days of the completion of each Requirement R1 risk assessment. The Transmission Owner then has 60 calendar days to modify its identification consistent with any recommendations

[68] *See* Physical Security Order at 11.

or document the technical basis for not doing so. The standard drafting team concluded that such timeframes appropriately balance the need to accomplish these tasks quickly while providing sufficient time for the Transmission Owner to complete the verification.

Lastly, consistent with the Commission's directive to protect confidential or sensitive information from public disclosure,[69] Part 2.4 creates an affirmative obligation on the Transmission Owner to guard against the release of any sensitive or confidential information, such as the list or location of critical Transmission Stations and Substations, to the public. As the Commission stated, if this information is disclosed to the public, it could jeopardize the reliable operation of the Bulk-Power System. Part 2.4 requires Transmission Owners to implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier or otherwise developed pursuant to this Reliability Standard from public disclosure. Below is an additional discussion of confidentiality issues under the proposed Reliability Standard.

Requirement R3 provides:

> **R3.** For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2.
>
> **3.1.** If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment,

[69] Physical Security Order at 10.

notify the Transmission Operator that has operational control of the primary control center of the removal.

Requirement R3 requires the Transmission Owner to notify a Transmission Operator that operationally controls a primary control center identified under Requirement R1 (as verified under Requirement R2) of such identification. Part 3.1 requires a Transmission Owner to notify the Transmission Operator of any removals from identification. This requirement helps ensure that such Transmission Operators have notice as to whether they have any obligations under the proposed Reliability Standard to protect any of their control centers.

Requirement R4 addresses the Commission's directive to require owners and operators evaluate the potential threats and vulnerabilities to their critical facilities.[70] It also satisfies the directive for the periodic reevaluation and revision of the evaluation of critical facilities.[71] Requirement R4 provides:

> R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:
>
> **4.1.** Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);
>
> **4.2.** Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and
>
> **4.3.** Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

---

[70] Physical Security Order at P 8.

[71] *Id*. at P 11.

Although Requirement R4 does not mandate a specific, one-size-fits-all method for evaluating potential threats and vulnerabilities, it obligates applicable entities to consider elements that form the foundation of an effective evaluation of security threats and vulnerabilities. First, consistent with the Commission's acknowledgement that threats and vulnerabilities may vary from facility to facility, Part 4.1 requires that the Transmission Owner or Transmission Operator tailor their evaluations to the unique characteristics of the facility in question so as to consider factors such as the facility's location, size, function, existing protections, and attractiveness as a target. Second, entities must consider prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events (Part 4.2). Lastly, entities must consider intelligence or threat warnings (Part 4.3). Collectively, Parts 4.1-4.3 help to ensure that the Transmission Owner and Transmission Operator tailor their evaluations to "the types of attacks that can be realistically contemplated," as the Commission directed.[72] The guidance section of the proposed Reliability Standard provides a list of resources that entities may consult for information on conducting effective threat and vulnerability evaluations.

Consistent with the directive in the Physical Security Order that the Reliability Standard require periodic evaluations, Transmission Owners and Transmission Operators must conduct an evaluation following each Requirement R1 risk assessment. Although Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur, Requirement R5, requires that entities develop their security plan(s) within 120 calendar days following completion of the Requirement R2 verifications. Because the development of the Requirement R5 security plan(s) is dependent on the completion of the Requirement R4 evaluation, Transmission Owners

[72] Physical Security Order at P 8.

and Transmission Operators must simply complete the Requirement R4 evaluation in time to comply with the 120-day period for completing the Requirement R5 security plan(s).

Requirement R5 addresses the Commission's directive to require owners and operators to develop and implement a security plan designed to protect against physical attacks to their critical facilities based on the assessment of the potential threats and vulnerabilities to those facilities.[73] It also satisfies the directive for the periodic reevaluation and revision of the security plans.[74] Requirement R5 provides:

> **R5.** Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:
>
> **5.1.** Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.
>
> **5.2.** Law enforcement contact and coordination information.
>
> **5.3.** A timeline for executing the physical security enhancements and modifications specified in the physical security plan.
>
> **5.4.** Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

Requirement R5 creates an affirmative obligation on Transmission Owners and Transmission Operators to develop and implement security plans to protect their critical

---

[73] Physical Security Order at P 9.

[74] *Id*. at P 11.

Transmission stations, Transmission substations, and primary control centers. Rather than dictate the specific steps entities must take to protect their critical facilities, however, Requirement R5 obligates entities to develop security plan(s) that include elements that will help ensure that the security plans will result in an adequate level of protection against the potential physical threats and vulnerabilities identified pursuant to Requirement R4. These elements are set forth in Parts 5.1-5.4, each of which is discussed below.

Part 5.1 requires entities to include in their security plan(s) "[re]siliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4." Security measures refer to those steps an entity takes to strengthen the physical security of the site, such as security guards, video cameras, fences, or ballistic protections. Based on the Requirement R4 evaluation, entities should consider the need to implement security measures applicable to the entire site (e.g., the construction of a fence or wall around an entire facility, or the hiring security guards to guard the entire facility) as well as security measures that target specific critical components at the site (e.g., ballistic protections for some or all transformers at a Transmission substation).

Resiliency measures refer to those steps an entity may take that, while not specifically targeted as hardening the physical security of the site, help to decrease the potential adverse impact of a physical attack at an identified critical facility. These measures could include modifications to system topology or the construction of a new Transmission station or Transmission substation that would lessen the criticality of the facility. Entities may choose to focus their resources on redesigning their systems to limit the number of critical facilities, which will ultimately make it more difficult for the perpetrators of a physical attack to cause significant harm to the Bulk-Power

System.[75] Additionally, resiliency measures include providing for access to spare or replacement equipment. Many components of Transmission stations, Transmission substations, and primary control centers are expensive and difficult to replace quickly. Having spare equipment available will enable entities to limit the length of outages caused by a physical attacks. Entities should not necessarily be limited to implementing conventional security measures but should also seek to build resiliency into their system to enhance their ability to mitigate the risk and impact of a physical attack. The flexibility provided in Part 5.1 is thus consistent with the Commission's directive to allow applicable entities to consider elements of resiliency in identifying and protecting their critical facilities.

Part 5.2 requires entities to include in their security plan(s) provisions for "law enforcement contact and coordination information." Such provisions may include, among other things, providing substation safety and familiarization training for local and federal law enforcement, fire department, and Emergency Medical Services. Working with law enforcement is essential to both preventing and responding to physical attacks.

Part 5.3 requires entities to include in their security plan(s) a "timeline for executing the physical security enhancements and modifications specified in their physical security plan." Entities must have the flexibility to prioritize the implementation of the various resiliency or security enhancements and modifications in their security plan according to risk, resources, or other factors, such as the lead times necessary to implement certain security or resiliency measures. Entities must design these timelines, however, to protect their critical facilities from the threats and vulnerabilities identified pursuant to Requirement R4. For measures that have long lead times,

[75] The implementation of certain resiliency measures, such as the construction of a new Transmission station or Transmission substation, could affect the results of an entity's next Requirement R1 risk assessment such that a facility previously identified as critical would no longer meet that criteria.

entities must consider whether interim protections are necessary to address the identified threats and vulnerabilities. As part of the third party review of the security plans required by Requirement R6, as well as any ERO compliance monitoring activity, entities must be able to justify their implementation timelines and demonstrate that they are implementing their security plan in a manner that will provide an adequate level of protection as soon as reasonably practicable.[76]

Lastly, Part 5.4 requires entities to include in their security plans "[p]rovisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s)." These provisions will help ensure that a Transmission Owner's and Transmission Operator's physical security protections evolve to meet a dynamic and changing risk environment. An entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various sources. Such sources include the ERO, ES-ISAC, and US and/or Canadian federal agencies. Transmission Owners and Transmission Operators should then use that information to reevaluate or consider changes in the security plan and the corresponding security measures of the security plan.

The approach to specify the fundamental attributes that an entity must include in its security plan(s), as opposed to specifying the steps the entity must take, is consistent with the directives in the Physical Security Order[77] and preferable from a security perspective. As noted, the threat environment is dynamic and continually evolving. As such, Reliability Standards addressing security issues must allow entities to adapt to changing threats and encourage entities to develop

---

[76] If, in the course of assessing an entity's compliance with the proposed Reliability Standard, NERC, a Regional Entity, or FERC finds that the timelines were patently deficient in their ability to adequately deter, detect, delay, assess, communicate, and respond to the identified physical threats and vulnerabilities, they could use their enforcement authority to compel the Transmission Owners or Transmission Operator to modify those timelines.

[77] Physical Security Order at PP 2, 9.

and implement new and innovative measures to deter, detect, delay, assess, communicate, and respond to emerging security threats. As the Commission noted, there is not a one-size-fits all approach to protecting against physical security threats.[78] A specific measure that would be effective at one facility may not be appropriate for a different facility. Listing specific steps in the proposed Reliability Standard could also potentially stunt the types of security measures that entities would ultimately implement. Entities must have the flexibility to develop security measures that are unique to the threats and vulnerabilities of their facilities.

As described above, however, the plan must include measures designed "to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4." Accordingly, as part of the third party review of the security plans required by Requirement R6, as well as any ERO compliance monitoring activity, entities must demonstrate that their security plans are designed to result in an adequate level of protection against the potential physical threats and vulnerabilities identified pursuant to Requirement R4.

As to timing, Requirement R5 obligates Transmission Owners and Transmission Operators to develop (or revise) their security plans within 120 calendar days of the date the Transmission Owner completes Requirement R2.[79] This 120-day period is for the development of the plan, not implementation of the measures included with the security plan(s). Requirement R5 specifically states that entities must execute their security plans according to the timelines specified therein. As noted above, to comply with Requirement R5 Transmission Owners and Transmission

---

[78] See Physical Security Order at P 2.

[79] Requirement R2 is complete when there is nothing left to do under the requirement. If the verifier does not make any recommendations, then the Transmission Owner completes Requirement R2 once the verifier completes its verification. If the verifier makes one or more recommendations, the Transmission Owner only completes Requirement R2 when it has modified its identification of critical facilities consistent with the recommendations or documented its reasons for not doing so.

Operators must establish timelines reasonably designed to address the identified security threats and vulnerabilities to the critical facility in a timely manner.

Finally, Requirement R6 addresses the Commission directive that the Reliability Standard require that an entity other than the owner or operator of the critical facility review the Requirement R4 evaluation of threats and vulnerabilities and the Requirement R5 security plan(s). Requirement R6 provides:

> **R6.** Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5.
>
> **6.1.** Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:
>
> - An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
> - An entity or organization approved by the ERO.
> - A governmental agency with physical security expertise.
> - An entity or organization with demonstrated law enforcement, government, or military physical security expertise.
>
> **6.2.** The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.
>
> **6.3.** If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator

shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or

- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

Similar to Requirement R2, the purpose of Requirement R6 is to have a third party with the appropriate expertise provide an independent review of a Transmission Owner's and Transmission Operator's Requirement R4 evaluation or Requirement R5 security plans(s). The third party review will provide an additional layer of expertise and assurance that the Transmission Owner and Transmission Operator (1) properly evaluated potential threats and vulnerabilities, and (2) developed a security plan that results in an adequate level of protection against the potential physical threats and vulnerabilities it faces at the identified facilities.[80]

To meet the intent of this element of the Physical Security Order, Requirement R6 requires that the reviewing entity meet certain criteria. First, the reviewing entity must be an "unaffiliated third party." As in Requirement R2, the term "unaffiliated" means that the selected entity cannot be a corporate affiliate (i.e., the verifying entity cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner or Transmission

[80] The third party review thus addresses the Commission directive that NERC should consider whether to require owners and operators to consult with entities with appropriate expertise as part of the evaluation process. *See* Physical Security Order at P 8.

Operator). The reviewing entity also cannot be a division of the Transmission Owner or Transmission Operator that operates as a functional unit.[81]

Additionally, Requirement R6 states that Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer that meets one of the following criteria: (1) an entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional ("CPP") or Physical Security Professional ("PSP") certification; (2) an entity or organization approved by the ERO; (3) a governmental agency with physical security expertise;[82] and (4) an entity or organization with demonstrated law enforcement, government, or military physical security expertise. NERC and the standard drafting team determined that unaffiliated entities or organizations that meet these qualifications will have the expertise necessary to provide an effective and independent review. Applicable Transmission Owners and Transmission Operators have the flexibility to have one reviewer review both the Requirement R4 evaluation and the Requirement R5 security plan or have separate reviewers for each step.

Under either scenario, the Transmission Owner and Transmission Operator must show that the selected entity has the appropriate expertise to conduct the review. As noted for Requirement R2, in cases where the Transmission Owner or Transmission Operator shows that the reviewing entity is qualified, sufficiently independent, and the scope of their review is clear, auditors are encouraged to rely on the reviews. In cases where the reviewing entity lacks the qualifications

---

[81] The prohibition on Transmission Owners using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

[82] CPP and PSP certifications are widely-recognized in the physical security industry to demonstrate expertise in the physical security domain.

specified in Requirement R6, the reviewer is not sufficiently independent, or where the scope of the review is unclear, it is expected that auditors will apply increased audit testing of Requirements R4 and R5.

As with the verification under Requirement R2, Requirement R6 provides that the "review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5." This provision provides applicable Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5. In other words, a Transmission Owner or Transmission Operator could collaborate with its unaffiliated third party reviewer to perform the Requirement R4 evaluation or develop the Requirement R5 security plan. This collaboration may allow entities to create efficiencies in their processes for complying with the proposed Reliability Standard. The intent of Requirement R6 is to have an entity other than the owner or operator of the facility be involved with and provide input on the Requirement R4 evaluation and the development of the Requirement R5 security plans, rather than simply have an after-the-fact review. Accordingly, Requirement R6 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the evaluation and develops the security plan itself and then has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the evaluation and develop the security plan.

Requirement R6, Part 6.2 provides that applicable Transmission Owners and Transmission Operators are responsible for ensuring that the reviewer(s) complete the review within 90 calendar days of the completion of the development of the security plan under Requirement R5. Part 6.2 also specifies that the review may "include recommended changes to the evaluation performed

under Requirement R4 or the security plan(s) developed under Requirement R5." Part 6.3 then specifies that the Transmission Owner or Transmission Operator must address those recommendations, within 60 calendar days, in one of two ways. The Transmission Owner or Transmission Operator must either: (i) modify its evaluation or security plan consistent with the reviewer's recommendation(s); or (ii) document the reason for not modifying the evaluation or security plan in accordance with the recommendation. Requiring documentation of these reasons will help ensure that the Transmission Owner or Transmission Operator properly considers the reviewer's recommendations and follows those recommendations unless it can justify not doing so. The ERO or the Commission can then review that documentation when evaluating the entity's compliance with the proposed Reliability Standard. Although Part 6.3 allows the Transmission Owner or Transmission Operator to consider a variety of factors for not following the reviewer's recommendations, to satisfy Part 6.3, the Transmission Owner or Transmission Operator must provide a reasonable justification for not doing so.

Lastly, consistent with the Commission's directive to protect confidential or sensitive information from public disclosure,[83] Part 6.4 creates an affirmative obligation on the Transmission Owner and Transmission Operator to guard against the release of any sensitive or confidential information, such as site vulnerabilities or the security protection established for a particular site. Release of such information could provide a roadmap to those individuals or groups intent on physically attacking critical Bulk-Power System facilities. As the Commission stated, if this information is disclosed to the public, it could jeopardize the reliable operation of the Bulk-Power System.[84] Part 6.4 thus requires Transmission Owners to implement procedures, such as

---

83 Physical Security Order at 10.

84 *Id.*

the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and or otherwise developed pursuant to this Reliability Standard from public disclosure. Below is an additional discussion of confidentiality issues under the proposed Reliability Standard.

D. Protection of Sensitive or Confidential Information

As discussed above, the Commission sought to ensure that any sensitive or confidential information that entities develop in the course of complying with the proposed Reliability Standard remains confidential to decrease the possibility that such information could become available to individuals or groups that may use such information to perpetrate physical attacks on the Bulk-Power System.[85] To that end, the proposed Reliability Standard affirmatively obligates entities to protect their sensitive and confidential information from public disclosure (Requirement R2, Part 2.4 and Requirement R6, Part 6.4). Procedures for protecting confidential information may include, among other things, the following elements: (1) the control and retention of information at the applicable entity's facility for third party verifiers/reviewers; (2) restricting information to only those employees that need to know such information for purposes of carrying out their job functions; (3) marking all relevant documents as confidential; (4) securely storing and destroying information, both physical and electronically; and (5) requiring senior manager sign-off prior to releasing any sensitive or confidential information to an outside entity.

Additionally, the compliance monitoring section of the proposed Reliability Standard provides that all evidence for demonstrating compliance with this standard will be retained at the Transmission Owner's and Transmission Operator's facilities.[86] Requiring that evidence remain

---

[85] *Id.*

[86] Specifically, Compliance Monitoring Section 1.4 provides:

on site will reduce the possibility of releasing sensitive or confidential information to individuals who should not have access to such information. NERC and the Regional Entities will develop policies to ensure that sensitive or confidential information reviewed during compliance monitoring activities will remain on site and confidential.

During the standard development process, certain registered entities raised issues as to the relationship between the confidentiality provisions of the proposed Reliability Standard and public disclosure laws, such as the U.S. Freedom of Information Act, and similar state, provincial, or local laws. Registered entities were concerned that public disclosure laws would require them to publicly disclose certain sensitive or confidential information, thereby jeopardizing the reliability of the Bulk-Power System. NERC notes that the confidentiality provisions in proposed Reliability Standard CIP-014-1 may provide registered entities subject to public disclosure laws the authority to limit public disclosure of sensitive or confidential information developed pursuant to the proposed Reliability Standard. NERC understands that many public disclosure laws in various jurisdictions in the United States and Canada include provisions that exempt from public disclosure information that entities must keep confidential pursuant to another federal, state, provincial, or local law.[87] Such exemptions may apply to the sensitive or confidential information developed in the course of complying with the Reliability Standard given the affirmative obligation in the proposed Reliability Standard (Parts 2.4 and 6.4) that applicable entities protect such information from public disclosure. Additionally, certain public disclosure laws already exempt from disclosure certain confidential information specifically related to critical infrastructures, such as

> Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

[87] *See*, *e.g.*, Colorado Open Records Act, C.R.S. § 24-72-204; Washington Public Records Act, Wash. Rev. Code § 42.56.070.

energy, water, or telecommunications infrastructure,[88] or information that is vital to governmental interests.[89] Such provisions may exempt some, if not all, of the sensitive or confidential information developed under the standard from disclosure.

Nevertheless, NERC understands that public disclosure laws are different across the various jurisdictions in North America and there may be some laws that do not have existing provisions to exempt from public disclosure the sensitive or confidential information developed under the proposed Reliability Standard. The purpose of NERC Reliability Standards is to establish and impose mandatory requirements that owners, operators and users of the Bulk-Power System must follow to help protect the reliability of the Bulk-Power System. NERC Reliability Standards do not stipulate whether certain information is exempt from public disclosure laws. The applicability of such laws to the information developed under proposed Reliability Standard CIP-014-1 may be addressed in other forums at the federal, state, provincial, or local levels. NERC understands that certain registered entities may ask the Commission for a statement indicating that the proposed Reliability Standard will govern any contrary state or local public disclosure law. Such a statement could help to clarify the applicability of public disclosure laws and further the intent of the Physical Security Order to protect sensitive or confidential information.

E. Enforceability of the Proposed Reliability Standards

The proposed Reliability Standard includes VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC will enforce the requirements of the proposed Reliability Standard. The VRFs and VSLs for the proposed Reliability Standard comport with NERC and

---

[88] *See, e.g.*, Arizona Public Records Act, A.R.S. §39-126 (stating "[n]othing in this chapter requires the disclosure of a risk assessment that is performed by or on behalf of a federal agency to evaluate critical energy, water or telecommunications infrastructure to determine its vulnerability to sabotage or attack.")

[89] *See, e.g.*, Wash. Rev. Code § 42.56.210.

Commission guidelines related to their assignment. Exhibit E provides a detailed review of the VRFs and VSLs, and the analysis of how the VRFs and VSLs were determined using these guidelines.

The proposed Reliability Standard also includes measures that support each requirement by clearly identifying what is required and how the ERO will enforce the requirement. These measures help ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.[90]

V. EFFECTIVE DATE

In the Physical Security Order, the Commission stated that "NERC should develop an implementation plan that requires owners or operators of the Bulk-Power System to implement the Reliability Standards in a timely fashion, balancing the importance of protecting the Bulk-Power System from harm while giving the owners or operators adequate time to meaningfully implement the requirements."[91] The Commission also specified that the implementation plan should include timeframes for completion of the risk assessment, threat and vulnerability evaluations, and development and implementation of the security plan.

Consistent with the Commission's directive, NERC respectfully requests that the Commission approve the proposed Reliability Standard to become effective on the first day of the first calendar quarter that is six months after Commission approval. The Implementation Plan for proposed Reliability Standard CIP-014-1, attached hereto as Exhibit B, provides a timeline for initial performance under the proposed Reliability Standard following the proposed effective date.

---

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

[91] Physical Security Order at P 12.

As described in the Implementation Plan, applicable Transmission Owners must conduct their initial Requirement R1 risk assessment on or before the effective date of the proposed Reliability Standard. Transmission Owners and Transmission Operators must then complete initial performance of Requirements R2 through R6, as applicable, according to the timelines specified in those requirements, as follows:

- *Requirement R2* - The Transmission Owner must (i) complete the third party verification of the risk assessment (Parts 2.1, 2.2, and 2.4) within 90 calendar days of the effective date of the proposed Reliability Standard, and (ii) make any modifications to the list of identified facilities or documentation as to why no modifications were required (Part 2.3) within 60 days of completing the third party verification.

- *Requirement R3* – The Transmission Owner must make the required notification to the Transmission Operator within 7 calendar days of completion of performance under Requirement R2.[92]

- *Requirements R4 and R5* – Applicable Transmission Owners and Transmission Operators must complete the evaluation of threats and vulnerabilities and develop the security plan within 120 calendar days of completion of performance under Requirement R2.

- *Requirement R6* – Transmission Owners and Transmission Operators must (i) complete the third party review of the Requirement R4 evaluation and the Requirement R5 security plan (Parts 6.1 and 6.2) within 90 calendar days of completion of developing the Requirement R5 security plans, and (ii) make any modifications to the evaluation or security, or documentation as to why no modifications were required (Part 6.3) within 60 days of completing the third party review.

The standard drafting team concluded that the timeframes set forth in the Implementation Plan appropriately balances the urgency of implementing the requirements of the proposed Reliability Standard to protect the Bulk-Power System with providing entities sufficient time for effective implementation. While many entities are already taking steps to implement security measures, others may require time to develop internal processes, procedures, and budget

[92] Requirement R2 is complete when there is nothing left to do under the requirement. Specifically, if the verifier does not make any recommendations, then the Transmission Owner completes Requirement R2 once the verifier completes its verification. If the verifier makes one or more recommendations, the Transmission Owner only completes Requirement R2 when it has modified its identification of critical facilities consistent with the recommendations or documented its reasons for not doing so.

allocations to comply with proposed Reliability Standard CIP-014-1. In the interim, NERC will continue to use its existing reliability tools to work with industry to protect the security of the Bulk-Power System

VI. CONCLUSION

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

- the proposed Reliability Standard and associated elements included in Exhibit A, effective as proposed herein; and
- the proposed implementation plan included in Exhibit B;

Respectfully submitted,

/s/ Shamai Elstein

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Associate General Counsel
Shamai Elstein
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: May 23, 2014

Exhibit A

Proposed Reliability Standard

A. Introduction

1. Title: Physical Security

2. Number: CIP-014-1

3. Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner that owns a Transmission station or Transmission substation that meets any of the following criteria:

4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

4.1.1.3 Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or

Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

5. Effective Dates:

CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

This Reliability Standard addresses the directives from the FERC order issued March 7, 2014, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014), which required NERC to develop a physical security reliability standard(s) to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

B. Requirements and Measures

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or

- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner

shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

R5. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan.

R6. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified

Protection Professional (CPP) or Physical Security Professional (PSP) certification.

- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.
- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or
- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

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

The Transmission Owner and Transmission Operator shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation.

The responsible entities shall retain documentation as evidence for three years.

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

The CEA shall keep the last audit records and all requested and submitted subsequent audit records, subject to the confidentiality provisions of Section 1500 of the Rules of Procedure and the provisions of Section 1.4 below.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information

Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**High**	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection	Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.	Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.	performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.	uncontrolled separation, or Cascading within an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
R2	**Long-term Planning**	**Medium**	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than or equal to 100 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.	less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.	120 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed	following completion of Requirement R1; OR The Transmission Owner failed to have an unaffiliated third party verify the risk assessment performed under Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by Part 2.3.	
R3	**Long-term Planning**	**Lower**	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.	operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.	of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.	center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						identification in Requirement R1.
R4	**Operations Planning, Long-term Planning**	**Medium**	N/A	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
R5	**Long-term Planning**	**High**	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.	The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						center(s) identified in Requirement R1 and verified according to Requirement 2 but failed to include Parts 5.1 through 5.4 in the plan.
R6	**Long-term Planning**	**Medium**	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed	The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.	under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.	under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not document the reason for not modifying the security plan(s) as specified in Part 6.3.	the security plan(s) developed under Requirement R5; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	May 13, 2014	Adopted by NERC Board of Trustees	

Guidelines and Technical Basis

Section 4 Applicability

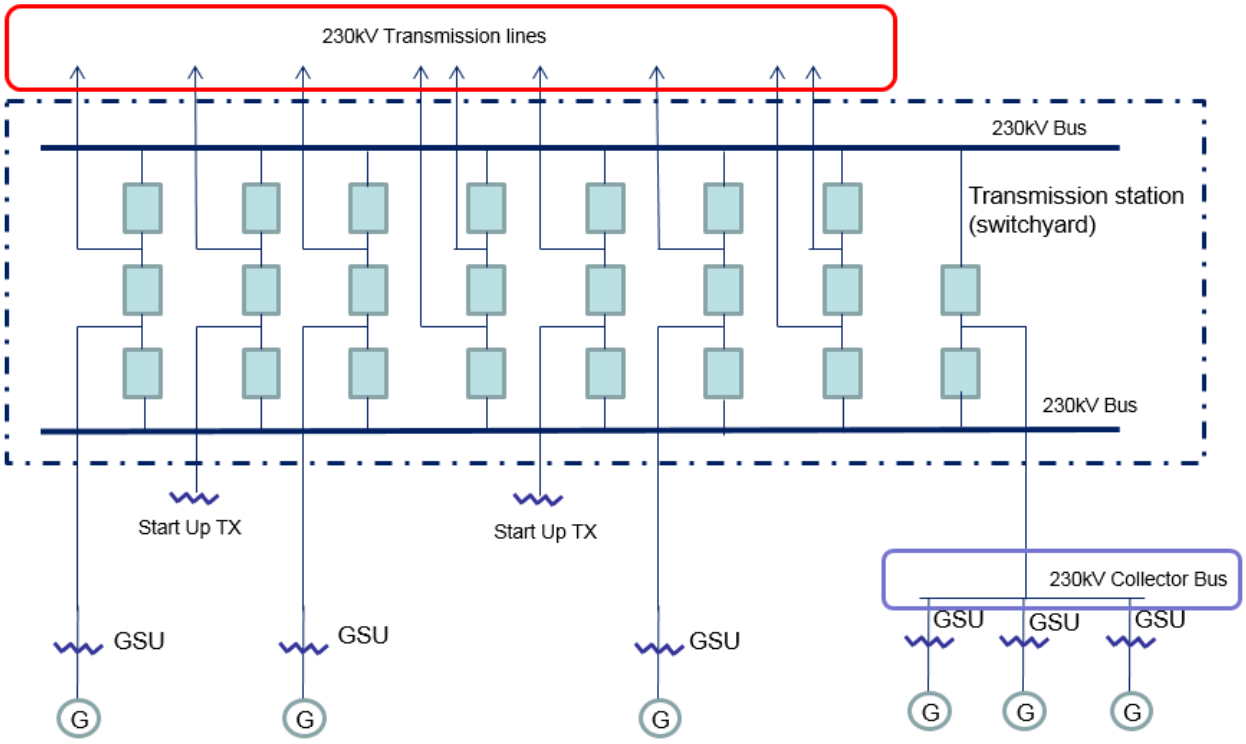
The purpose of Reliability Standard CIP-014-1 is to protect Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014-1 first applies to Transmission Owners that own Transmission Facilities that meet the specific criteria in Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4 mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1. Each Transmission Owner that owns Transmission Facilities that meet the criteria in Section 4.1.1.1 through 4.1.1.4 is required to perform a risk assessment as specified in Requirement R1 to identify its Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Standard Drafting Team (SDT) expects this population will be small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities. Only those Transmission Owners with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6.

This standard also applies to Transmission Operators. A Transmission Operator's obligations under the standard, however, are only triggered if the Transmission Operator is notified by an applicable Transmission Owner under Requirement R3 that the Transmission Operator operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the Requirement R1 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only Transmission Operators who are notified that they have primary control centers under this standard have performance obligations under Requirements R4 through R6. In other words, primary control center for purposes of this Standard is the control center that the Transmission Owner or Transmission Operator, respectively, uses as its primary, permanently-manned site to physically operate a Transmission station or Transmission substation that is identified in Requirement R1 and verified in Requirement R2. Control centers that provide back-up capability are not applicable, as they are a form of resiliency and intentionally redundant.

The SDT considered several options for bright line criteria that could be used to determine applicability and provide an initial threshold that defines the set of Transmission stations and Transmission substations that would meet the directives of the FERC order on physical security (*i.e.*, those that could cause widespread instability, uncontrolled separation, or Cascading within

an Interconnection). The SDT determined that using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. Additionally, the SDT concluded that using the CIP-002-5.1 Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment. As described in CIP-002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). The SDT understands that using this bright line criteria to determine applicability may require some Transmission Owners to perform risk assessments under Requirement R1 that will result in a finding that none of their Transmission stations or Transmission substations would pose a risk of widespread instability, uncontrolled separation, or Cascading within an Interconnection. However, the SDT determined that higher bright lines could not be technically justified to ensure inclusion of all Transmission stations and Transmission substations, and their associated primary control centers that, if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Further guidance and technical basis for the bright line criteria for Medium Impact Facilities can be found in the Guidelines and Technical Basis section of CIP-002-5.1.

Additionally, the SDT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. First, Transmission stations or Transmission substations interconnecting generation facilities are considered when determining applicability. Transmission Owners will consider those Transmission stations and Transmission substations that include a Transmission station on the high side of the Generator Step-up transformer (GSU) using Applicability Section 4.1.1.1 and 4.1.1.2. As an example, a Transmission station or Transmission substation identified as a Transmission Owner facility that interconnects generation will be subject to the Requirement R1 risk assessment if it operates at 500kV or greater or if it is connected at 200 kV – 499kV to three or more other Transmission stations or Transmission substations and has an "aggregate weighted value" exceeding 3000 according to the table in Applicability Section 4.1.1.2. Second, the Transmission analysis or analyses conducted under Requirement R1 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities. The diagram below shows an example of a station.



Also, the SDT uses the phrase "Transmission stations or Transmission substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (switching stations or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

On the issue of joint ownership, the SDT recognizes that this issue is not unique to CIP-014-1, and expects that the applicable Transmission Owners and Transmission Operators will develop memorandums of understanding, agreements, Coordinated Functional Registrations, or procedures, etc., to designate responsibilities under CIP-014-1 when joint ownership is at issue, which is similar to what many entities have completed for other Reliability Standards.

The language contained in the applicability section regarding the collector bus is directly copied from CIP-002-5.1, Attachment 1, and has no additional meaning within the CIP-014-1 standard.

Requirement R1

The initial risk assessment required under Requirement R1 must be completed on or before the effective date of the standard. Subsequent risk assessments are to be performed at least once every 30 or 60 months depending on the results of the previous risk assessment per Requirement R1, Part 1.1. In performing the risk assessment under Requirement R1, the

Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Applicability Section 4.1.1. Requirement R1 then requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The standard does not mandate the specific analytical method for performing the risk assessment. The Transmission Owner has the discretion to choose the specific method that best suites its needs. As an example, an entity may perform a Power Flow analysis and stability analysis at a variety of load levels.

Performing Risk Assessments

The Transmission Owner has the discretion to select a transmission analysis method that fits its facts and system circumstances. To mandate a specific approach is not technically desirable and may lead to results that fail to adequately consider regional, topological, and system circumstances. The following guidance is only an example on how a Transmission Owner may perform a power flow and/or stability analysis to identify those Transmission stations and Transmission substations that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. An entity could remove all lines, without regard to the voltage level, to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a significant area of the Interconnection. Using engineering judgment, the Transmission Owner (possibly in consultation with regional planning or operation committees and/or ISO/RTO committee input) should develop criteria (e.g. imposing a fault near the removed Transmission station or Transmission substation) to identify a contingency or parameters that result in potential widespread instability, uncontrolled separation, or Cascading within an Interconnection. Regional consultation on these matters is likely to be helpful and informative, given that the inputs for the risk assessment and the attributes of what constitutes widespread instability, uncontrolled separation, or Cascading within an Interconnection will likely vary from region-to-region or from ISO-to-ISO based on topology, system characteristics, and system configurations. Criteria could also include post-contingency facilities loadings above a certain emergency rating or failure of a power flow case to converge. Available special protection systems (SPS), if any, could be applied to determine if the system experiences any additional instability which may result in uncontrolled separation. Example criteria may include:

(a) Thermal overloads beyond facility emergency ratings;

(b) Voltage deviation exceeding ± 10%; or

(c) Cascading outage/voltage collapse; or

(d) Frequency below under-frequency load shed points

Periodicity

A Transmission Owner who identifies one or more Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection is required to conduct a risk assessment at least once every 30 months. This period ensures that the risk assessment remains current with projected conditions and configurations in the planned system. This risk assessment, as the initial assessment, must consider applicable planned Transmission stations and Transmission substations to be in service within 24 months. The 30 month timeframe aligns with the 24 month planned to be in service date because the Transmission Owner is provided the flexibility, depending on its planning cycle and the frequency in which it may plan to construct a new Transmission station or Transmission substation to more closely align these dates. The requirement is to conduct the risk assessment at least once every 30 months, so for a Transmission Owner that believes it is better to conduct a risk assessment once every 24 months, because of its planning cycle, it has the flexibility to do so.

Transmission Owners that have not identified any Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection are unlikely to see changes to their risk assessment in the Near-Term Planning Horizon. Consequently, a 60 month periodicity for completing a subsequent risk assessment is specified.

Identification of Primary Control Centers

After completing the risk assessment specified in Requirement R1, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center “operationally controls” a Transmission station or Transmission substation when the control center’s electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

Requirement R2

This requirement specifies verification of the risk assessment performed under Requirement R1 by an entity other than the owner or operator of the Requirement R1 risk assessment.

A verification of the risk assessment by an unaffiliated third party, as specified in Requirement R2, could consist of:

1. Certifying that the Requirement R1 risk assessment considers the Transmission stations and Transmission substations identified in Applicability Section 4.1.1.

2. Review of the model used to conduct the risk assessment to ensure it contains sufficient system topology to identify Transmission stations and Transmission substations that if rendered inoperable or damaged could cause widespread instability, uncontrolled separation, or Cascading within an Interconnection.
3. Review of the Requirement R1 risk assessment methodology.

This requirement provides the flexibility for a Transmission Owner to select from unaffiliated registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term unaffiliated means that the selected verifying entity cannot be a corporate affiliate (*i.e.,* the verifying or third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

The prohibition on registered entities using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. For instance, a U.S. federal power marketing agency may select as its verifier another U.S. federal agency to conduct its verification so long as the selected entity has transmission planning or analysis experience. Similarly, a Transmission Owner owned by a Canadian province can use a separate agency of that province to perform the verification. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

Requirement R2 also provides that the "verification may occur concurrent with or after the risk assessment performed under Requirement R1." This provision is designed to provide the Transmission Owner the flexibility to work with the verifying entity throughout (*i.e.,* concurrent with) the risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could collaborate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently. The intent of Requirement R2 is to have an entity other than the owner or operator of the facility to be involved in the risk assessment process and have an opportunity to provide input. Accordingly, Requirement R2 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the risk assessment and subsequently has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the risk assessment.

Characteristics to consider in selecting a third party reviewer could include:

- Registered Entity with applicable planning and reliability functions.
- Experience in power system studies and planning.
- The entity's understanding of the MOD standards, TPL standards, and facility ratings as they pertain to planning studies.

- The entity's familiarity with the Interconnection within which the Transmission Owner is located.

With respect to the requirement that Transmission owners develop and implement procedures for protecting confidential and sensitive information, the Transmission Owner could have a method for identifying documents that require confidential treatment. One mechanism for protecting confidential or sensitive information is to prohibit removal of sensitive or confidential information from the Transmission Owner's site. Transmission Owners could include such a prohibition in a non-disclosure agreement with the verifying entity.

A Technical feasibility study is not required in the Requirement R2 documentation of the technical basis for not modifying the identification in accordance with the recommendation.

On the issue of the difference between a verifier in Requirement R2 and a reviewer in Requirement R6, the SDT indicates that the verifier will confirm that the risk assessment was completed in accordance with Requirement R1, including the number of Transmission stations and substations identified, while the reviewer in Requirement R6 is providing expertise on the manner in which the evaluation of threats was conducted in accordance with Requirement R4, and the physical security plan in accordance with Requirement R5. In the latter situation there is no verification of a technical analysis, rather an application of experience and expertise to provide guidance or recommendations, if needed.

Parts 2.4 and 6.4 require the entities to have procedures to protect the confidentiality of sensitive or confidential information. Those procedures may include the following elements:

1. Control and retention of information on site for third party verifiers/reviewers.
2. Only "need to know" employees, etc., get the information.
3. Marking documents as confidential
4. Securely storing and destroying information when no longer needed.
5. Not releasing information outside the entity without, for example, General Counsel sign-off.

Requirement R3

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first completing the risk assessment specified by Requirement R1 and the verification specified by Requirement R2. Requirement R3 is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 receive notice so that the Transmission Operator may fulfill the rest of the obligations required in Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include within the notice the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk

assessment under Requirement R1 or as a result of the verification process under Requirement R2.

Requirement R4

This requirement requires owners and operators of facilities identified by the Requirement R1 risk assessment and that are verified under Requirement R2 to conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process. Threats and vulnerabilities may vary from facility to facility based on any number of factors that include, but are not limited to, location, size, function, existing physical security protections, and attractiveness as a target.

In order to effectively conduct a threat and vulnerability assessment, the asset owner may be the best source to determine specific site vulnerabilities, but current and evolving threats may best be determined by others in the intelligence or law enforcement communities. A number of resources have been identified in the standard, but many others exist and asset owners are not limited to where they may turn for assistance. Additional resources may include state or local fusion centers, U.S. Department of Homeland Security, Federal Bureau of Investigations (FBI), Public Safety Canada, Royal Canadian Mounted Police, and InfraGard chapters coordinated by the FBI.

The Responsible Entity is required to take a number of factors into account in Parts 4.1 to 4.3 in order to make a risk-based evaluation under Requirement R4.

To assist in determining the current threat for a facility, the prior history of attacks on similarly protected facilities should be considered when assessing probability and likelihood of occurrence at the facility in question.

Resources that may be useful in conducting threat and vulnerability assessments include:

- NERC Security Guideline for the Electricity Sector: Physical Security.
- NERC Security Guideline: Physical Security Response.
- ASIS International General Risk Assessment Guidelines.
- ASIS International Facilities Physical Security Measure Guideline.
- ASIS International Security Management Standard: Physical Asset Protection.
- Whole Building Design Guide - Threat/Vulnerability Assessments.

Requirement R5

This requirement specifies development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Requirement R5 specifies the following attributes for the physical security plan:

- *Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.*

  Resiliency may include, among other things:

  a. System topology changes,

  b. Spare equipment,

  c. Construction of a new Transmission station or Transmission substation.

  While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site.

- *Law enforcement contact and coordination information.*

  Examples of such information may be posting 9-1-1 for emergency calls and providing substation safety and familiarization training for local and federal law enforcement, fire department, and Emergency Medical Services.

- *A timeline for executing the physical security enhancements and modifications specified in the physical security plan.*

  Entities have the flexibility to prioritize the implementation of the various resiliency or security enhancements and modifications in their security plan according to risk, resources, or other factors. The requirement to include a timeline in the physical security plan for executing the actual physical security enhancements and modifications does not also require that the enhancements and modifications be completed within 120 days. The actual timeline may extend beyond the 120 days, depending on the amount of work to be completed.

- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

  A registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various sources. Some of these sources could include the ERO, ES-ISAC, and US and/or Canadian federal agencies. This information should be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in R5.

  Incremental changes made to the physical security plan prior to the next required third party review do not require additional third party reviews.

Requirement R6

This requirement specifies review by an entity other than the Transmission Owner or Transmission Operator with appropriate expertise for the evaluation performed according to

Requirement R4 and the security plan(s) developed according to Requirement R5. As with Requirement R2, the term unaffiliated means that the selected third party reviewer cannot be a corporate affiliate (*i.e.,* the third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Operator). A third party reviewer also cannot be a division of the Transmission Operator that operates as a functional unit.

As noted in the guidance for Requirement R2, the prohibition on registered entities using a corporate affiliate to conduct the review, however, does not prohibit a governmental entity from selecting as the third party reviewer another governmental entity within the same political subdivision. For instance, a city or municipality may use its local enforcement agency, so long as the local law enforcement agency satisfies the criteria in Requirement R6. The third party reviewer, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

The Responsible Entity can select from several possible entities to perform the review:

- *An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.*

  In selecting CPP and PSP for use in this standard, the SDT believed it was important that if a private entity such as a consulting or security firm was engaged to conduct the third party review, they must tangibly demonstrate competence to conduct the review. This includes electric industry physical security experience and either of the premier security industry certifications sponsored by ASIS International. The ASIS certification program was initiated in 1977, and those that hold the CPP certification are board certified in security management. Those that hold the PSP certification are board certified in physical security.

- *An entity or organization approved by the ERO.*

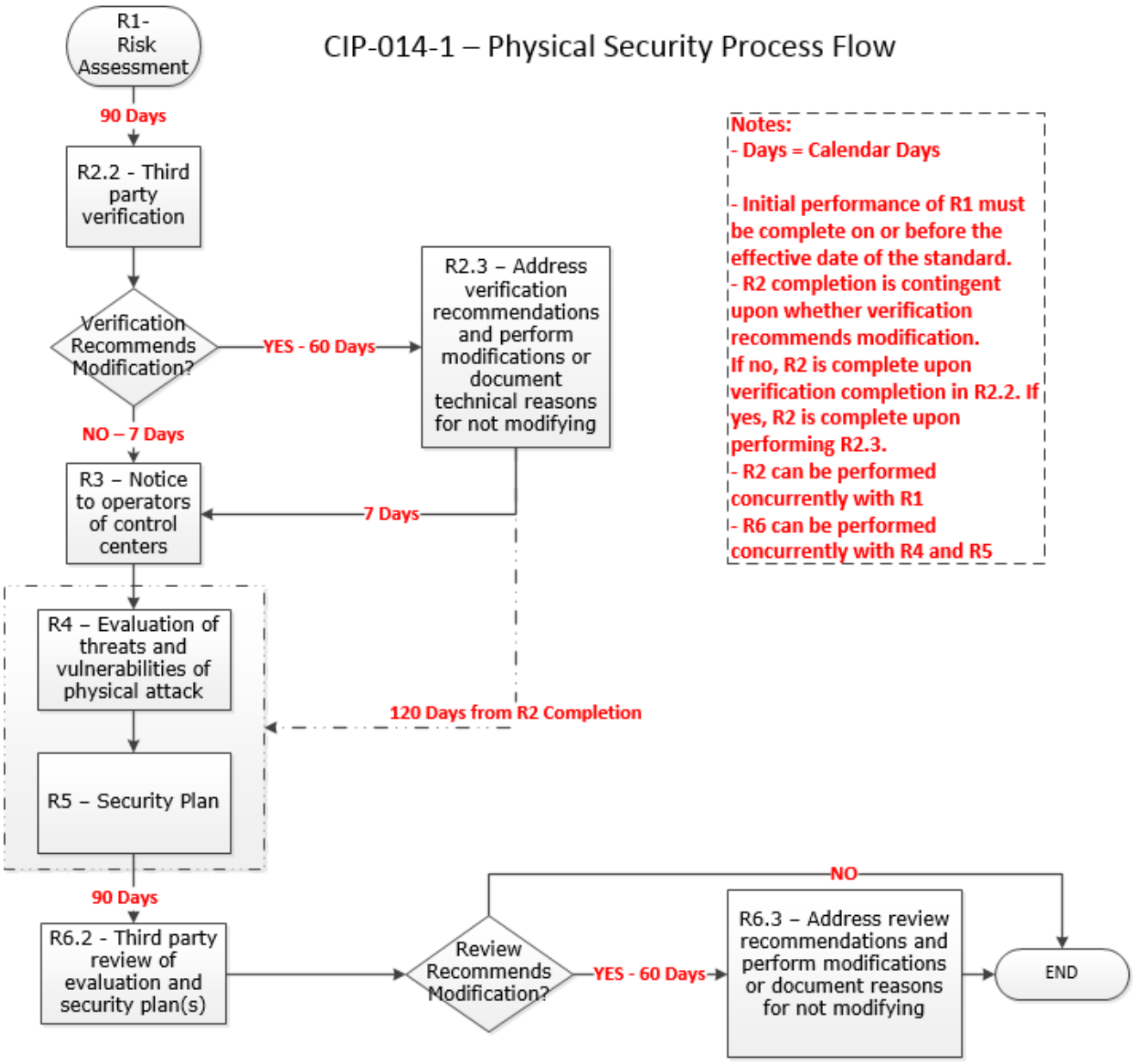
- *A governmental agency with physical security expertise.*

- *An entity or organization with demonstrated law enforcement, government, or military physical security expertise.*

As with the verification under Requirement R2, Requirement R6 provides that the "review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5." This provision is designed to provide applicable Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout (*i.e.,* concurrent with) the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5, which for some Responsible Entities may be more efficient and effective. In other words, a Transmission Owner or Transmission Operator could collaborate with their unaffiliated third party reviewer to perform an evaluation of potential threats and vulnerabilities (Requirement R4) and develop a security plan (Requirement R5) to satisfy Requirements R4 through R6 simultaneously. The

intent of Requirement R6 is to have an entity other than the owner or operator of the facility to be involved in the Requirement R4 evaluation and the development of the Requirement R5 security plans and have an opportunity to provide input on the evaluation and the security plan. Accordingly, Requirement R6 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the evaluation and develops the security plan itself and then has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the evaluation and develop the security plan.

Timeline


CIP-014-1 – Physical Security Process Flow
R1- Risk Assessment
90 Days
R2.2 - Third party verification
Verification Recommends Modification?
YES - 60 Days
R2.3 – Address verification recommendations and perform modifications or document technical reasons for not modifying
NO – 7 Days
R3 – Notice to operators of control centers
7 Days
R4 – Evaluation of threats and vulnerabilities of physical attack
120 Days from R2 Completion
R5 – Security Plan
90 Days
R6.2 - Third party review of evaluation and security plan(s)
Review Recommends Modification?
YES - 60 Days
R6.3 – Address review recommendations and perform modifications or document reasons for not modifying
NO
END
Notes:
- Days = Calendar Days
- Initial performance of R1 must be complete on or before the effective date of the standard.
- R2 completion is contingent upon whether verification recommends modification. If no, R2 is complete upon verification completion in R2.2. If yes, R2 is complete upon performing R2.3.
- R2 can be performed concurrently with R1
- R6 can be performed concurrently with R4 and R5

Rationale:

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

Rationale for Requirement R1:

This requirement meets the FERC directive from paragraph 6 in the order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through widespread instability, uncontrolled separation, or cascading failures. It also meets the portion of the directive from paragraph 11 for periodic reevaluation by requiring the risk assessment to be performed every 30 months (or 60 months for an entity that has not identified in a previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection).

After identifying each Transmission station and Transmission substation that meets the criteria in Requirement R1, it is important to additionally identify the primary control center that operationally controls that Transmission station or Transmission substation (*i.e.,* the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).

Rationale for Requirement R2:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring verification by an entity other than the owner or operator of the risk assessment performed under Requirement R1.

This requirement provides the flexibility for a Transmission Owner to select registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term “unaffiliated” means that the selected verifying entity cannot be a corporate affiliate (*i.e.*, the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit. The term “unaffiliated” is not intended to prohibit a governmental entity from using another government entity to be a verifier under Requirement R2.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout the Requirement R1 risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform a Requirement R1 risk assessment to satisfy both Requirement R1 and Requirement R2 concurrently.

Planning Coordinator is a functional entity listed in Part 2.1. The Planning Coordinator and Planning Authority are the same entity as shown in the NERC Glossary of Terms Used in NERC Reliability Standards.

Rationale for Requirement R3:

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first identifying which Transmission stations and Transmission substations meet the criteria specified by Requirement R1, as verified according to Requirement R2. This requirement is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1, Part 1.2 of a Transmission station or Transmission substation verified according to Requirement R2 receives notice of such identification so that the Transmission Operator may timely fulfill its resulting obligations under Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include notice of the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or the verification process under Requirement R2.

Rationale for Requirement R4:

This requirement meets the FERC directive from paragraph 8 in the order on physical security that the reliability standard must require tailored evaluation of potential threats and vulnerabilities to facilities identified in Requirement R1 and verified according to Requirement R2. Threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections, and attractiveness of the target. As such, the requirement does not mandate a one-size-fits-all approach but requires entities to account for the unique characteristics of their facilities.

Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur or be completed. However, Requirement R5 requires that the entity's security plan(s), which is dependent on the Requirement R4 evaluation, must be completed within 120 calendar days following completion of Requirement R2. Thus, an entity has the flexibility when to complete the Requirement R4 evaluation, provided that it is completed in time to comply with the requirement in Requirement R5 to develop a physical security plan 120 calendar days following completion of Requirement R2.

Rationale for Requirement R5:

This requirement meets the FERC directive from paragraph 9 in the order on physical security requiring the development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Rationale for Requirement R6:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring review by an entity other than the owner or operator with appropriate expertise of the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5.

As with the verification required by Requirement R2, Requirement R6 provides Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout the Requirement R4 evaluation and the development of the Requirement R5 security plan(s). This would allow entities to satisfy their obligations under Requirement R6 concurrent with the satisfaction of their obligations under Requirements R4 and R5.

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Project 2014-04

Approvals Requested
CIP-014-1 Physical Security

Prerequisite Approvals
None

Effective Date

New or Revised Standards
CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Standards for Retirement
None

Initial Performance of Periodic Requirements
The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard. Subsequent risk assessments shall be performed according to the timelines specified in CIP-014-1, Requirement R1.

The initial performance of CIP-014-1, Requirements R2 through R6, must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows:

- Requirement R2 shall be completed as follows:
    - Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard.
    - Part 2.3 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2.

- Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2.
- Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2.
- Requirement R6 shall be completed as follows:
    - Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5.
    - Part 6.3 shall be completed within 60 calendar days of Requirement R6 part 6.2.

Exhibit C

Order No. 672 Criteria

EXHIBIT C

Order No. 672 Criteria

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

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

Proposed Reliability Standard CIP-014-1 achieves the specific reliability goal of enhancing physical security measures for the most critical Bulk-Power System facilities and thereby lessening the overall vulnerability of the Bulk-Power System to physical attacks. The proposed Reliability Standard requires Transmission Owners and Transmission Operators to protect those critical Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Consistent with the Physical Security Order, the proposed Reliability Standard requires Transmission Owners to take the following steps to address the risks that physical attacks pose to the reliable operation of the Bulk-Power System:

1) Perform a risk assessment of their systems to identify (i) their critical Transmission stations and Transmission substations, and (ii) the primary control centers that operationally (i.e., physically) control the identified Transmission stations and Transmission substations.

---

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

[2] Order No. 672 at PP 321, 324.

2) Evaluate the potential threats and vulnerabilities of a physical attack to the facilities identified in the risk assessment.

3) Develop and implement a security plan, based on the evaluation of threats and vulnerabilities, designed to protect against and mitigate the impact of physical attacks that may compromise the operability or recovery of the identified critical facilities.

Further, the proposed Reliability Standard requires Transmission Operators that operate primary control centers that operationally control any of the Transmission stations or substations identified by the Transmission Owner to also:

1) evaluate the potential threats and vulnerabilities of a physical attack to such primary control centers; and

2) develop and implement a security plan, based on the evaluation of threats and vulnerabilities, designed to protect against and mitigate the impact of physical attacks that may compromise the operability or recovery of such primary control centers.

Additionally, proposed Reliability Standard CIP-014-1 includes requirements for: (i) the protection of sensitive or confidential information from public disclosure; (ii) third party verification of the identification of critical facilities as well as third party review of the evaluation of threats and vulnerabilities and the security plans; and (iii) the periodic reevaluation and revision of the identification of critical facilities, the evaluation of threats and vulnerabilities, and the security plans to help ensure their continued effectiveness.

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

The proposed Reliability Standard is clear and unambiguous as to what is required and who is required to comply, in accordance with Order No. 672. The proposed Reliability Standard applies to Transmission Owners and Transmission Operators. The proposed Reliability Standard clearly articulates the actions that such entities must take to comply with the standard.

---

[3] Order No. 672 at PP 322, 325.

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

The Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") for the proposed Reliability Standard comport with NERC and Commission guidelines related to their assignment, as discussed further in Exhibit E. The assignment of the severity level for each VSL is consistent with the corresponding requirement and the VSLs should ensure uniformity and consistency in the determination of penalties. The VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations. For these reasons, the proposed Reliability Standard includes clear and understandable consequences in accordance with Order No. 672.

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

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

---

4 Order No. 672 at P 326.

5 Order No. 672 at P 327.

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

The proposed Reliability Standard achieves the reliability goal effectively and efficiently in accordance with Order No. 672. The proposed Reliability Standard clearly enumerates the responsibilities of applicable entities with respect to the identification and protection of critical Bulk-Power System facilities and provides entities the flexibility to tailor their processes and plans required under the standard to best suit the needs of their organization.

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

The proposed Reliability Standard does not reflect a "lowest common denominator" approach. To the contrary, the proposed Reliability Standard contains significant benefits for the Bulk-Power System. The requirements of the proposed Reliability Standard help ensure that entities provide an adequate level of protection against physical attacks to critical facilities.

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

The proposed Reliability Standard applies throughout North America and does not favor one geographic area or regional model.

---

6 Order No. 672 at P 328.

7 Order No. 672 at P 329-30.

8 Order No. 672 at P 331.

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

The proposed Reliability Standard has no undue negative impact on competition. The proposed Reliability Standard requires the same performance by each applicable entity. The standard does not unreasonably restrict the available transmission capability or limit use of the Bulk-Power System in a preferential manner.

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

The proposed effective date for the standard is just and reasonable and appropriately balances the urgency in the need to implement the standard against the reasonableness of the time allowed for those who must comply to develop and implement the necessary procedures and policies. The proposed implementation period will allow applicable entities adequate time to meaningfully implement the requirements. The proposed effective date is explained in the proposed Implementation Plan, attached as Exhibit B.

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

The proposed Reliability Standard was developed in accordance with NERC's Commission-approved, ANSI- accredited processes for developing and approving Reliability Standards. Exhibit F includes a summary of the Reliability Standard development proceedings, and details the processes followed to develop the Reliability Standards. These processes included, among other things, comment and balloting periods. Additionally, all meetings of the

---

9 Order No. 672 at P 332.

10 Order No. 672 at P 333.

11 Order No. 672 at P 334.

drafting team were properly noticed and open to the public. The initial and additional ballots achieved a quorum and exceeded the required ballot pool approval levels.

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

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

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

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

---

[12] Order No. 672 at P 335.

[13] Order No. 672 at P 323.

Exhibit D

Consideration of Directives

Consideration of Issues and Directives

Project 2014-04 - Physical Security

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
P.6. The Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the Bulk-Power System. First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities." A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards. Instead, the Commission is directing NERC to develop Reliability	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring Transmission Owners to perform a risk assessment of its Transmission stations and substations that meet the criteria in Attachment 1 of CIP-002-5.1 for a Medium Impact rating to identify which of those Transmission stations and substations, if rendered inoperable or damaged as a result of a physical attack, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Transmission Owner must also identify the primary control centers that operationally controls each identified Transmission station or Transmission substation. The standard drafting team (SDT) determined that the CIP-002-5 bright line would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. If the Transmission Owner does not have any Transmission stations or Transmission substations that meet the Medium

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System and thereby warrant the directive imposed here.		Impact rating, it is not subject to the proposed Reliability Standard and, in turn, would not have to conduct the risk assessment. Consistent with the Commission's directive, Requirement R1 does not require a specific methodology for identifying facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; rather, the requirement mandates that the risk assessment shall consist of a transmission analysis or transmission analyses to ensure that the risk assessment is based on objective analysis, technical expertise, and experienced judgment. Lastly, Requirement R1 identifies the periodicity for conducting the risk assessments.
7. Issuance of this directive will help provide for the resiliency and reliable operation of the Bulk-Power System. To that end, the proposed Reliability Standards should allow owners or operators to consider resilience of the grid in the risk assessment when identifying critical facilities, and the elements that make up those facilities, such as transformers that typically require significant time to repair or replace. As part of this process, owners or operators may consider elements of resiliency such as how the system is designed,	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 provides Transmission Owners the flexibility to consider the resilience of their system when conducting their risk assessments. As noted above, Requirement R1 does not require a specific methodology for identifying their critical facilities and, in turn, allows an entity to use a methodology that considers how their system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
operated, and maintained, and the sophistication of recovery plans and inventory management.		
8. In the second step, the Reliability Standards should require owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities. The threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target. Thus, the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R4 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that the applicable Transmission Owner or Transmission Operator of facilities identified in accordance with Requirement R1 and verified in accordance with Requirement R2 conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive to "tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated," Requirement R4 states that the evaluation must consider: (1) the unique characteristics of the identified facilities; (2) prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and (3) intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U. S. federal and/or Canadian governmental agencies, or their successors.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Consistent with the Commission's statement that NERC should consider requiring owners and operators of identified facilities to consult with entities with appropriate expertise, Requirement R6 requires applicable Transmission Owners and Transmission Operators to select a third party to review their evaluation. This review may occur concurrently with or after the evaluation.
9. Third and finally, the Reliability Standards should require those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Reliability Standards themselves need not dictate specific steps an entity must take to protect against attacks on the identified facilities. However, the Reliability Standards need to require that owners or operators of identified critical facilities have a plan that results in an adequate level of protection against the potential physical threats and vulnerabilities they face at the identified critical facilities.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R5 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring the applicable Transmission Owner or Transmission Operator of facilities identified in accordance with Requirement R1 and verified in accordance with Requirement R2 to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive, Requirement R5 does not dictate specific steps an entity must take to protect against attacks on the identified facilities but requires applicable entities to develop a security plan that includes the following attributes to help ensure an adequate level of protection: (1) resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4; (2) law enforcement

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		contact and coordination information; (3) a timeline for executing the physical security enhancements and modifications specified in the physical security plan; and (4) provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).
10. All three steps of compliance with the Reliability Standard described above could contain sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure. Therefore, NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information that is needed to ensure compliance with the Reliability Standards.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	To protect confidential or sensitive information, the Compliance Monitoring section of the standard provides that evidence demonstrating compliance with the standard must be retained at the applicable entities' facilities. Additionally, Requirements R2 and R6 require applicable entities to implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to third party verifiers and reviewers and to protect or exempt sensitive or confidential information developed pursuant to the standard from public disclosure.
11. In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a	*Reliability Standards for Physical Security*	Requirements R2 and R6 respond to this directive. Under Requirement R3 Transmission Owners must have an unaffiliated third party verify the risk assessment performed under Requirement R1. The third party verifier must be either (1) a

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Reliability Coordinator, or another entity. The Reliability Standards should include a procedure for the verifying entity, as well as the Commission, to add or remove facilities from an owner's or operator's list of critical facilities. Similarly, the determination of threats and vulnerabilities and the security plan should also be reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise. Finally, the Reliability Standards should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. NERC should establish a timeline for when such reevaluations should occur.	*Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or (2) an entity that has transmission planning or analysis experience. The requirement provides that the verification shall either verify the Transmission Owner's risk assessment or include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The verification may occur concurrently with the Requirement R1 risk assessment but must be completed within 90 calendar days of the risk assessment. The Transmission Owner is required to either modify its identification based on the verifier's recommendation or, if it disagrees with the verifier's recommendations, document the technical basis for not modifying its identification. Similarly, under Requirement R6, applicable Transmission Owners and Operators must have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The reviewing entity must be (1) an entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification; (2) an entity or organization approved by the ERO; (3) a governmental agency with physical security expertise; or (4) an entity or organization with demonstrated law

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		enforcement, government, or military physical security expertise. The third party review must be completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The applicable Transmission Owners and Transmission Operators are required to either modify their evaluation or security plan(s) consistent with the reviewer's recommendations or, if they disagree with the recommendations, document the reasons for not modifying. Consistent with the directive to establish a timeline for periodic reevaluation of the identification of facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection, the assessment of the potential risks and vulnerabilities, and the security plans, the standard provides that Requirement R1 risk assessment should be performed at least once every 30 calendar months for those Transmission Owners that identified facilities in their previous risk assessment and once every 60 calendar months for those Transmission Owners that did not identify facilities in their previous risk assessment. Upon completion of each subsequent risk assessment, the applicable entities must satisfy the obligations under the remaining requirements.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
12. Under the Reliability Standards, we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard. We also recognize that the industry has engaged in longstanding efforts to address the physical security of its critical facilities. Thus, NERC should develop an implementation plan that requires owners or operators of the Bulk-Power System to implement the Reliability Standards in a timely fashion, balancing the importance of protecting the Bulk-Power System from harm while giving the owners or operators adequate time to meaningfully implement the requirements. NERC should file the plan with the Reliability Standards for Commission review.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	The proposed Implementation Plan addresses this directive. As provided in the Implementation Plan, the standard becomes effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows: - Requirement R2, Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard. Requirement R2, Part 2.3 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2. - Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		- Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2. - Requirement R6, Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5. Requirement R6, Part 6.3 shall be completed within 60 calendar days of Requirement R6 Part 6.2.

Exhibit E

Analysis of Violation Risk Factors and Violation Security Levels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2014-04: Physical Security

VRF and VSL Justifications for CIP-014-1

VRF and VSL Justifications – CIP-014-1, R1	
Proposed VRF	High
NERC VRF Discussion	Initial and subsequent risk assessments identify Transmission stations or Transmission substations that need to be assessed for threats and vulnerabilities and potential physical security measures. Since this is a Requirement in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition. This justifies a High VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the risk assessment periodicity and the identification of the primary control center that has operational control of Transmission stations and/or Transmission substations.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable CIP-002-5.1 R1, which deals with categorizing cyber systems, is assigned a High VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date;

VRF and VSL Justifications – CIP-014-1, R1	
	OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.
Proposed Moderate VSL	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.
Proposed High VSL	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in

VRF and VSL Justifications – CIP-014-1, R1	
	the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.
Proposed Severe VSL	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within

VRF and VSL Justifications – CIP-014-1, R1	
	an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if the risk assessment is not performed or if the risk assessment is not performed within required intervals.
FERC VSL G3 Violation Severity Level	The language of the VSL directly mirrors the language in the corresponding requirement.

VRF and VSL Justifications – CIP-014-1, R1	
Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to submit perform a risk assessment.

VRF and VSL Justifications – CIP-014-1, R2	
Proposed VRF	Medium
NERC VRF Discussion	Unaffiliated third party verification of initial and subsequent risk assessments provides reinforcement that the risk assessment was performed with due consideration to risk to the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of this requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. This justifies a Medium VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the unaffiliated third party verification including entities that may perform the verification, provisions for adding or removing Transmission stations and/or Transmission substations, and provisions for confidentiality of sensitive information.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable EOP-005-2 R6, which deals with verifying that its restoration plan accomplishes its intended function is assigned a medium VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but less than or equal to 100 calendar days following completion of Requirement R1;

VRF and VSL Justifications – CIP-014-1, R2	
	OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.
Proposed Moderate VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.
Proposed High VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to 120 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by part 2.3.
Proposed Severe VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days following completion of Requirement R1; OR The Transmission Owner failed to have an unaffiliated third party

VRF and VSL Justifications – CIP-014-1, R2	
	verify the risk assessment performed under Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if an unaffiliated third party verification is not performed or if the verification is not performed within prescribe timelines. The VSLs are also written indicating violation of the Requirement Part regarding protection of information.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based	The VSL is assigned for a single instance of failing to have an unaffiliated third party verification performed; or failing to perform the verification within prescribe timelines; or failing to implement procedures to protect information.

VRF and VSL Justifications – CIP-014-1, R2	
on A Single Violation, Not on A Cumulative Number of Violations	

VRF and VSL Justifications – CIP-014-1, R3	
Proposed VRF	Lower
NERC VRF Discussion	Notifying the Transmission Operator that it has operational control of a Transmission station or Transmission substation identified in Requirement R1 and verified in Requirement R2 is necessary so that the Transmission Operator may begin performance of subsequent physical security requirements for the primary control center. This is a requirement that is administrative in nature and in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. This justifies a Lower VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the notification of the Transmission Operator regarding the removal of a Transmission station or Transmission substation.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable INT-006-4 R6, which deals with notifying other entities so that Confirmed Interchange may be implemented, is assigned a Lower VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar

VRF and VSL Justifications – CIP-014-1, R3	
	days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.
Proposed Moderate VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.
Proposed High VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.
Proposed Severe VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1.

VRF and VSL Justifications – CIP-014-1, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if notification is not made subject to the conditions of the requirement.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to make the appropriate notification.

VRF and VSL Justifications – CIP-014-1, R4	
Proposed VRF	Medium
NERC VRF Discussion	Performing an evaluation of potential threats and vulnerabilities of a physical attack to each of respective Transmission station(s), Transmission substation(s), and primary control center(s) is necessary to ensure the physical security of those assets as well as the reliability of the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of this requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. This justifies a Medium VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the evaluation of potential threats and vulnerabilities of a physical attack to Transmission stations and/or Transmission substations.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable CIP-007-5 R2, which deals with a patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets, is assigned a Medium VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	N/A

VRF and VSL Justifications – CIP-014-1, R4	
Proposed Moderate VSL	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.
Proposed High VSL	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.
Proposed Severe VSL	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if a responsible entity fails to conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) or failed to consider any of the Requirement Parts 4.1-4.3.

VRF and VSL Justifications – CIP-014-1, R4	
Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) or failing to consider any of the Requirement Parts 4.1-4.3.

VRF and VSL Justifications – CIP-014-1, R5	
Proposed VRF	High
NERC VRF Discussion	Development, implementation and execution of a documented physical security plan(s) that covers applicable Transmission station(s), Transmission substation(s), and primary control center(s) is necessary to ensure the physical security of those assets as well as the reliability of the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition. This justifies a High VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the physical security plan for applicable Transmission stations, Transmission substations, or primary control centers.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable CIP-003-3 R4, which deals with implementing and documenting a program to identify, classify, and protect information associated with Critical Cyber Assets, is assigned a High VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2;

VRF and VSL Justifications – CIP-014-1, R5	
	OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.
Proposed Moderate VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.
Proposed High VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.
Proposed Severe VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission

VRF and VSL Justifications – CIP-014-1, R5	
	station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include Parts 5.1 through 5.4 in the plan.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if a responsible entity fails to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) or if the responsible entity failed to include any of the Requirement Parts 5.1-5.4.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level	The VSL is assigned for a single instance of failing to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and

VRF and VSL Justifications – CIP-014-1, R5	
Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	primary control center(s) or failing to include any of the Requirement Parts 5.1-5.4.

VRF and VSL Justifications – CIP-014-1, R6	
Proposed VRF	Medium
NERC VRF Discussion	Unaffiliated third party review of the threat evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 provides reinforcement that these requirements were performed with due consideration to risk to the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of this requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. This justifies a Medium VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the unaffiliated third party review including entities that may perform the review, timelines for completing the review and provisions for confidentiality of sensitive information.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable EOP-005-2 R6, which deals with verifying that its restoration plan accomplishes its intended function is assigned a medium VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days;

VRF and VSL Justifications – CIP-014-1, R6	
	OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.
Proposed Moderate VSL	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.
Proposed High VSL	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not and modify or document the reason for not modifying the security plan(s) as specified in Part 6.3.
Proposed Severe VSL	The Responsible Entity failed to have an unaffiliated third party

VRF and VSL Justifications – CIP-014-1, R6	
	review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.3.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if an unaffiliated third party review is not performed or if the review is not performed within prescribe timelines. The VSLs are also written indicating violation of the Requirement Part regarding protection of information.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The language of the VSL directly mirrors the language in the corresponding requirement.

VRF and VSL Justifications – CIP-014-1, R6	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to have an unaffiliated third party review performed; or failing to perform the review within prescribe timelines; or failing to implement procedures to protect information.

Exhibit F

Summary of Development History and Record of Development

Summary of Development History

Summary of Development History

The development record for proposed Reliability Standard CIP-014-1 is summarized below.

I. Overview of the Standard Drafting Team

When evaluating a proposed Reliability Standard, the Commission is expected to give "due weight" to the technical expertise of the ERO.[1] The technical expertise of the ERO is derived, in part, from the standard drafting team. For this project, the standard drafting team consisted of industry experts, all a diverse set of experiences. A roster of the standard drafting team members is included in Exhibit G.

II. Standard Development History

Following the issuance of the Physical Security Order, the NERC Standards Committee ("SC"), working with NERC staff, initiated Project 2014-04 Physical Security to develop a proposed Reliability Standard to satisfy FERC's directive to submit one or more physical security Reliability Standards by June 5, 2014 (i.e., within 90 days of the Physical Security Order).

A. Standard Processes Manual Waivers and Formation of Standards Drafting Team

To facilitate meeting the 90-day timeline, the NERC Standards Committee approved waivers to the Standard Processes Manual to shorten the comment and ballot periods for the Standards Authorization Request ("SAR") and draft Reliability Standard. The Standards Committee, working with NERC staff, also moved expeditiously to form a standard drafting team.

---

[1] Section 215(d) (2) of the Federal Power Act; 16 U.S.C. §824(d) (2) (2006).

Specifically, on March 12, 2014, the following actions were taken: (1) Standards Committee authorized solicitation of a drafting team; (2) the SC chair presented to the SC a proposal for waiver of certain provisions in the Standard Processes Manual to shorten the comment and ballot periods for the Standards Authorization Request ("SAR") and draft Reliability Standard; and (3) NERC posted solicitation of standard drafting team announcement, with nominations due Tuesday, March 18. On March 14, 2014 NERC posted notice of request for waiver of certain Standards Processes Manual provisions in accordance with Section 16 of the Standard Processes Manual. On March 21, 2014, the Standards Committee approved the requested waivers and appointed the standards drafting team.

B. Standard Authorization Request Development

NERC submitted a SAR to the SC on March 12, 2014. On March 21, 2014, the SC accepted the SAR and NERC posted the SAR for a seven-day informal comment period from March 21-28, 2014 in accordance with the SC-approved waiver of the Standard Processes Manual.

C. Technical Conference

On April 1, 2014, NERC held a technical conference to provide an opportunity for the standards drafting team, NERC, and industry participants to discuss issues related to applicability, identification of critical facilities, evaluation of threats and vulnerabilities, development and implementation of physical security plans, and a proposed implementation plan for the proposed Reliability Standard.

D. First Posting

Following standard drafting team meetings, NERC posted proposed Reliability Standard CIP-014-1 for a 15-day formal comment period from April 10, 2014 through April 24, 2014 in

accordance with the SC-approved waiver. On April 9, 2014, the Standards Committee authorized the posting of the proposed Reliability Standard for comment and ballot.

There were 136 sets of responses to the posting, including comments from approximately 240 different people from approximately 165 companies representing all 10 of the industry segments. The proposed Reliability Standard received a quorum of 88.60% and an approval of 82.07%.

The standard drafting team considered all comments and made the following non-substantive changes, among others, to the standard to incorporate stakeholder recommendations:

- Part 4.1.1 of the applicability section was changed to clarify that applicable Transmission Owners are those that own transmission stations or transmission substations meeting the criteria in 4.1.1.4 through 4.1.1.4.
- The exemption for covered by a security plans under Nuclear Regulatory Commission or Canadian Nuclear Safety Commission jurisdiction was changed to provide clarity on the scope of the exemption.
- Several additions were made to the guidance section of the standard to address stakeholder concerns.
- The standard drafting team drafted language in Requirement R2, Part 2.4, Requirement R6, Part 6.4 and Section 1.4 of the Compliance section of the standard to address confidentiality.
- The standard drafting team added language to the Guidelines and Technical Basis section to clarify the use of the term collector bus.
- Requirement R2, Part 2.2 was reworded to align with the intended applicable entity.
- A change was made to Requirement R3 to accurately state which primary control centers are included in the requirement.
- Changes were made to clarify factors to be considered by the responsible entity in Requirements R4 Parts 4.2 and 4.3.
- Requirement R5 was reworded to clarify the standard drafting team's intent for security plans to be developed within 120 days of completing Requirement R2 and executed according to the timeline specified in the security plan.

- Requirement R6, Part 6.1 was changed to clearly indicate that one or more of the criteria must be met.

- The standard drafting team added commentary in the Guidelines and Technical Basis section to address joint ownership.

E. Final Ballot

Proposed Reliability Standard CIP-014-1 was posted for a 5-day final ballot period from May 1, 2014 through May 5, 2014 in accordance with the SC-approved waiver. The proposed Reliability Standard received a quorum of 92.53% and an approval of 85.61%.

F. Board of Trustees Approval

Proposed Reliability Standard CIP-014-1 was approved by NERC Board of Trustees on May 13, 2014.

Record of Development

Project 2014-04 Physical Security

Related Files

Status:

The NERC Board of Trustees adopted the CIP-014-1 standard at their May 13, 2014 meeting and NERC staff is preparing the FERC filing.

Background:

This project will address the directives issued in the FERC Order on Reliability Standards for Physical Security Measures under Docket No. RD14-6-000 issued March 7, 2014. The Commission directed "The North American Electric Reliability Corporation (NERC), as the Commission-certified Electric Reliability Organization (ERO), to submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. The Commission directs NERC to submit the proposed Reliability Standards to the Commission within 90 days of the date of this order."

Purpose/Industry Need:

From the Order: "Physical attacks to the Bulk-Power System can adversely impact the reliable operation of the Bulk-Power System, resulting in instability, uncontrolled separation, or cascading failures. However, the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks on the Bulk-Power System. Therefore, to carry out section 215 of the FPA and to provide for the reliable operation of the Bulk-Power System, the Commission directs the ERO to develop and file for approval proposed Reliability Standards that address threats and vulnerabilities to the physical security of critical facilities on the Bulk-Power System. Such Reliability Standards will enhance the Commission's ability to assure the public that critical facilities are reasonably protected against physical attacks."

Draft	Actions	Dates	Results	Consideration of Comments
CIP-014-1 Clean (21) | Redline to Last Posted (22) Implementation Plan (23)	Final Ballot Info>> (29) Vote>>	05/01/14 - 05/05/14	Summary>> (30) Ballot Results>> (31)	

Supporting Materials: Consideration of Issues and Directives Clean (24) | Redline to Last Posted (25) VRF/VSL Justifications (26) Draft RSAW Clean (27) | Redline to Last Posted (28)				
CIP-014-1 (7) Implementation Plan (8) **Supporting Materials:** Project Overview (9) FAQ (10) Unofficial Comment Form (Word) (11) Consideration of Issues and Directives (12) Draft RSAW (13)	Initial Ballot and Non-Binding Poll Info>> (14) Vote>>	04/20/14 - 04/24/14	Summary>> (16) Ballot Results>> (17) Non-Binding Poll Results>> (18)	Consideration of Comments>> (20)
	Comment Period Info>> (15) Submit Comments>>	04/10/14 - 04/24/14	Comments Received>> (19)	
	Join Ballot Pool>>	04/10/14 - 04/19/14		
	Please send feedback on the draft RSAW to: RSAWfeedback@nerc.net	04/10/14 - 04/24/14		
Standards Authorization Request (3)	Comment Period Info>> (5) Submit Comments>>	03/21/14 – 03/28/14	Comments Received>> (6)	

Supporting Materials: Unofficial Comment Form (Word) (4)	Join Ballot Pool>>			
Supporting Materials: Nomination Form (Word) (1)	Nomination Period Info>> (2) Submit Nominations>>	03/12/14 - 03/18/14		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2014-04 Physical Security Standard Drafting Team

Please complete the electronic nomination form as soon as possible, but no later than **March 18, 2014.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form. If you have any questions, please contact Stephen Crutchfield.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in the drafting team meetings (see dates of technical conference and first drafting team meeting below) if appointed by the Standards Committee. If appointed, you are expected to attend most of the face-to-face drafting team meetings as well as participate in all the team meetings held via conference calls. Failure to do so may result in your removal from the drafting team.

Background Information

Nominations are being sought for the Project 2014-04 Physical Security Standard Drafting Team (SDT). On March 7, 2014, FERC issued an Order, directing NERC to develop a new Reliability Standard to address concerns about the physical security of the Bulk-Power System. From the order:

> "The Commission directs the North American Electric Reliability Corporation (NERC), as the Commission-certified Electric Reliability Organization (ERO), to submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. The Commission directs NERC to submit the proposed Reliability Standards to the Commission within 90 days of the date of this order."

Potential SDT members should have experience in physical security programmatic design, risk assessments, evaluations, management, and identification of critical transmission substations and control centers, rather than the execution of physical security plan mitigation measures. In addition, compliance, legal, regulatory, and technical writing are desired. Previous drafting team experience and/or experience with development of standards is beneficial, but not required.

The expected time commitment for this team is aggressive because of directives with a deadline associated with them. The SDT is expected to meet in person for up to three full three-day meetings

during the project which is anticipated to last 90 days, with additional conference calls between face-to-face meetings as necessary to meet the aggressive project schedule. The first technical conference will be held in Atlanta on April 1, 2014 and the new drafting team will meet immediately following, April 2-4, 2014. SDT members are expected to attend both events.

Please provide the following information for the nominee:	
Name:	
Title:	
Organization:	
Address:	
Telephone:	
Email:	

Please briefly describe the nominee's experience and qualifications to serve on the selected project:

If you are currently a member of any NERC SAR or standard drafting team(s), please list each team here:

☐ Not currently on any active SAR or standard drafting team.

☐ Currently a member of the following SAR or standard drafting team(s):

If you previously worked on any NERC SAR or standard drafting team(s)s, please identify the team(s):

☐ No prior NERC SAR or standard drafting team.

☐ Prior experience on the following SAR or standard drafting team(s):

Select each NERC Region in which you have experience relevant to Project 2014-04:

☐ ERCOT	☐ NPCC	☐ SPP
☐ FRCC	☐ RFC	☐ WECC
☐ MRO	☐ SERC	☐ NA – Not Applicable

Select each Industry Segment that you represent:	
☐	1 — Transmission Owners
☐	2 — RTOs, ISOs
☐	3 — Load-serving Entities
☐	4 — Transmission-dependent Utilities
☐	5 — Electric Generators
☐	6 — Electricity Brokers, Aggregators, and Marketers
☐	7 — Large Electricity End Users
☐	8 — Small Electricity End Users
☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
☐	10 — Regional Reliability Organizations and Regional Entities
☐	NA – Not Applicable

Select each Function[1] in which you have current or prior expertise:	
☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:		Telephone:	
Organization:		Email:	

[1] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

Name:		Telephone:	
Organization:		Email:	
Provide the names and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:		Telephone:	
Title:		Email:	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security Standard Drafting Team

Nomination Period Now Open through March 18, 2014

This email distribution list may include individuals subject to ex parte communication restrictions pursuant to Rule 2201 of the Federal Energy Regulatory Commission's regulations governing off-the-record communications (18 C.F.R. § 385.2201 (2014)). Please refrain from using this distribution list for any substantive communications related to Project 2014-04, Physical Security.

Link to Official Nomination Form
Link to Word Version of Nomination Form

Nominations are being sought for the Project 2014-04 Physical Security Standard Drafting Team (SDT). On March 7, 2014, FERC issued an Order, directing NERC to develop a new Reliability Standard to address concerns about the physical security of the Bulk-Power System. From the order:

> "The Commission directs the North American Electric Reliability Corporation (NERC), as the Commission-certified Electric Reliability Organization (ERO), to submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. The Commission directs NERC to submit the proposed Reliability Standards to the Commission within 90 days of the date of this order."

Potential SDT members should have experience in physical security programmatic design, risk assessments, evaluations, management, and identification of critical transmission substations and control centers, rather than the execution of physical security plan mitigation measures. In addition, compliance, legal, regulatory, and technical writing are desired. Previous drafting team experience and/or experience with development of standards is beneficial, but not required.

The expected time commitment for this team is aggressive because of directives with a deadline associated with them. The SDT is expected to meet in person for up to three full three-day meetings during the project which is anticipated to last 90 days, with additional conference calls between face-to-face meetings as necessary to meet the aggressive project schedule. The first technical conference will be held in Atlanta on April 1, 2014 and the new drafting team will meet immediately following, April 2-4, 2014. SDT members are expected to attend both events.

Submitting a Nomination

If you are interested in serving on the SDT, please complete the official nomination form by **March 18, 2013**. The nomination form should be submitted describing the individual's experience or qualifications related to the project.

An unofficial Word version of the nomination form is also posted on the Standard Drafting Team Vacancies page.

For information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Standards Authorization Request Form

When completed, email this form to:
Barbara.Nutter@nerc.net

For questions about this form or for assistance in completing the form, call Barb Nutter at 404-446-9692.

NERC welcomes suggestions for improving the reliability of the Bulk-Power System through improved Reliability Standards. Please use this form to submit your proposal for a new NERC Reliability Standard or a revision to an existing standard.

Request to propose a new or a revision to a Reliability Standard			
Proposed Standard:	Project 2014-04 Physical Security Reliability Standard(s)		
Date Submitted:	March 12, 2014		
SAR Requester Information			
Name:	Stephen Crutchfield		
Organization:	NERC Staff		
Telephone:	609-651-9455	E-mail:	Stephen.crutchfield@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard		☐ Withdrawal of existing Standard	
☐ Revision to existing Standard		☐ Urgent Action	

SAR Information
Industry Need (What is the industry problem this request is trying to solve?):
On March 7, 2014, FERC issued an order directing the ERO to develop a standard to address the physical security of critical facilities on the Bulk-Power System. In the order, FERC stated: "The Commission directs the North American Electric Reliability Corporation (NERC), as the Commission-certified Electric Reliability Organization (ERO), to submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. The Commission directs NERC to submit the proposed Reliability Standards to the Commission within 90 days of the date of this order." *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 at P 1 (2014) ("FERC Order").
SAR Information
Purpose or Goal (How does this request propose to address the problem described above?):
The primary goal of this SAR is to allow the Standard Drafting Team (SDT) for Project 2014-04, Physical Security to develop a standard(s) to address the directives of the March 7, 2014 FERC Order and to ensure consistency within the NERC body of Reliability Standards.
Identify the Objectives of the proposed standard's requirements (What specific reliability deliverables are required to achieve the goal?):
Provide clear, unambiguous requirements and standard(s) to address the directives in the March 7, 2014 FERC Order regarding the physical security of critical facilities on the Bulk-Power System.
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The SDT shall develop standard requirements, Violation Risk Factors, Violation Severity Levels, and implementation plan and shall work with compliance on an accompanying RSAW to address each of the directives in the March 7, 2014 FERC Order.

SAR Information
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
The SDTs execution of this SAR requires the SDT to address each of the FERC directives in the deadline required by the Order. The reliability assessment and justification is also set forth in the March 7, 2014 FERC Order. The March 7, 2014 FERC Order is incorporated in its entirety into this SAR, so as not to unnecessarily repeat or paraphrase the substance of the Order. There are no market interface impacts resulting from the standard action on physical security.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☐ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☐ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☐ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐ Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.

Reliability Functions		
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☐	Distribution Provider	Delivers electrical energy to the End-use customer.
☐	Generator Owner	Owns and maintains generation facilities.
☐	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☐	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.

Reliability and Market Interface Principles	
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Related Standards	
Standard No.	Explanation
CIP-006-5 CIP-008-5 CIP-009-5	Review to ensure no language and terminology inconsistency with requirements developed under this project.

Related Standards	

Related SARs	
SAR ID	Explanation
N/A	N/A

Regional Variances	
Region	Explanation
ERCOT	N/A
FRCC	N/A
MRO	N/A
NPCC	N/A
RFC	N/A
SERC	N/A
SPP	N/A
WECC	N/A

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2014-04 Physical Security

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments on the draft Physical Security Standard Authorization Request (SAR). The electronic comment form must be completed by **8:00 p.m. Eastern on March 28, 2014**.

If you have questions please contact Stephen Crutchfield via email or by telephone at 609-651-9455.

The project page may be accessed by clicking here.

Background Information

On March 7, 2014, FERC issued an order directing the ERO to develop a standard to address the physical security of critical facilities on the Bulk-Power System. In the order, FERC stated:

"The Commission directs the North American Electric Reliability Corporation (NERC), as the Commission-certified Electric Reliability Organization (ERO), to submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. The Commission directs NERC to submit the proposed Reliability Standards to the Commission within 90 days of the date of this order."

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

Questions

1. Do you agree with the scope and contents of the SAR? If not, please provide specific comments and suggestions for SDT consideration.

   ☐ Yes
   ☐ No
   Comments:

2. Are you aware of any regional variances associated with approved NERC Reliability Standards that will be needed as a result of this project? If yes, please identify the Regional Variance.

   ☐ Yes
   ☐ No
   Comments:

3. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standard(s)? If yes, please identify the jurisdiction and specific regulatory requirements.

   ☐ Yes
   ☐ No
   Comments:

4. Are there any other concerns with this SAR?

   ☐ Yes
   ☐ No
   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security Standards Authorization Request

Informal Comment Period: March 21-28, 2014

Ballot Pools Forming Now

This email distribution list may include individuals subject to ex parte communication restrictions pursuant to Rule 2201 of the Federal Energy Regulatory Commission's regulations governing off-the-record communications (18 C.F.R. § 385.2201 (2014)). Please refrain from using this distribution list for any substantive communications related to Project 2014-04, Physical Security.

Now Available

A 7-day informal comment period for the **Project 2014-04 Physical Security Standards Authorization Request** is open through **8 p.m. Eastern on Friday, March 28, 2014.**

If you have questions please contact Stephen Crutchfield via email or by telephone at (609) 651-9455.

Background information for this project can be found on the project page.

Instructions for Commenting

Please use the electronic form to submit comments on the revised definition. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Instructions for Joining Ballot Pool

Ballots pools are being formed for Project 2014-04 – Physical Security and the associated non-binding poll on this project. Registered Ballot Body members must join the ballot pools to be eligible to vote in the balloting and submittal of an opinion for the non-binding poll of the associated VRFs and VSLs. Registered Ballot Body members may join the ballot pools at the following page: Join Ballot Pool

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list servers for this project are:

Initial Ballot: bp-2014-04_CIP-014-1_in@nerc.com
Non-Binding poll: bp-2014-04_CIP-014-1_NB_in@nerc.com

For information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Comment Summary

Project 2014-04 Physical Security

The Project 2014-04 Physical Security Standard Authorization Request (SAR) was posted for a 7-day public comment period from March 21, 2014 through March 28, 2014. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form.

Index to Questions, Comments, and Responses

1. **Do you agree with the scope and contents of the SAR? If not, please provide specific comments and suggestions for SDT consideration.** 10
2. **Are you aware of any regional variances associated with approved NERC Reliability Standards that will be needed as a result of this project? If yes, please identify the Regional Variance** 30
3. **Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standard(s)? If yes, please identify the jurisdiction and specific regulatory requirements.**.....35
4. **Are there any other concerns with this SAR?** 40

The Industry Segments are:

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

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

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	David Burke	Orange and Rockland Utilities Inc.	NPCC	3
3.	Greg Campoli	New Yorki Independent System Operator	NPCC	2
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
5.	Ben Wu	Orange and Rockland Utilities Inc.	NPCC	1
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
7.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Ayesha Sabouba	Hydro One Networks, Inc.	NPCC	1
10.	Mark Kenny	Northeast Utilities	NPCC	1

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

11.	Christina Koncz	PSEG Power LLC	NPCC	5
12.	Helen Lainis	Independent Electricity System Operator	NPCC	2
13.	Michael Lombardi	Northeast Power Coordinating Council	NPCC	10
14.	Alan MacNaughton	New Brunswick Power Corporation	NPCC	9
15.	Bruce Metruck	New York Power Authority	NPCC	6
16.	Silvia Parada Mitchell	NextEra energy, LLC	NPCC	5
17.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
18.	Robert Pellegrini	The United Illuminating Company	NPCC	1
19.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
20.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
21.	Wayne Sipperly	New York Power Authority	NPCC	5

2.	Group	Richard Hoag	FirstEnergy Corp.	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	William Smith	FirstEnergy Corp		1
2.	Cindy Stewart	FirstEnergy Corp		3
3.	Doug Hohlbaugh	Ohio Edison		4
4.	Ken Dresner	FirstEnergy Solutions		5
5.	Kevin Querry	FirstEnergy Solutions		6
6.	Richard Hoag	FirstEnergy Corp		NA

3.	Group	Jared Shakespeare	Peak Reliability	X									

No Additional Responses.

4.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Larry Nash	Dominion	SERC	1, 3, 5, 6
2.	Mike Garton	Dominion	NPCC	5, 6
3.	Randi Heise	Dominion	MRO	6
4.	Louis Slade	Dominion	RFC	5, 6

5.	Group	Marcus Pelt	Southern Company; Southern Company Services,Inc; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company;	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Southern Company Generation and Energy Marketing										
No Additional Responses													
6.	Group	Colby Bellville	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Lee Schuster	Duke Energy	FRCC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

7.	Group	Dennis Chastain	Tennessee Valley Authority	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	DeWayne Scott		SERC	1
2.	Ian Grant		SERC	3
3.	David Thompson		SERC	5
4.	Marjorie Parsons		SERC	6

8.	Group	Greg Campoli	ISO RTO standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Lori Spence	MISO	MRO	2
2.	Cheryl Moseley	ERCOT	ERCOT	2
3.	Matt Goldberg	ISONE	NPCC	2
4.	Charles Yeung	SPP	SPP	2
5.	Ben Li	IESO	NPCC	2
6.	Tom Bowe	PJM	RFC	2
7.	Ali Miremadi	CAISO	WECC	2

9.	Group	Warren Cross	ACES Standards Collaborators						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Old Dominion Electric Cooperative		SERC	3, 4
2.	Brazos Electric Power Cooperative		ERCOT	1, 5
3.	Golden Spread Electric Cooperative		ERCOT	5
4.	Sunflower Electric Power Corporation		SPP	1

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
5. Great River Energy			MRO	1, 3, 5, 6									
6. Hoosier Energy Rural Electric Cooperative			RFC	1									
10.	Group	Robert Rhodes	SPP Standards Review Group		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Matthew Bordelon	Cleco Power	SPP	1, 3, 5, 6
2.	Chris Carlson	Grand River Dam Authority	SPP	1
3.	Phil Clark	Grand River Dam Authority	SPP	1
4.	Michelle Corley	Cleco Power	SPP	1, 3, 5, 6
5.	Tony Eddleman	Nebraska Public Power District	MRO	1, 3, 5
6.	Louis Guidry	Cleco Power	SPP	1, 3, 5, 6
7.	Robert Hirchak	Cleco Power	SPP	1, 3, 5, 6
8.	Kyle McMenamin	Xcel Energy	SPP	1, 3, 5, 6
9.	Fred Meyer	Empire Electric District	SPP	1, 3, 5
10.	Shannon Mickens	Southwest Power Pool	SPP	2
11.	Pat Morrill	Kansas City Board of Public Utilities	SPP	3
12.	James Nail	City of Independence, MO	SPP	3
13.	Dennis Sauriol	American Electric Power	SERC	1, 3, 5
14.	Don Schmit	Nebraska Public Power District	MRO	1, 3, 5
15.	Angela Summer	Southwestern Power Administration	SPP	1
16.	Tracey Stewart	Southwestern Power Administration	SPP	1
17.	Ellen Watkins	Sunflower Electric Power Corporation	SPP	1

11.	Group	Andrea Jessup	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jeff Millennor	Physical Security	WECC	1
2.	Richard Becker	Substation Engineering	WECC	1

12.	Group	William Harris	Foundation for Resilient Societies								X		
No Additional Responses													
13.	Individual	Dan Inman	Minnkota Power Cooperative	X									
14.	Individual	Oliver Burke	Entergy Services, Inc.	X									
15.	Individual	Peter Scalici	NPCC										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
16.	Individual	Debra R Warner	Self								X		
17.	Individual	Steve Hamburg	Encari	X									
18.	Individual	Chris Scanlon	Exelon	X		X	X	X	X				
19.	Individual	Harold Dalson	Consumers Energy		X	X	X						
20.	Individual	Kevin Weber	Entergy Services, Inc.	X		X							
21.	Individual	Tim Reagan	Ameren	X									
22.	Individual	Gary Pagel	Idaho Power Co.	X									
23.	Individual	Karen Webb	City of Tallahassee - Electric Utility					X					
24.	Individual	David Kiguel	David Kiguel								X		
25.	Individual	Ralph Meyer	The Empire District Electric Company	X		X		X					
26.	Individual	mike kidwell	the empire district electric company					X					
27.	Individual	Kalem Long	The Empire District Electric Company			X							
28.	Individual	Megan Wagner	Westar Energy	X		X	X	X	X				
29.	Individual	Aaron Staley	Orlando Utilities Commission	X		X		X					
30.	Individual	Michelle R D'Antuono	Occidental Energy Ventures Corp.			X		X		X			
31.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
32.	Individual	Shannon Fair	Colorado Springs Utilities	X				X					
33.	Individual	Bill Fowler	City of Tallahassee			X							
34.	Individual	Scott Langston	City of Tallahassee	X									
35.	Individual	Michael Falvo	Independent Electricity System Operator		X								
36.	Individual	Joseph DePoorter	Madison Gas and Electric Company				X						
37.	Individual	Nazra Gladu	Manitoba Hydro	X		X		X	X				
38.	Individual	Thomas Foltz	American Electric Power	X		X		X	X				
39.	Individual	David Ramkalawan	OPG					X					
40.	Individual	Lisa Martin	City of Austin dba Austin Energy	X		X	X	X	X				
41.	Individual	Ayesha Sabouba	Hydro One	X		X							

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
42.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
43.	Individual	Bill Temple	Northeast Utilities	X									
44.	Individual	Amy Casuscelli	Xcel Energy Inc.	X			X	X	X				
45.	Individual	Brian Evans-Mongeon	Utility Services, Inc								X		
46.	Individual	Tony Eddleman	Nebraska Public Power District	X		X		X					
47.	Individual	David Jendras	Ameren	X		X		X	X				
48.	Individual	Alan MacNaughton	New Brunswick Power Corporation	X	X	X		X					
49.	Individual	Sergio Banuelos	Tri-State Generation and Transmission Association, Inc.	X		X		X					
50.	Individual	Bob Steiger	Salt River Project	X		X		X	X				
51.	Individual	Jennifer Flandermeyer	Kansas City Power & Light	X		X		X	X				

If you support the comments submitted by another entity and would like to indicate you agree with their comments, please select "agree" below and enter the entity's name in the comment section (please provide the name of the organization, trade association, group, or committee, rather than the name of the individual submitter).

Organization	Agree	Supporting Comments of "Entity Name"
NPCC	Agree	
Ameren	Agree	Eric ScottAmeren

1. Do you agree with the scope and contents of the SAR? If not, please provide specific comments and suggestions for SDT consideration.

Organization	Yes or No	Question 1 Comment
Tennessee Valley Authority	No	The SDT should consider expanding the applicable entities identified in the SAR. For instance, the type of system risk assessment that FERC suggests in the March 7 order is likely to be conducted by the Transmission Planner / Planning Authority. The Reliability Coordinator might also have information that is pertinent to such a risk assessment from a wide area operations viewpoint. In the event that a generating plant or associated transmission switchyard is identified as a critical facility, the Generator Owner / Generator Operator should be involved in the process of evaluating potential threats and vulnerabilities to those facilities and the development and implementation of the security plan.The following standards should be added to the list of relavent standards to be reviewed by the SDT: CIP-002-3 (R1, R1.2);CIP-002-5.1 (R1 and Attachment 1, Impact Rating Criteria for BES Cyber Systems);FAC-010-2.1 (addresses the Planning Authority(Coordinator) methodology for identifying IROLs);FAC-011-2 (addresses the Reliability Coordinator methodology for identifying IROLs;FAC-014-2 (R5.1.1, use of “critical” in reference to Facility(ies) used to derive an IROL);IRO-002-2 (R5, use of “critical” in reference to BES elements);IRO-003-2 (R2, use of “critical facilities”);IRO-008-1 / IRO-009-1 / IRO-010-1a / TOP-001-2 / TOP-004-2 (the purpose statement for these standards includes “to prevent instability, uncontrolled separation, or cascading outages”, which is language used in the FERC order for identifying critical facilities);TPL-001-4 (R6, addresses the criteria or methodology used by the TP and PC to identify System instability)The SDT should also consider the definition of Interconnection Reliability Operating Limit (IROL) in

Organization	Yes or No	Question 1 Comment
		development of the physical security standard. This definition includes language used in the FERC order to describe a "critical facility".
SPP Standards Review Group	No	The FERC order references facilities which we assume are then tied to the existing definition of Critical Assets as defined in the Glossary of Terms. This definition is scheduled to be retired on March 31, 2016. How does one then determine the list of 'critical' facilities if that definition no longer exists? The distinction between critical facility and critical asset needs to be figured out. Also, FERC's interpretation of 'facility' isn't consistent with the NERC definition of Facility since FERC implies a control center is a facility in Footnote 6 on Page 3 of the order. We need to come to some resolution of terms in order to determine where the playing field lies.The SAR refers only to TOs and TOPs with no reference to GOs and GOPs who also own and operate facilities on the BES. Why were they left out? Also, BAs and RCs are not listed as applicable entities. Shouldn't they be included also? Will FERC accept a standard without these entities being included?While the SAR refers to the entire order being incorporated into the SAR we suggest that the SDT specifically list each of the directives in bullet fashion in the SAR such that the stakeholders can be assured that they have all been included and will then be addressed by the SDT.
Bonneville Power Administration	No	BPA believes that generally, this type of standard would be useful to the electric industry. The biggest issue for the SAR is the scope is loosely defined. As described, the objective of protecting critical facilities of the BES is stated too broadly and it is not apparent what countermeasures would be considered adequate or sufficient. ..."Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities." BPA believes that there are also many questions and issues to resolve to get to an acceptable level of risk that is lower than what may be in place today, and the 90 day drafting

Organization	Yes or No	Question 1 Comment
		period may not be long enough to define adequate expectations. A phased development approach may be more conducive to obtaining the benefits desired - - for example, assessment and ranking standard(s) first followed by mitigation options and requirements standard(s) to address gaps identified by the assessment.
Foundation for Resilient Societies	No	SAR Only includes Transmission Owners and Operators. This does not include all critical facilities.
Self	No	After reviewing the SAR, where in the Reliability and Market Interface Principles the box 5 for facilities for communication monitoring and control are referenced, I believe that the Reliability Coordinator Function should have been checked also. Is this an oversight in the draft SAR?
Consumers Energy	No	The information contained in the attached PDF files seems very vague and open ended. I would specifically point ot page 2, under the Industry Need section 2nd paragraph, line 3:"will require certain registered entities" I believe the term certain should be changed to a term of greater focus such as "entities that meet a predetermined set of criteria used to determine local, regional, and national criticality."2nd paragraph, line 8:"may compromise", again I think there needs to be some "degree" of compromise contained in this section. Example a chunk of stolen copper, to some degree can compromise a system, just as a VBIED can compromise a system. In areas where a "compromise" could cause a consequence at a local level, and the primary identified risk is trespass and copper theft this SAR as written suggests we 'Mitigate" the risk of compromise, not the cause of compromise coupled with the identified consequence of the compromise. An owner should have the ability to identify the risk, the consequence, and the mitigations to "prevent" that type of compromise in areas or sections of the system that would impact local, and perhaps to some degree regional consequences. If in fact an owner has assets that

Organization	Yes or No	Question 1 Comment
		could, if compromised cause cascading events that impact areas outside of their system operational area, those assets would show a greater consequence area and would require a greater level of protection.
City of Tallahassee - Electric Utility	No	TAL has concerns with the expedited nature of the timeline. The issue of physical security has been known for quite some time. The timeline of this directive appears to be solely in reaction to the publishing of the Metcalf incident. This directive and expedited time line precludes the dialog from occurring that needs to take place to truly understand what is expected to satisfy the Commission's desires. TAL believes this directive will yield a standard that is difficult to enforce with little benefit to the large majority of the BES. Additionally, the publicizing of certain "known" studies indicating that as little as nine substations will cause a large blackout is problematic.
David Kiguel	No	1. The SAR should include other entities in the applicability section such as Generator Owners (GO) and Generator Operators (GOP). The FERC Directive indicates that the proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of theBulk-Power System. It is clear that GOs and GOPs also own and operate Bulk-Power System facilities. 2. The FERC Directive requires that a risk assessment of the systems to identify their "critical facilities" be performed. In many cases, the entity that would be in the best position to perform such assessment would be the RC or the PC. It is suggested one of these be added in the SAR so the SDT can assign this responsibility to one of these functional entities. 3. The FERC Directive contains a requirement that NERC includes in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential informationbut still allow for the Commission, NERC and the Regional Entities to review and inspect any information that is needed to ensure compliance with the Reliability

Organization	Yes or No	Question 1 Comment
		Standards. Review and inspect such information on the part of the Commission should be limited to entities that are under FERC's jurisdiction. Canadian and/or Mexican data should be provided to regulators in the respective jurisdiction only, unless aggregated in a manner that will not allow to identify individual entities.
The Empire District Electric Company	No	The FERC order references facilities which we assume are then tied to the existing definition of Critical Assets as defined in the Glossary of Terms. This definition is scheduled to be retired on March 31, 2016. How does one then determine the list of 'critical' facilities if that definition no longer exists? The distinction between critical facility and critical asset needs to be addressed so that the expectation of a critical facility is clear to entities. Also, FERC's interpretation of 'facility' isn't consistent with the NERC definition of Facility since FERC implies a control center is a facility in Footnote 6 on Page 3 of the order. There needs to be some resolution of terms in order to determine where FERC's concern is focused so that a proper solution can be devloped.The SAR refers only to TOs and TOPs with no reference to GOs and GOPs who also own and operate facilities on the BES. These may be considered? Also, BAs and RCs are not listed as applicable entities-shouldn't they be included also as they have the overall ability to direct and control the BES? Will FERC accept a standard without these entities being included?While the SAR refers to the entire order being incorporated into the SAR we suggest that the SDT specifically list each of the directives in bullet fashion in the SAR such that the stakeholders can be assured that they have all been included and will then be addressed by the SDT.
the empire district electric company	No	The FERC order references facilities which we assume are then tied to the existing definition of Critical Assets as defined in the Glossary of Terms. This definition is scheduled to be retired on March 31, 2016. How does one then determine the list of 'critical' facilities if that definition no longer exists? The distinction between critical facility and critical asset needs to be figured out.

Organization	Yes or No	Question 1 Comment
		Also, FERC's interpretation of 'facility' isn't consistent with the NERC definition of Facility since FERC implies a control center is a facility in Footnote 6 on Page 3 of the order. We need to come to some resolution of terms in order to determine where the playing field lies.The SAR refers only to TOs and TOPs with no reference to GOs and GOPs who also own and operate facilities on the BES. Why were they left out? Also, BAs and RCs are not listed as applicable entities. Shouldn't they be included also? Will FERC accept a standard without these entities being included?While the SAR refers to the entire order being incorporated into the SAR we suggest that the SDT specifically list each of the directives in bullet fashion in the SAR such that the stakeholders can be assured that they have all been included and will then be addressed by the SDT.
The Empire District Electric Company	No	The FERC order references facilities which we assume are then tied to the existing definition of Critical Assets as defined in the Glossary of Terms. This definition is scheduled to be retired on March 31, 2016. How does one then determine the list of 'critical' facilities if that definition no longer exists? The distinction between critical facility and critical asset needs to be figured out. Also, FERC's interpretation of 'facility' isn't consistent with the NERC definition of Facility since FERC implies a control center is a facility in Footnote 6 on Page 3 of the order. We need to come to some resolution of terms in order to determine where the playing field lies.The SAR refers only to TOs and TOPs with no reference to GOs and GOPs who also own and operate facilities on the BES. Why were they left out? Also, BAs and RCs are not listed as applicable entities. Shouldn't they be included also? Will FERC accept a standard without these entities being included?While the SAR refers to the entire order being incorporated into the SAR we suggest that the SDT specifically list each of the directives in bullet fashion in the SAR such that the stakeholders can be assured that they have all been included and will then be addressed by the SDT.

Organization	Yes or No	Question 1 Comment
Westar Energy	No	The SAR refers only to TOs and TOPs with no reference to other registered functions. Should the applicability be expanded to include all registered functions who own and operate facilities on the BES and would be involved in the assessment process?
Colorado Springs Utilities	No	The SAR refers to the entire order being incorporated into the SAR we suggest that the SDT specifically list each of the directives in bullet fashion in the SAR such that the stakeholders can be assured that they have all been included and will then be addressed by the SDT. We would recommend Brightline Criteria For the identification of critical Bulk Electric System Facilities, based on either the Transmission Planning Standard TPL-004a or identification of the largest single contingency for each interconnection. If we need a single number, including only Facilities that provide or control over 3000 MW of generation or transmission or transmission operating at 300 kV and above. Case-specific analysis and consideration of exceptions will be needed, but we need to start with a high lower limit.
City of Tallahassee	No	TAL has concerns with the expedited nature of the timeline. The issue of physical security has been known for quite some time. The timeline of this directive appears to be solely in reaction to the publishing of the Metcalf incident. This directive and expedited time line precludes the dialog from occurring that needs to take place to truly understand what is expected to satisfy the Commission's desires. TAL believes this directive will yield a standard that is difficult to enforce with little benefit to the large majority of the BES. Additionally, the publicizing of certain "known" studies indicating that as little as nine substations will cause a large blackout is problematic.

Organization	Yes or No	Question 1 Comment
City of Tallahassee	No	TAL has concerns with the expedited nature of the timeline. The issue of physical security has been known for quite some time. The timeline of this directive appears to be solely in reaction to the publishing of the Metcalf incident. This directive and expedited timeline precludes the dialog from occurring that needs to take place to truly understand what is expected to satisfy the Commission's desires. TAL believes this directive will yield a standard that is difficult to enforce with little benefit to the large majority of the BES. Additionally, the publicizing of certain "known" studies indicating that as little as nine substations will cause a large blackout is problematic.
Independent Electricity System Operator	No	We generally agree with the purpose and scope of the SAR, but we disagree with the applicability.The purpose of this project is develop a standard that will require owners and/or operators of the Bulkâ€Power System, as appropriate, to identify facilities on the Bulkâ€Power System that are critical to the reliable operation of the Bulkâ€Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. We interpret the "identify facilities" part in the first sentence to mean assessing the reliability impacts of the facilities which, if deemed inoperable, can result in instability, uncontrolled separation or cascading failures on the Bulk-Power System. Such tasks will thus require power system analysis not unlike the type required for transmission planning assessment, with a focus on losing the all the facilities at a location (e.g. a transmission substation, a large power plant, a right of way, etc.). These tasks will likely involve the Planning Coordinator and/or the Reliability Coordinator.This interpretation is also inferred from Para. 6 and Footnote #6 of the Order. Below is an excerpt of Para. 6 and FN#6:6. First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their

Organization	Yes or No	Question 1 Comment
		systems to identify their “critical facilities.” A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards. (FN#6) Instead, the Commission is directing NERC to develop Reliability Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System.FN#6 says: However, the Commission expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers.Two key points:a. FN#6 clearly indicates that it is the Commission’s expectation that control centres are critical facilities. The most critical control centres are those of the RCs. Hence, the RC’s inclusion in the standard appears to be very likely.b. Para 6 suggests that critical facilities are necessary those that if rendered not operable, they have wide-area reliability impact associated with instability, uncontrolled separation or cascading failures. We fully expect the standard to require responsible entities to have a process and criteria in place with which to identify the critical facilities from a wide-area reliability impact point of view. Such tasks will involve reliability assessments that are normally performed by the Planning Coordinator and Reliability Coordinator, depending on the time frame. In the Applicability Section, however, neither the PC’s nor the RC’s box is checked. We suggest the SAR be revised to include at least these two entities as potential applicable entities so that the drafting team does not foreclose the possibility that reliability assessments need to be conducted to aid the identification of critical facilities. Further, we believe Generator

Organization	Yes or No	Question 1 Comment
		Owners and Generator Operators may also be involved since critical facilities may not be just limited to transmission facilities of control centres. Large power plants, if deemed inoperable, can also result in wide-area reliability concerns. We suggest the SAR be revised to include these two entities as potential applicable entities.
American Electric Power	No	Please see comments provided in response to Question 4.
Hydro One	No	The SAR does not ask the SDT to identify timelines by which the third-party verification, following the completion of the risk assessment, would be required. The FERC Order also does not specify timelines for how soon the third-party verification must be completed after the completion of the risk assessment. The scope of the standard should be limited to protection against physical attacks.Identifying which physical facilities are critical facilities should be determined through a BPS assessment of risk and the methodology by which this assessment is conducted should be identified in the standard. The assessment of risk or vulnerabilities should consider other standards including CIP and the new GMD Stage 2 project which will be a new TPL standard.
American Transmission Company, LLC	No	Currently, only Transmission Owners (TOs) and Transmission Operators (TOPs) are applicable Reliability Functions checked on the SAR on page 4. ATC believes those having experience in performing risk assessments and identifying critical facilities should also be included, which would be Planning Coordinators(PCs), Reliability Coordinators(RCs), and Transmission Planners(TPs). (and checked as applicable in the SAR for Reliability Functions on pp. 3 and 4) The basis for making PCs, RCs, and TPs applicable to the SAR and new Standard is also implied by one of the FERC Directives below addressing the need for a risk assessment: The following is an excerpt from the FERC Order:..... the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk

Organization	Yes or No	Question 1 Comment
		assessment of their systems to identify their "critical facilities." A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System.5 Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards.6 Instead, the Commission is directing NERC to develop Reliability Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System and thereby warrant the directive imposed here.In addition, ATC believes that Generator Owners (GOs) and Generator Operators (GOPs) should be added to the Reliability Functions of the SAR. The FERC Order states that "The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities." To address owners and operators of generation facilities that are part of the Bulk-Power System, GOs and GOPs should be included in the Reliability Functions of the SAR. With the above justification, ATC is recommending that the GOs, GOPs, PCs, RCs and TPs be checked on the SAR as applicable Reliability Functions.
Utility Services, Inc	No	The SAR attempts to address the Commission's directive by requiring only Transmission Owners and Transmission Operators to protect certain types

Organization	Yes or No	Question 1 Comment
		of facilities , however this may not fully address the directives. The Commission is seeking to physically protect BPS facilities that will impact to the reliable operation of the BPS. Generation is recognized to be a part of maintaining the reliability and resiliency of the BPS. Based on several factors, including but not limited to location and operating profile, a significant generation facility could have a huge effect on the reliable operation of the BPS. The SAR should, at a minimum, examine whether generating stations consisting of 3000 MW or more need to be included in the applicability of this project. This matches up to the treatment of the other types of assets being contemplated herein.
Nebraska Public Power District	No	If a list of the most critical substations exists, why are we trying to develop a new process to determine the list without first getting to see the list? The draft standard is due to FERC within 90 days, but we are being asked to develop a process to match their list, when we don't even know what is on the list. Shouldn't Congress get involved and pass a law within 90 days to require the military to protect the substations? No, just as we shouldn't have to draft a new standard within 90 days. Our NERC standard development process, similar to the process Congress uses to pass new federal requirements is intentionally designed with checks and balances, plus adequate time for review to prevent knee-jerk reactions to events. We need to spend time to get this right and not rush something through.This expedited standard development has the potential to derail our entire NERC standard development process. I feel like we have been blind folded and put into a room and told to hit a small target with a dart and we don't even know which wall or direction to throw the dart. We work in a very complex industry with very talented staff across North America. FERC's staff is more appropriately aligned toward oversight, without the technical expertise to understand the full impact of implementation of new rules and regulations. Why are we jeopardizing our entire process for this standard? Is there an imminent threat? If so, our leaders should find a more

Organization	Yes or No	Question 1 Comment
		appropriate path for a solution (i.e., deploy our military). We already have multiple NERC requirements to identify and designate our facilities as critical. Introducing a new requirement to identify critical facilities will create confusion and unintended consequences. The CIP standards have been through several iterations of identifying critical facilities and continue to evolve. This has been a moving target, so why introduce yet another process to determine critical facilities. Our planning standards require us to study our systems and methodically improve the infrastructure to prevent cascading outages. Do those planning standards need to be modified to consider physical attacks? Would that be a more appropriate path to a solution for this issue?
Ameren	No	1) The related standards section of the SAR should include CIP-002-5 so that the criteria to determine which facilities are critical as a preliminary list for the new physical security standard will not conflict with the bright-line criteria in CIP-002-5.
Tri-State Generation and Transmission Association, Inc.	No	TSGT does not agree that Transmission Operators should be included in the Reliability Functions. The March 7, 2014 FERC Order, paragraph 1, states "...owners or operators of the Bulk-Power System, as appropriate...". Transmission Owners have the legal and/or contractual ability to dictate how physical environments within a facility are addressed. There is nothing within the TOP function that formally allows the entity to dictate or ensure that any physical security concerns are met under this standard, unless otherwise dictated by contracts and/or agreements. If Transmission Operators are kept as a Reliability Function under this standard, the standard should clearly define which TOPS versus TOs should be included to ensure the "appropriate" entity is included and that the same facilities are not repeatedly reported by multiple entities.

Organization	Yes or No	Question 1 Comment
Salt River Project	No	The SAR, under the section "Related Standards" lists only CIP-006-5, CIP-008-5 and CIP-009-5. It should also consider additional related standards CIP-002-5, CIP-002-3, CIP-006-3, CIP-008-3, CIP-009-3, EOP-004-1, and the TPL family of standards. The SAR should work both to avoid inconsistencies between any new standard and the existing standards and also avoid redundancies as well.
Kansas City Power & Light	No	The FERC order references facilities and it is assumed this is linked to the existing definition of Critical Assets as defined in the Glossary of Terms. This definition is scheduled to be retired on March 31, 2016. There are many references to critical in the standards. Clarity as well as consistency is needed in the definition of critical and expressly for what purpose (reliability, security, relisiency, etc.). If the definition of critical facilities will be retired, common understanding of this term should be defined somewhere for consistent language between ERO staff and registered entities. The distinction between critical facility and critical asset should also be defined. Also, FERC's interpretation of facility is inconsistent with the NERC definition of Facility as FERC implies a control center is a facility in Footnote 6 on Page 3 of the order. Before this would become mandatory and enforceable, resolution of definition of terms is required to ensure consistency in application.The SAR reference determines applicability only to the TO and TOP functions. Whether based on the registry criteria or functional model activities, the determination of critical can be impacted or influenced by Transmission Planners, Generator Owners and Generator Operators who also model, plan, own and operate facilities on the BES. Applicability should be considered for Balancing Authorities, Planning Coordinators, and Reliability Coordinators depending on criticality for the purpose of reliability, security and resiliency. While the SAR refers to the entire order being incorporated into the SAR, KCP&L recommends that the SDT specifically list each of the directives in the SAR such that the

Organization	Yes or No	Question 1 Comment
		stakeholders can be assured that they have all been included and will then be addressed by the SDT.
Northeast Power Coordinting Council	Yes	Agree generally with the scope. Care must be taken that the requirements developed are consistent with the applicable reliability functions as noted in the SAR. The scope of the standard should be limited to protection against physical attacks. The determination of which physical facilities to protect (identified to be "critical") should come through a BPS assessment of risk that will need to be defined in the Standard, and depending on how that is done, might involve other types of registered entities or work done under other standards (e.g., CIP or even the GMD Stage 2 effort in which a new TPL Standard is under development, for similar reasons of determining what system risks to address).Regarding the Applicability, the purpose of this project is develop a standard that will require owners and/or operators of the Bulk Power System, as appropriate, to identify facilities on the Bulk Power System that are critical to the reliable operation of the Bulk Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. Such tasks might require power system impact analyses not unlike the type required for system impact assessments, with a focus on losing all the facilities at a location (e.g. a transmission substation, a large power plant, a right of way, etc.). We do not disagree with the applicable entities as specified in the proposed SAR, but are looking for clarification on how the assessments are obtained, and whether other functional entities might be asked for input from owners/operators. Put another way, depending on the types of impacts the Standard will seek to protect against, entities within the entire Interconnection, or maybe even specific regions within the Interconnection, might need to be included in the Standard. Can NERC or the SDT provide guidance on whether the loss of generating facilities might have interconnection or area wide impacts that the Standard needs to

Organization	Yes or No	Question 1 Comment
		protect against happening?To avoid compromising operations as stated in the SAR, we believe that consideration should be given to entities focusing more on the resiliency and the redundancy of the network rather than on additional physical security measures. Attacks may not be able to be prevented, but the consequences of an attack can be mitigated. This is the type of assessment that is best performed using the techniques in the TPL standards.Furthermore, according to the SAR, the SDT is to develop a standard that addresses risk factors, levels of acceptable security and the implementation of a protection plan. We believe that these elements can not be standardized as threat assessments are not the same from one entity to another. Consequently, the acceptable levels of safety cannot be identical. All of these factors lead us to believe that the development of fixed criteria regarding levels of acceptable risk and security cannot be identical from one entity to another. The SDT also has to consider and address the standard with respect to Canadian differences.
Duke Energy	Yes	(1)Duke Energy agrees with the scope and contents of the SAR.
ISO RTO standards Review Committee	Yes	We generally agree with the purpose and scope of the SAR, but we ask for clarification on how the SAR will address certain aspects of the FERC Order. Based upon the FERC Order for Physical Security Standards, we understand the task for NERC and the industry is to develop a standard that will require owners and/or operators of the Bulkâ€Power System, as appropriate, to identify facilities on the Bulkâ€Power System that are critical to the reliable operation of the Bulkâ€Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. Such tasks may require power system analysis not unlike the type required for transmission planning assessment, with a focus on loss of all the facilities at a physical location (e.g. a transmission substation, a large power plant, a right of way, etc.). We

Organization	Yes or No	Question 1 Comment
		do not disagree with the applicable entities as denoted in the proposed SAR snd are not seeking to expand the SAR to apply to Planning Authority (PA) and Reliability Coordinator (RC). However, we ask for clarification of how the assessments are obtained. Depending on the nature of the type of risk assessment developed under this Standard, certain tasks may need to involve the PA and/or the RC. Moreover, while the identification of "critical facilities" might not be the same as what may be identified under CIP-002-5 effective April 1, 2016 for High and Medium impact systems), CIP-002-5 (or PRC-023) might provide a model to use for RC/PA providing information to asset owners. We ask if these requirements can and will be relied upon.
ACES Standards Collaborators	Yes	ACES supports Project 2014-04 Physical Security SAR and NERC's efforts to protect the BES from either a cyber or physical security attack. NERC guidance should be developed to provide industry with examples of acceptable protections against various threat vectors and what level of resiliency should be in place. We support the drafting team in its development of a consistent and effective physical security standard for impacted registered entities across the regions. We also caution the drafting team to consider and minimize unintended consequences of these standards. For example, if the standards require visual impairments to prevent a Metcalf style attack could such visual impairments become projectiles during a storm. If so, would such visual impairments improve reliability in areas prone to many storms and tornadoes?
Exelon	Yes	Yes, Exelon agrees the primary goal is to develop a standard with clear unambiguous requirements that address the FERC directives.
Occidental Energy Ventures Corp.	Yes	Occidental Energy Ventures Corp. ("OEVC") agrees that the SAR properly captures the language and intent of FERC's order to address physical attacks on the BES. In addition, it is appropriate to limit the scope to high priority transmission assets - which we believe pose the most difficult

Organization	Yes or No	Question 1 Comment
		logistical challenges based upon their sheer number and wide geographic distribution.Having said that, there is a concern that the 90 day turn around interval mandated by the Commission could introduce flaws that would normally be caught in the vetting process. We realize that FERC has the legal authority to compel an expedited time frame, but would prefer that the SAR clearly indicate a commitment to risk-based principles that will allow flexibility to the industry and CEA community alike. For example, it may be appropriate at this time to require entities to develop strategies that engage law enforcement and the FBI when a threat appears - whereas a requirement to fortify substations and/or control rooms would not be. As the industry gains experience with protective techniques through exercises and actual experience, the best-in-class strategies can be encoded in a standard - but not before.
Madison Gas and Electric Company	Yes	The SAR seems to directly reflect the FERC Order but to assure system reliability and perform adequate studies the PC and TP may need to be added to the applicability section, since they have the ability to perform reliability studies. Plus studies could be used within the TPL Standards.
OPG	Yes	The reliability functions identified in the SAR are TO (Transmission Owner) and TOP (Transmission Operator). GO (Generator Owner) and GOP (Generator Operator) are not identified and this makes good sense. BPS impacted equipment that may be owned by a GO is contained within a plant environment and are already protected by existing Physical Security Measures in place to protect the plant.
City of Austin dba Austin Energy	Yes	City of Austin dba Austin Energy (AE) agrees with the scope and contents of the SAR; however, we think it is appropriate to include #7 in the list of Applicable Reliability Principles. #7 states “The security of the

Organization	Yes or No	Question 1 Comment
		interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis."
Northeast Utilities	Yes	NU agrees with scope and applicability. NU urges the SDT to take care that the requirements developed are consistent with the applicable reliability functions (TO & TOP) as noted in the SAR.
FirstEnergy Corp.	Yes	
Peak Reliability	Yes	
Dominion	Yes	
Southern Company; Southern Company Services,Inc; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	Yes	
Minnkota Power Cooperative	Yes	
Entergy Services, Inc.	Yes	
Encari	Yes	
Entergy Services, Inc.	Yes	
Idaho Power Co.	Yes	
Orlando Utilities Commission	Yes	

Organization	Yes or No	Question 1 Comment
LCRA Transmission Services Corporation	Yes	
Manitoba Hydro	Yes	

2. **Are you aware of any regional variances associated with approved NERC Reliability Standards that will be needed as a result of this project? If yes, please identify the Regional Variance**

Organization	Yes or No	Question 2 Comment
FirstEnergy Corp.	No	
Peak Reliability	No	
Dominion	No	
Southern Company; Southern Company Services,Inc; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	No	
Duke Energy	No	
Tennessee Valley Authority	No	
ISO RTO standards Review Committee	No	
ACES Standards Collaborators	No	
Bonneville Power Administration	No	

Organization	Yes or No	Question 2 Comment
Foundation for Resilient Societies	No	
Minnkota Power Cooperative	No	
Entergy Services, Inc.	No	
Self	No	
Encari	No	
Exelon	No	
Consumers Energy	No	
Entergy Services, Inc.	No	
Idaho Power Co.	No	
City of Tallahassee - Electric Utility	No	
Westar Energy	No	
Orlando Utilities Commission	No	
Occidental Energy Ventures Corp.	No	
LCRA Transmission Services Corporation	No	

Organization	Yes or No	Question 2 Comment
Colorado Springs Utilities	No	
City of Tallahassee	No	
City of Tallahassee	No	
Madison Gas and Electric Company	No	
Manitoba Hydro	No	
American Electric Power	No	American Electric Power is not currently aware of any regional variances associated with approved NERC Reliability Standards that will be needed as a result of this project.
OPG	No	
City of Austin dba Austin Energy	No	
Hydro One	No	
American Transmission Company, LLC	No	
Northeast Utilities	No	
Xcel Energy Inc.	No	
Utility Services, Inc	No	

Organization	Yes or No	Question 2 Comment
Ameren	No	
Tri-State Generation and Transmission Association, Inc.	No	
Salt River Project	No	
Northeast Power Coordinting Council	Yes	There are regional differences in Quebec. The SDT should not establish predefined criteria for risk assessment since it cannot be the same for different entities. Each entity should have its basis of a threat and security level defined accordingly.
SPP Standards Review Group	Yes	Regional variances may need to be incorporated into the standards simply due to geographical differences across the regions which will need to be factored into the standards themselves. It may be necessary to give special consideration to specific situations.
The Empire District Electric Company	Yes	Regional variances may need to be incorporated into the standards simply due to geographical differences across the regions which will need to be factored into the standards themselves. It may be necessary to give special consideration to specific situations.
the empire district electric company	Yes	Regional variances may need to be incorporated into the standards simply due to geographical differences across the regions which will need to be factored into the standards themselves. It may be necessary to give special consideration to specific situations.
The Empire District Electric Company	Yes	Regional variances may need to be incorporated into the standards simply due to geographical differences across the regions which will need to be factored into the standards themselves. It may be necessary to give special consideration to specific situations.

Organization	Yes or No	Question 2 Comment
Kansas City Power & Light	Yes	Regional variances may need to be incorporated into the standards simply due to geographical differences across the regions which will need to be factored into the standards themselves - topography, climate, vegetation,etc.

3. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standard(s)? If yes, please identify the jurisdiction and specific regulatory requirements.

Organization	Yes or No	Question 3 Comment
ISO RTO standards Review Committee	No	At this time, we are not aware of any jurisdictional issues that need to be considered by the drafting team and addressed in the standard. In addition, if the standard should involve protection of nuclear power plants, then there are differences in nuclear power plant regulations between the USA and Canada that may require recognition by the proposed standard.
American Electric Power	No	American Electric Power is not currently aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standard.
Dominion	No	
Southern Company; Southern Company Services,Inc; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	No	
Tennessee Valley Authority	No	
ACES Standards Collaborators	No	

Organization	Yes or No	Question 3 Comment
Bonneville Power Administration	No	
Foundation for Resilient Societies	No	
Minnkota Power Cooperative	No	
Entergy Services, Inc.	No	
Self	No	
Encari	No	
Exelon	No	
Consumers Energy	No	
Entergy Services, Inc.	No	
Idaho Power Co.	No	
City of Tallahassee - Electric Utility	No	
The Empire District Electric Company	No	
the empire district electric company	No	

Organization	Yes or No	Question 3 Comment
The Empire District Electric Company	No	
Orlando Utilities Commission	No	
Occidental Energy Ventures Corp.	No	
LCRA Transmission Services Corporation	No	
Colorado Springs Utilities	No	
City of Tallahassee	No	
City of Tallahassee	No	
Madison Gas and Electric Company	No	
Manitoba Hydro	No	
OPG	No	
City of Austin dba Austin Energy	No	
American Transmission Company, LLC	No	
Northeast Utilities	No	

Organization	Yes or No	Question 3 Comment
Xcel Energy Inc.	No	
Utility Services, Inc	No	
Ameren	No	
Tri-State Generation and Transmission Association, Inc.	No	
Salt River Project	No	
Kansas City Power & Light	No	
Northeast Power Coordinting Council	Yes	At this time, it is uncertain whether or not there are any jurisdictional issues that need to be considered by the Standard Drafting Team and addressed in the standard. It depends on the proposed requirements as they relate to detection, protection and reporting of potential physical risks to safeguard physical security. In addition, if the standard should involve protection of nuclear power plants, then there are differences in nuclear power plant regulations between the United States and Canada that may require recognition by the proposed standard.
Duke Energy	Yes	(1)The SDT should ensure that facilities regulated by the Nuclear Regulatory Commission or Canadian Nuclear Safety Commission are considered for exemption in the drafting of a Physical Security standard.
David Kiguel	Yes	Please see my comment with respect to confidential information above (Question 1).
Hydro One	Yes	As well, there may be provincial regulations in Ontario that require government-owned entities such as utilities to follow procurement rules and if the new standard included timelines by which assessments must be verified by third-party, these utilities may not be able to go through procurement processes for normal work (i.e.

Organization	Yes or No	Question 3 Comment
		not emergency or restoration work) quickly enough if the timelines are insufficient. (I am looking into this to confirm).

4. Are there any other concerns with this SAR?

Organization	Yes or No	Question 4 Comment
FirstEnergy Corp.	No	
Peak Reliability	No	
Dominion	No	
Southern Company; Southern Company Services,Inc; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	No	
Self	No	
Exelon	No	
Consumers Energy	No	
Entergy Services, Inc.	No	
City of Tallahassee - Electric Utility	No	
Orlando Utilities Commission	No	

Organization	Yes or No	Question 4 Comment
LCRA Transmission Services Corporation	No	
City of Tallahassee	No	
OPG	No	
City of Austin dba Austin Energy	No	
Northeast Power Coordinting Council	Yes	The Standard Drafting Team is urged to not be too prescriptive in the development of these requirements. Operators should be able to conduct a vulnerability assessment and implement any mitigation actions that were deemed appropriate by the entity. The Standard Drafting team should carefully consider the cost impact that the standard will have on entities to implement and therefore limit the site selection.Minimum vulnerabilities should be defined to be included in vulnerability assessments.Critical facilities determination are recommended to be carried out via a TPL standard based assessment.Timing should be provided for the effective date of standard versus the time required to conduct assessments and implement the mitigation actions identified.It has to be considered that electrical analysis and physical analysis are related, but are not one in the same. For example, using an electrical criteria, e.g., >3,000MVA, does not take into account that multiple voltages can reside on a single site, within a single footprint and fence. “Substations” is not a stand alone term. The SAR needs to recognize that there is not a total correlation between Cyber Security (CIPâ€002â€5.1) and Physical Security (CIPâ€014â€1). They are related, but different, and may need to use identical and as well as some different criteria. The current proposal for CIPâ€014 is to use the same criteria as those specifying a Medium Asset in CIPâ€002â€5.1. This may represent an over simplification. Physical Security is different. You do not need access in order to violate physical security. A TPL standards based assessment is a better approach.The SDT

Organization	Yes or No	Question 4 Comment
		must ensure that the scope of this standard and applicability of facilities subject to the standard is consistent with existing CIP standards.Furthermore, consider the impact of this standard on the existing standard EOP-004-2 and ensure the coordination with the EOP-004-2 standard.We believe that the SDT should consider network redundancy in the case of an attack, the potential consequences associated with a physical attack and threats specific to each entity before imposing a standard level of acceptance for all.The SDT should define how the verification of the risk assessment used by the owner or operator of critical facilities will be completed. The standard should identify the methodology by which critical facilities were identified. Once the methodology is determined, then the SAR should also define the methodology for doing this verification. The definition of the methodology for review should be applied to the review of all three of the identification of critical facilities, determination of threats and vulnerabilities, and mitigation plans, and that the standard should clarify whether the mitigation plans also have to be reviewed by a third party.The SDT should ensure that the new standard does not call for requirements that will impact or impede the normal operational capacity, access for maintenance or restoration, or the safety of people or equipment.The standard should clearly define the timelines for conducting assessments and implementing the mitigation actions identified with respect to when the standard becomes effective. Timelines for assessment of risk or vulnerabilities in this new standard should coincide with the timelines for which assessment of risk or vulnerabilities for other standards including the CIP and the new GMD Stage 2 project which will be a new TPL standard.
Duke Energy	Yes	(1)Duke Energy would like to reiterate to the SDT that any set of physical security standards need to provide the specific deliverables and that the requirements developed are clear and concise. We ask that the SDT proceed with caution and focus its attention on all potential physical threats and vulnerabilities to transmission substations, and not solely focus its attention on the recent activities in California and elsewhere. Also, stakeholders should have the flexibility to implement a staged level approach of security measures that are appropriate for the criticality of the facility

Organization	Yes or No	Question 4 Comment
		and the assessment of the vulnerabilities at a facility.(2)In addition to the CIP standards identified in the SAR for review of consistency in language and terminology, Duke Energy recommends the SDT review CIP-002-5 and EOP-004-2 as well.
Tennessee Valley Authority	Yes	While not stated in the SAR, it appears the SDT is preparing to develop an initial draft physical security standard as CIP-014-1 based on the ballot pool title. We agree that physical security of critical power system facilities can be considered a critical infrastructure protection issue; however we are concerned that development and implementation of a physical security standard (as outlined in the FERC order) under the CIP family of standards during the transition period from CIP version 3 to CIP version 5 will create an unnecessary distraction from the ongoing industry efforts to protect Cyber Assets under a changing regulatory framework. We respectfully request the SDT to consider developing the physical security standard for critical facilities (as outlined in the FERC order) under the FAC standards group to maintain a distinction from the CIP version 5 standards that are more focused on BES Cyber Assets and the associated protection of those Cyber Assets.
ISO RTO standards Review Committee	Yes	The IRC SRC is committed to working under this extremely expedited standards process timeline to provide our resources and technical expertise to help develop a standard that satisfies the FERC directive and above all, is effective and adds value to the numerous in effect reliability standards and practices that are designed to protect the Bulk-Power System from instability, uncontrolled separation and cascading failures. We do ask the standards drafting team to be aware that many facility owners already have physical protections in place for facilities they have determined to be critical. A NERC standard for physical security needs to be flexible so that it not only increases protections where they may be deficient - but also does not hinder or disincents the continued use of any protections already in place which have been effective.

Organization	Yes or No	Question 4 Comment
ACES Standards Collaborators	Yes	(1) FERC has stated in their order that they want grid owners and operators to "consider resilience of the grid" when identifying critical facilities. We recommend that the drafting team provide additional guidance to what level of resilience is needed, how will this be measured for each type of facility, and the level of resilience based upon risk to the BES. (2) FERC is requiring that an applicable entity must have "NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity" review the process for identifying a critical facility. Given that only a TO and TOP have been identified as potential applicable functions, we question if this directive has been considered appropriately in the SAR.(3) Given that third parties may evaluate critical facility information, further guidance is needed and controls are required to address this highly sensitive level information. Is this information subject to the Freedom of Information Act? This will need to be clear as to how information, data, and protection plans are to be reviewed, secured and monitored.Thank you for your time and consideration.
SPP Standards Review Group	Yes	The 90-day response requested by FERC is well short of the normal standard development time at NERC. This process is an established, ANSI accredited and transparent process which is intended to consider all technical considerations and to establish a broad stakeholder consensus. To drastically reduce the process to a 90-day turnaround will present a challenge to developing a broad industry consensus and achieving the best technical solution.If the apparent driver behind this effort, the Metcalf event referenced in the WSJ article, truly raises a credible threat to the reliability of the Bulk Electric System(BES), it should be addressed logically in a well, thought-out process to reach the right conclusion and not be done in haste. The credibility of the analysis referred to in the WSJ article, pointing to a limited set of substations in North America causing a widespread outage, must be vetted by industry experts to first determine if there is a reliability gap in existing NERC standards. This is an appropriate scientific and logical approach to establishing a benchmark for developing any additional standards to further protect the North American electric grid from harm.We request that in order to give this project the

Organization	Yes or No	Question 4 Comment
		proper thought and effort that it deserves, NERC should reconsider seeking an extension from FERC in order to allow more time for a broader cross section of industry and as many technical experts as possible to participate in developing a product which will be more effective at maintaining the reliability of the BES.What does RISC say about the need for this standard? Have they been consulted? Also, what about the Independent Expert Review Panel? Have these parties voiced an opinion?Do the studies referenced in Table 1 of the TPL standards point to the list of the limited set of substations which this project is intended to address? Are the substations tied to these studies in any manner?The order mentions facilities being inoperable or not available but there was no reference to misuse as there is in the CIPs standards. Can we assume that cyber-type attacks on substations are already adequately accounted for in the CIPs standards and therefore do not need to be factored into the Physical Security standard?
Bonneville Power Administration	Yes	BPA believes it is virtually impossible to fully protect all critical BES facilities from attack by a determined foe. The means to damage BES facilities is readily available, constructible, and implementable regardless of what level of physical hardening is implemented. There are many question and issues to resolve, and the 90 day drafting period may not be long enough to address them all. The biggest general question to answer is what will be considered adequate protection.Will we need a 24 hour on site armed security force because the location is too remote to augment detection technology with fast response that will minimize the scale of impact to an acceptable level of loss? Will we need security walls constructed to be as impervious as those of a maximum security prison? The list of potential risk mitigation barriers is endless, as is the cost of building and maintaining elaborate barriers for facilities that cover acres of ground. It will be interesting to see what a standard of this type will prescribe as required to obtain a level of risk that is significantly lower than the current state potential for experiencing another Metcalf type event.BPA has concerns that the compressed time frame will impact quality and thoroughness of the dialog needed to develop “unambiguous” standards.

Organization	Yes or No	Question 4 Comment
Foundation for Resilient Societies	Yes	Detectors for Intentional Electromagnetic Interference (IEMI) and Electromagnetic Pulse as a Physical Security MeasureBecause an IEMI attack would take place in the physical proximity of critical facilities of the bulk electric system, it should be considered a physical security vulnerability for standard-setting for FERC Order RD14-6-000, just as a kinetic attack or physical intrusion would be covered in a physical security standard. Electronic upsets and failures occur under normal operating circumstances, even in high-reliability equipment such as that supporting critical infrastructure. Intentional Electromagnetic Interference (IEMI) and other electromagnetic pulse (EMP) induced upsets and failures, however, are different from those encountered in the normal operation of infrastructure systems, and in fact have unique aspects not encountered under any other circumstances. A coordinated physical attack using IEMI could produce nearly simultaneous upset and damage of electronic equipment over wide geographic areas. Since such non-random upset and damage is not encountered in other circumstances, the normal experience of otherwise skilled system operators and others in positions of responsibility and authority will not prepare them to identify what has happened to the system, what actions to take to minimize further adverse consequences, and what actions must be carried out to restore the impacted systems as swiftly and effectively as possible.Special system capabilities and operator awareness, planning, training, and testing will be required to deal with IEMI/EMP-induced system impacts. The first requirement is for the operators of critical infrastructure systems to be able to determine that a IEMI/EMP attack has occurred.It will be necessary to distinguish high altitude nuclear EMP (HEMP) effects from localized IEMI effects that could be generated by a cruise missile or ground based vehicle employing non-nuclear intentional electronic interference devices. IEMI attacks have fast rise times measured in nanoseconds but limited geographic range; detectors can be designed to distinguish between nuclear EMP and IEMI.Indications of IEMI or EMP attack should be transmitted to electric grid control rooms so operators can gain a comprehensive picture and adjust operational response. Without electromagnetic sensors and

Organization	Yes or No	Question 4 Comment
		associated telemetry and alarm systems, operators would be flying blind in case of IEMI/EMP attack.
Minnkota Power Cooperative	Yes	a) On page 5 of the SAR, under the Related Standards section, there lists 3 CIP Reliability Standards (CIP-006-5, CIP008-5, and CIP-009-5), with an explanation to review them to ensure no language and terminology inconsistency with requirements developed under this project. CIP-011-1 - Cyber Security Information Protection should also be added to the list. Paragraph (10) of the FERC order describes the importance of guarding sensitive or confidential information. While CIP-011-1 is focused towards BES Cyber System Information, the information protection program entities may adopt could be hindered if CIP-011-1 was not considered when developing new standard(s) to address the directives in the March 7, 2014 FERC Order regarding the physical security of critical facilities on the Bulk-Power System.b) On page 3 of the SAR, under the Reliability Functions section, lists the Functions the Standard(s) would be applicable to (TO and TOP are checked). Shouldn't GO and GOP also be checked. The FERC order states the "proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System". The key words to note are "owners or operators". A generation plant, under the BES definition enforceable July 1, 2014, could be considered critical to the reliable operation of the Bulk-Power System.
Entergy Services, Inc.	Yes	Compressed timeline will limit NERC's ability to acquire input from owners or operators of the Bulk-Power System.
Encari	Yes	If the proposed standard under this project takes effect and is implemented prior to 3/31/2016, then the proposed standard should take into account CIP-002-3 which has a process for identifying Critical Assets. After 3/31/2016, CIP-002-3 and the term "Critical Asset" become inactive.

Organization	Yes or No	Question 4 Comment
Idaho Power Co.	Yes	Related Standards. CIP-002-5 is not mentioned and as one of the instructions is 'to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System' unless we are going with another set of criteria and labelling the facilities differently, this seems to be what CIP-002-5 does.
The Empire District Electric Company	Yes	The 90-day response requested by FERC is well outside the normal standard development process at NERC. This process is an established, transparent process which incorporates stakeholder consensus. How will the industry be able to adequately respond to the directive when the process we use isn't designed for such a quick development time? Trying to respond within a 90-day period while maintaining some resemblance of our existing process will be difficult indeed. The apparent driver behind this effort, the WSJ article, seems a bit misdirected. The Metcalf event occurred over a year ago, yet the standard has been mandated to be issued within 90 days. If the issue was that critical, why hasn't something been done sooner? And if this is a truly critical situation, we need to be sure to move logically in a well, thought-out process to reach the right conclusion rather than respond with a "knee-jerk" reaction to a newspaper article. How was the list of 9 substations in the WSJ article determined? What studies were ran to make this determination? What process was used to validate the study? What were the credentials of those conducting the study? Numerous questions like these come to mind regarding the credibility of the analysis behind the study upon which the article is founded. The WSJ article referred to entire interconnections going down due to the loss of 9 substations across 3 interconnections. Four substations are credited with being able to bring down the entire EI. This is doubtful. This study must be vetted by industry experts to first establish if a reliability gap exists.
the empire district electric company	Yes	The 90-day response requested by FERC is well outside the normal standard development process at NERC. This process is an established, transparent process which incorporates stakeholder consensus. How will the industry be able to adequately respond to the directive when the process we use isn't geared to such a

Organization	Yes or No	Question 4 Comment
		quick turn-around? Trying to respond within a 90-day period while maintaining some semblance of our existing process will be difficult indeed. It's literally like trying to hit a target that is hidden in the dark.The apparent driver behind this effort, the WSJ article, seems a bit misdirected. The Metcalf event occurred over a year ago, yet no action has been taken to date to address the situation. If the issue was that critical, why hasn't something been done sooner? And if this is a truly critical situation, we need to be sure to move logically in a well, thought-out process to reach the right conclusion rather than respond with a knee-jerk reaction to a newspaper article. How was the list of 9 substations in the WSJ article determined, what studies were ran to make this determination, what process was used to validate the study, what were the credentials of those conducting the study? Numerous questions like these come to mind regarding the credibility of the analysis behind the study upon which the article is founded. The WSJ article referred to entire interconnections going down due to the loss of 9 substations across 3 interconnections. Four substations are credited with being able to bring down the entire EI. This is doubtful. This study must be vetted by industry experts to first establish if a reliability gap exists.We request that in order to give this project the proper thought and effort that it deserves, NERC seek an extension from FERC which will allow more time to complete the project. Allowing more time and consideration will result in a better product which will be more effective at maintaining the reliability of the BES.What does RISC say about the need for this standard? Have they been consulted? Also, what about the Independent Expert Review Panel? Have these parties voiced an opinion?Do the studies referenced in Table 1 in the TPL standards point to the list of 'the 9 substations' mentioned? Are the substations tied to these studies in any manner?The order mentions facilities being inoperable or not available but there was no reference to misuse as there is in the CIPs standards. Can we assume that cyber-type attacks on substations are already adequately accounted for in the CIPs standards and therefore do not need to be factored into the Physical Security standard?

Organization	Yes or No	Question 4 Comment
The Empire District Electric Company	Yes	The 90-day response requested by FERC is well outside the normal standard development process at NERC. This process is an established, transparent process which incorporates stakeholder consensus. How will the industry be able to adequately respond to the directive when the process we use isn't geared to such a quick turn-around? Trying to respond within a 90-day period while maintaining some semblance of our existing process will be difficult indeed. It's literally like trying to hit a target that is hidden in the dark.The apparent driver behind this effort, the WSJ article, seems a bit misdirected. The Metcalf event occurred over a year ago, yet no action has been taken to date to address the situation. If the issue was that critical, why hasn't something been done sooner? And if this is a truly critical situation, we need to be sure to move logically in a well, thought-out process to reach the right conclusion rather than respond with a knee-jerk reaction to a newspaper article. How was the list of 9 substations in the WSJ article determined, what studies were ran to make this determination, what process was used to validate the study, what were the credentials of those conducting the study? Numerous questions like these come to mind regarding the credibility of the analysis behind the study upon which the article is founded. The WSJ article referred to entire interconnections going down due to the loss of 9 substations across 3 interconnections. Four substations are credited with being able to bring down the entire EI. This is doubtful. This study must be vetted by industry experts to first establish if a reliability gap exists.We request that in order to give this project the proper thought and effort that it deserves, NERC seek an extension from FERC which will allow more time to complete the project. Allowing more time and consideration will result in a better product which will be more effective at maintaining the reliability of the BES.What does RISC say about the need for this standard? Have they been consulted? Also, what about the Independent Expert Review Panel? Have these parties voiced an opinion?Do the studies referenced in Table 1 in the TPL standards point to the list of 'the 9 substations' mentioned? Are the substations tied to these studies in any manner?The order mentions facilities being inoperable or not available but there was no reference to misuse as there is in the CIPs standards. Can we assume that cyber-type attacks on

Organization	Yes or No	Question 4 Comment
		substations are already adequately accounted for in the CIPs standards and therefore do not need to be factored into the Physical Security standard?
Westar Energy	Yes	The FERC imposed development timeframe of 90 days is inadequate. The normal Standard Development Process allows for a transparent process which incorporates stakeholder consensus.The quality of the regulation will be adversely impacted by such an accelerated schedule.Westar requests that in order to give this project the proper thought and effort that it deserves, NERC seek an extension from FERC which will allow more time to complete the project. Allowing more time and consideration will result in a better product which will be more effective at maintaining the reliability of the BES.
Occidental Energy Ventures Corp.	Yes	This project is one of several which FERC has clearly established their expectation of urgent action. The CIP Version 5 Cyber Security, Geomagnetic Disturbance, and Gas/Electricity Industry Interoperability standards come immediately to mind. In OEVC's view, this means that NERC's standards development prioritization must be updated to take on the new work load - even if other project activity needs to be suspended in favor of Project 2014-04.Furthermore, there are a large number of new and/or modified standards which are scheduled to take effect this year and next - Generator Validations, and Protection System maintenance are among the most pressing. As a result, OEVC believes it is time for a second iteration of the Paragraph 81 process to aggressively retire those requirements that do little to support BES reliability. We understand that the obvious candidates have been addressed, but the industry's efforts must be continually re-focused on higher-priority activities. As long as less urgent requirements remain on the books, we all must set aside resources to capture evidence of compliance to routine tasks; leaving fewer available to address far more important threats to the BES.
Colorado Springs Utilities	Yes	The 90-day response requested by FERC is well outside the normal standard development process at NERC. This process is an established, transparent process which incorporates stakeholder consensus. The result of this accelerated process will

Organization	Yes or No	Question 4 Comment
		be an inferior standard.We request that in order to give this project the proper thought and effort that it deserves, NERC seek an extension from FERC which will allow more time to complete the project. Allowing more time and consideration will result in a better product which will be more effective at maintaining the reliability of the BES.We feel the focus should be on recovery from an attack, not solely prevention. We believe this has a larger impact on the reliability of the BES. Include something in the new standard that BES information should be protected, especially for public entities subject to Open Records Acts.
Manitoba Hydro	Yes	(1) Related Standards to avoid inconsistencies should include CIP-004-5 which addresses physical access management, a component of overall physical security. (2) "Applicability" should include an RC or PA/PC, as these would be the most appropriate Reliability Functions to determine if the loss of a facility would result in instability etc.
American Electric Power	Yes	While American Electric Power (AEP) appreciates the need for expediency in this FERC docket and relevant NERC SARs/Standards, we caution against an assumption that because a specific category of threat may be perceived as new, no efforts are yet underway to protect against that threat. In reality, AEP already has in place significant protections to secure the reliability of the grid - as does most of the electric utility industry. Many of these protections are in system configuration and design, inherently minimizing the criticality of any particular transformer, transmission circuit or station. These system configuration and design protections are incorporated to foster transmission system reliability in the event of weather and/or normal equipment failures. But they also answer the need for protection from other physical threats. In many cases our existing safeguards will protect the grid against new threats, including intentionally created damage.AEP agrees with FERC Commissioner John Norris' concurring comments filed with RD14-6-000 on March 7: "The owners and operators of our Bulk-Power System have already taken significant steps to protect critical facilities from physical attack. NERC's standards development process will benefit from the lessons learned from the owners and operators of the Bulk-

Organization	Yes or No	Question 4 Comment
		Power System and the communication that will take place across the stakeholder community regarding physical security. However, I am concerned that the procedural approach chosen by the Commission will inappropriately preclude an open and transparent process in which all interested parties would be able to engage with the Commission as the standards development process gets underway."AEP does not fully understand NERC's SAR which describes this effort as a New Standard, but not an Urgent Action. Certainly, the uniquely short timeframes allowed first by FERC and then by NERC for stakeholder participation imply an element of urgency. With no provision for comment to FERC and reduced input ability at NERC, the industry and our customers run the risk of unnecessary costs resulting from rushed decisions made with inadequate data. Likewise, addressing only Transmission Owners and Transmission Operators will provide less than a complete picture. Reliability Coordinators and Balancing Authorities also have a role to play and excluding that role from consideration will yield sub-par results. Additionally, some of the issues covered in the SAR and the FERC docket seem to overlap with existing Standards. Violations of a Standard that could stem from this effort might also be violations of CIP-002, CIP-006, CIP-008 and/or CIP-009. Care must be taken to ensure that the Standards dovetail, rather than duplicate each other, which would create a double-jeopardy situation for grid owners.In addition to our concerns about the process, AEP has reservations about the substance of the proposed SAR as well. First, AEP questions how the SAR proposes to define critical facilities. FERC and NERC have implied that the number of critical facilities identified in this process will be relatively small - fewer than 100 of the 55,000 transmission stations dispersed throughout the country. However, for previous "critical asset" determinations requested by NERC, AEP has already identified almost that many just on our own system. This would indicate we are starting over with the definition of critical facilities, which is counter-intuitive if not counter-productive. CIP-V5 switches the focus from protecting discrete cyber assets to protecting systems. Shouldn't we consider this same approach for physical security? AEP suggests that we begin by determining how critical facilities will be defined: 1) Will it be a bright-line test or a triage approach? 2) What will

Organization	Yes or No	Question 4 Comment
		distinguish critical cyber facilities from physical, and will one facility category be deemed more critical than the other? 3) Is there a distinction between a “critical facility” and “critical assets” defined in previous initiatives?4) Will there be distinctions between staffed and unstaffed stations, control centers or shared facilities?AEP believes that critical physical facilities will largely be a subset of the critical cyber asset list, tempered by:1) Availability of equipment spares, 2) Equipment redundancy located at the same vs. adjacent stations, 3) Level of interconnection to other stations at a particular voltage level,4) Proximity to a nuclear station, 5) Availability of alternative black start paths, 6) A sundry list of similar considerations. This analysis suggests that determination of a particular station as a critical physical facility is not a yes/no question, but rather a tiered approach to physical criticality is required. Considering the above, two stations similarly configured but in different parts of the system may not have the same physical criticality. Therefore, AEP is pleased with the nod to regional differences and the flexibility indicated in RD14-6-000. However, the changes NERC and FERC are proposing could result in massive changes, bringing excessive additional costs with no guarantee of desired outcomes. The question then becomes whether the cost to the nation’s electric customers far outweighs the benefits from additional protections layered on top of existing protocols. Are we being overly reactive to the isolated case of the Metcalf Station attack in San Jose a year ago? Are we painting targets on our critical infrastructure? Even with increased physical security, there will always be some potential for an attack on a critical facility. Larger fences and armed guards will make attacks marginally more difficult. They will not make the facilities immune to attack. A second primary concern is cost recovery - an issue that neither FERC nor NERC has addressed. Should NERC determine that a bright-line definition of critical facilities is the best way to go, cost recovery would be easier for grid owners, but costlier for customers. If NERC gives grid owners discretion to identify their critical facilities through risk-based assessments and determine their own protection strategies, state regulatory commissions will question every decision made, creating regulatory lag. That said, a risk-based assessment resulting in tiered levels of

Organization	Yes or No	Question 4 Comment
		criticality would yield the strongest results from a grid protection standpoint. While grid protection is paramount, we must weigh options. Poorly executed, these Standards could carry astronomical real costs as well as opportunity costs. Meanwhile, many customers are about to bear significant cost increases based on changes required by the EPA's Mercury and Toxics Standards. While we need to make whatever investment is necessary to adequately protect the grid, we also need to be responsible stewards of the grid and our ratepayers' pocket books. We must make sure we have taken necessary steps as cost-effectively as possible and that we are not simply being reactionary.In summary, AEP supports:1) Risk-based assessments conducted by transmission owners to define their own critical facilities2) Triage protocols based on those risk-based assessments3) Acknowledgement and inclusion of existing protections4) Adoption of a CIP-V5 approach of protecting critical systems rather than discrete facilities5) Cost-based assessments that include opportunity costs and factor in cost recovery.
Hydro One	Yes	The SAR should ask the SDT to define how the verification of the risk assessment used by the owner or operator of critical facilities will be completed. The standard should identify the methodology by which critical facilities were identified? If it is the methodology, then the SAR should also define the methodology for doing this verification. The FERC Order states "the Reliability Standards should require that the identification of the criticalfacilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness." The definition of the methodology for review should be applied to the review of all 3 of identification of critical facilities, determination of threats and vulnerabilities, and mitigation plans, and that the standard should clarify whether the mitigation plans also have to be reviewed by a third party.There is risk that significant investments may be needed as a result of the new standard.There SDT should ensure that the new standard does not call for requirements that will impact or impede the normal operational capacity, access for maintenance or restoration, or the safety of people or equipment.Minimum vulnerabilities should be defined in the standard to be included in vulnerability

Organization	Yes or No	Question 4 Comment
		assessments.The assessment of critical facilities should be defined in a TPL standard based assessment.The standard should clearly define the timelines for conducting assessments and implementing the mitigation actions identified with respect to when the standard becomes effective.Timelines for assessment of risk or vulnerabilities in this new standard should coincide with the timelines for which assessment of risk or vulnerabilities for other standards including the CIP and the new GMD Stage 2 project which will be a new TPL standard.
Northeast Utilities	Yes	NU urges that the SDT not be too prescriptive in the development of these requirements. Entities should be able to conduct a vulnerability assessment and implement any mitigation actions that they deem appropriate. SDT should carefully consider the cost impact that the standard will have on entities to implement and therefore limit the site selection.SDT should define minimum vulnerabilities to be included in vulnerability assessments.SDT to provide for timing of the effective date of standard versus the time required to conduct assessments and implement mitigation actions identified.SDT should clearly limit the scope of the standard to protection against physical attacks.
Xcel Energy Inc.	Yes	A review of the CIP standards (Version 5) is required by the SAR. However, considering that many, if not all of the facilities in scope of this new standard will also likely be considered Critical Assets, as defined by CIP-002-5, this has the possibility of creating double jeopardy situations and added Regulatory oversight. Instead, please consider addressing physical security through an existing standard like CIP-006-5 or EOP-004-2 (Event Reporting).
Utility Services, Inc	Yes	The identification method that will be used to determine applicability to the standard is a concern. The drafting team should take care to respect the work already crafted by the previous CIP drafting teams in creating a format and brightline thresholds to identify those facilities that require protection. From historical experience we have seen that “Risk Assessment” style applicability is not consistently and uniformly

Organization	Yes or No	Question 4 Comment
		applied and should therefore be avoided. We have seen this causes major issues and we should not repeat past mistakes.
Nebraska Public Power District	Yes	If we truly have a small subset of nine key substations that are as critical as was quoted in the Wall Street Journal, why isn't the military protecting these substations? We use our military to protect our Air Force bases, Army forts, Naval yards, etc. Is this threat real or is it political sensationalism? Is the number of substations nine, or is it 30 or is it less than 100 as the Wall Street Journal quoted former FERC chairperson Wellinghoff. Shouldn't the electric industry experts be allowed to review the modeling for this analysis? Was the modeling in sufficient detail or were many networks equivalized? Was it a steady-state model or were dynamics evaluated? What was the experience level of the engineers doing the analysis (have they performed similar analysis at large utilities)? Should we revoke this SAR and replace it with another new standard that would restrict utilities from building any new substations above a certain level? Should the standard require planned additions/expansions to provide for redundancy and resiliency as the Department of Homeland Security and Department of Energy recently recommended in their Physical Security of Substations Briefing? Do we have to build 500 kV and 765 kV systems? Does the market save us any money to transfer power between regions, if we have to add these systems that open up vulnerabilities to physical attacks?Should Congress fund a US based manufacturing plant for transformers?Should North America (those within NERC) standardize voltage levels, so replacement transformers are more readily available?The list of philosophical questions can continue, but we are not ready to draft a standard on this issue without first debating the problem we are trying to solve. What is the problem we are trying to solve?The Wall Street Journal article implied we need to protect our substations from automatic weapons. Is this the problem we are trying to solve? Will we be required to build walls around our substations? What do we do about a substation that is located in a valley with unlimited firing angles from surrounding higher ground? How do we protect the miles and miles of transmission structures leading to these substations? Do we have to protect one substation away, two substations away, etc.By installing additional

Organization	Yes or No	Question 4 Comment
		security on these facilities, aren't we painting those assets as targets by clearly identifying them?
Ameren	Yes	1) The time frame that is outlined in this SAR to create a new physical security standard is very short and we are concerned that a cost effective, reasonable, workable standard cannot be drafted in this short amount of time. We understand the need for a new physical security standard but creating a standard this quick could result in an incorrectly written standard which will not be understood by industry. We are concerned that this does not solve the problem but will end up making a new one.
New Brunswick Power Corporation	Yes	It is our desire to ensure the SDT consider the impacts of physical security threats that can arise between entities (wide area view) rather than a strict focus on the effects of physical security risks on elements within a given entity's footprint. Taking this approach and allowing the entity to determine the specific impact criteria for their footprint, should align the violation risk factors and severity levels to account for higher level threats rather than burden the entities with lower impact concerns.
Tri-State Generation and Transmission Association, Inc.	Yes	In agreement with the Commissioner, John Norris's, concurrence, the uniquely expedited nature of this standard development procedural approach will preclude an open and transparent process, limit the engagement of the industry, and, without the time to properly vet the security risks and measures, will negatively impact reliability and consumer costs.Co-owned facilities are not addressed in the standard. Co-owned facilities will have multiple assessments by different entities. This will lead to different threat assessments and different physical security plans. Conflicts may and most likely will occur on co-owned facilities. This is something that must to be taken into consideration.There is no requirement for 3rd party verification for CIP-002-5.1 R2 which requires assessment and categorization of assets. 3rd party verification is not required there and should not be required here. Senior approval should be all that's necessary. Some possibilities to address the FERC order for verification of entities' plans include a submittal to the RC/RE upon their request as currently

Organization	Yes or No	Question 4 Comment
		required by many of the emergency operations plans or an annual submittal to the RC/RE.Something else to consider is that audits for TO/TOPs are on a 3 year cycle. The RE could review the assessments and plans during audits removing the requirement for 3rd party verification.Physical threats run the gamut of simple to highly complex. What will limit this review? Addressing ALL potential threats will be cost prohibitiveThe value necessary for a facility to qualify should be raised. The criteria from CIP-002 v5 is meant to include a larger portion of the grid. This criteria will include too many facilities which was not the intent of FERC.
Salt River Project	Yes	The SAR should closely follow the FERC Order that owners and operators are to develop their specific plans to protect against physical attacks that may compromise their facilities. The FERC Order provides for flexibility for owners and operators to determine the methodology they will use in identifying their critical facilities. The standard should direct the entities to focus on station facilities and not 'outside the fence' assets. Critical facilities vary widely both in the type and extent of potential vulnerabilities to physical attacks. Customized defenses and protections are esstential and the owners and operators are correctly given flexibility both in identifying which assets are critical and then developing the most appropriate plans for protection. That plan should not be primarily directed at physical deterrence of the threats, there are two other important facets of a security plan: operational security, and recovery after an event. The flexibility will help avoid potential conflicts between any new standards and existing ones. The objectives of the SAR are to provide clear, unambiguous requirements and standard(s) to address the FERC Order. This should not mean development of requirements with highly prescriptive, detailed and specific physical protection structures, activities and programs but instead should mean the SAR will develop clear direction on identification of critical facilities and credible physical threats to such facilities followed by prudent plans for protection that are appropriate for each such facility.
Kansas City Power & Light	Yes	The 90-day response requested by FERC is well outside the normal standard development process at NERC. This process is an established, transparent process

Organization	Yes or No	Question 4 Comment
		which incorporates stakeholder consensus. Trying to respond within a 90-day period while giving the appropriate diligence and consideration to the topic of protection of BES assets will be difficult. We recommend taking appropriate time to give this project the proper thought and effort that it deserves for diligent actions to be taken to protect the grid. We respectfully ask NERC to remain open to the potential need to seek an extension from FERC to allow more time to complete the project if deemed necessary. The order mentions facilities being inoperable or not available but there was no reference to misuse or a resiliency concept. We believe the SDT should consider these options including the concept of a capability / maturity model and on a continuum for improvements in the hardening of our BES facilities. Ultimately the goal is to focus on protection and security of assets.

END OF REPORT

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. Nominations for the Standard Drafting Team (SDT) for Project 2014-04 Physical Security were solicited March 13-18, 2014, and the SDT was appointed by the Standards Committee on March 21, 2014.
2. Technical Conference was held April 1, 2014.

Description of Current Draft

This is the first draft of the proposed Reliability Standard, and it is being posted for stakeholder comment and initial ballot. This draft includes proposed requirements to meet the directives issued in the FERC order issued March 7, 2014, in Docket No. RD14-6-000, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

Anticipated Actions	Anticipated Date
15-day Formal Comment Period with a 5-day Initial Ballot, pursuant to a Standards Committee authorized waiver.	April 10, 2014
10-day Formal Comment Period with a 5-day Additional Ballot (if necessary), pursuant to a Standards Committee authorized waiver.	May 2014
5-day Final Ballot, pursuant to a Standards Committee authorized waiver.	May 2014
BOT Adoption.	May 2014
File with applicable Regulatory Authorities.	No later than June 5, 2014

Version History

Version	Date	Action	Change Tracking
1.0	TBD	Effective Date	New

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the NERC Glossary of Terms used in Reliability Standards (Glossary) are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

A. Introduction

1. Title: Physical Security

2. Number: CIP-014-1

3. Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner that owns any of the following:

4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

4.1.1.3 Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection

Reliability Operating Limits (IROLs) and their associated contingencies.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities within the scope of a security plan approved by the Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission are not subject to this Standard.

5. Effective Dates:

CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

This Reliability Standard addresses the directives from the FERC order issued March 7, 2014, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014), which required NERC to develop a physical security reliability standard(s) to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

B. Requirements and Measures

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify any Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or

- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1.

Rationale for Requirement R1:

This requirement meets the FERC directive from paragraph 6 in the order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through widespread instability, uncontrolled separation, or cascading failures. It also meets the portion of the directive from paragraph 11 for periodic reevaluation by requiring the risk assessment to be performed every 30 months (or 60 months for an entity that has not identified in a previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in

widespread instability, uncontrolled separation, or Cascading within an Interconnection).

After identifying each Transmission station and Transmission substation that meets the criteria in Requirement R1, it is important to additionally identify the primary control center that operationally controls that Transmission station or Transmission substation (*i.e.,* the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated verifying entity shall either verify the Transmission Owner's risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information exchanged with the unaffiliated verifying entity.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3.

Rationale for Requirement R2:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring verification by an entity other than the owner or operator of the risk assessment performed under Requirement R1.

This requirement provides the flexibility for a Transmission Owner to select registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term "unaffiliated" means that the selected verifying entity cannot be a corporate affiliate (*i.e.*, the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout the Requirement R1 risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform a Requirement R1 risk assessment to satisfy both Requirement R1 and Requirement R2 concurrently.

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1 and verified according to Requirement R2 that is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Rationale for Requirement R3:

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first identifying which Transmission stations and Transmission substations meet the criteria specified by Requirement R1, as verified according to Requirement R2. This requirement is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 and verified according to Requirement R2 receives notice of such identification so that the Transmission Operator may timely fulfill its resulting obligations under Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include notice of the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or the verification process under Requirement R2.

R4. Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Rationale for Requirement R4:

This requirement meets the FERC directive from paragraph 8 in the order on physical security that the reliability standard must require tailored evaluation of potential threats and vulnerabilities to facilities identified in Requirement R1 and verified according to Requirement R2. Threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections, and attractiveness of the target. As such, the requirement does not mandate a one-size-fits-all approach but requires entities to account for the unique characteristics of their facilities.

Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur or be completed. However, Requirement R5 requires that the entity's security plan(s), which is dependent on the Requirement R4 evaluation, must be completed within 120 calendar days following completion of Requirement R2. Thus, an entity has the flexibility when to complete the Requirement R4 evaluation, provided that it is completed in time to comply with the requirement in Requirement R5 to develop a physical security plan 120 calendar days following completion of Requirement R2.

R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.1. Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for implementing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating implementation of the physical security plan.

Rationale for Requirement R5:

This requirement meets the FERC directive from paragraph 9 in the order on physical security requiring the development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

R6. Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

6.1.1. An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.

6.1.2. An entity or organization approved by the ERO.

6.1.3. A governmental agency with physical security expertise.

6.1.4. An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated reviewing entity recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or
- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information exchanged with the unaffiliated reviewing entity.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3.

Rationale for Requirement R6:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring review by an entity other than the owner or operator with appropriate expertise of the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5.

As with the verification required by Requirement R2, Requirement R6 provides Transmission Owners and Transmission Operators the flexibility to work with the reviewing entity throughout the Requirement R4 evaluation and the development of the Requirement R5 security plan(s). This would allow entities to satisfy their obligations under Requirement R6 concurrent with the satisfaction of their obligations under Requirements R4 and R5.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

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

The Transmission Owner and Transmission Operator shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation.

The responsible entities shall retain documentation as evidence for three years.

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

The CEA shall keep the last audit records and all requested and submitted subsequent audit records, subject to the confidentiality provisions of Section 1500 of the Rules of Procedure and the provisions of Section 1.4 below.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information

Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**High**	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection	Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.	Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.	performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.	uncontrolled separation, or Cascading within an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
R2	**Long-term Planning**	**Medium**	The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but less than or equal to	The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but less than or equal to	The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to 120 calendar days	The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days following

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			100 calendar days following completion of Requirement R1; OR The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under R1 as required by part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.	110 calendar days following completion of Requirement R1; Or The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under R1 as required by part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.	following completion of Requirement R1; OR The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under R1 as required by part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 but failed to modify or document the technical basis for not	completion of Requirement R1; OR The Transmission Owner failed to have a third party verify the risk assessment performed under Requirement R1; OR The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					modifying its identification under R1 as required by part 2.3.	
R3	**Long-term Planning**	**Lower**	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 11	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control center identified in Requirement R1; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R1 but did so more than seven calendar days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.	Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.	calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.	The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1.
R4	**Operations Planning,**	**Medium**	N/A	The Responsible Entity conducted an	The Responsible Entity conducted an	The Responsible Entity failed to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Long-term Planning			evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.	evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.	conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						consider Parts 4.1 through 4.3.
R5	**Long-term Planning**	**High**	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR The Responsible Entity failed to develop and implement a documented physical security

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to include one of Parts 5.1 through 5.4 in the plan.	Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to include two of Parts 5.1 through 5.4 in the plan.	Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to include three of Parts 5.1 through 5.4 in the plan.	plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to include Parts 5.1 through 5.4 in the plan.
R6	**Long-term Planning**	**Medium**	The Responsible Entity had a third party review the	The Responsible Entity had a third party review the	The Responsible Entity had a third party review the evaluation	The Responsible Entity failed to have a third party review

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days; OR The Responsible Entity had a third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion	evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had a third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days	performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had a third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review;	the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have a third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5; OR The Responsible Entity had a third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the third party review.	following completion of the third party review.	OR The Responsible Entity had a third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not and modify or document the reason for not modifying the security plan(s) as specified in Part 6.3.	failed to implement procedures for protecting information per Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 Applicability

The purpose of Reliability Standard CIP-014-1 is to protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014-1 first applies to Transmission Owners (TO) that own Transmission Facilities that meet the specific criteria in Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4 mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1. Each TO that owns Transmission Facilities that meet the criteria in Section 4.1.1.1 through 4.1.1.4 is required to perform a risk assessment as specified in Requirement R1 to identify its Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Standard Drafting Team (SDT) expects this population will be small and that many TOs that meet the applicability of this standard will not actually identify any such Facilities. Only those TOs with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6.

This standard also applies to Transmission Operators (TOP). A TOP's obligations under the standard, however, are only triggered if the TOP is notified by an applicable TO under Requirement R3 that the TOP operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the Requirement R1 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only TOPs who are notified that they have primary control centers under this standard have performance obligations under Requirements R4 through R6.

The drafting team considered several options for bright line criteria that could be used to determine applicability and provide an initial threshold that defines the set of Transmission stations and Transmission substations that would meet the directives of the FERC order on physical security (*i.e.*, those that could cause widespread instability, uncontrolled separation, or Cascading within an Interconnection). The SDT determined that using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. Additionally, the SDT concluded that using the CIP-002-5.1 Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis

to determine which Transmission Owners should conduct the risk assessment. As described in CIP-002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). The SDT understands that using this bright line criteria to determine applicability may require some Transmission Owners to perform risk assessments under Requirement R1 that will result in a finding that none of their Transmission stations or Transmission substations would pose a risk of widespread instability, uncontrolled separation, or Cascading within an Interconnection. However, the SDT determined that higher bright lines could not be technically justified to ensure inclusion of all Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Further guidance and technical basis for the bright line criteria for Medium Impact Facilities can be found in the Guidelines and Technical Basis section of CIP-002-5.1.

Additionally, the SDT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. First, the transmission analysis or analyses conducted under Requirement R1 will take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities.

Requirement R1

In performing the risk assessment under Requirement R1, the Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Applicability Section 4.1.1. Requirement R1 then requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The standard does not mandate the specific analytical method for performing the risk assessment. The Transmission Owner has the discretion to choose the specific method that best suites its needs. As an example, an entity may perform a Power Flow analysis and stability analysis at a variety of load levels.

Performing Risk Assessments

The following is guidance on how a Transmission Owner may perform a traditional power flow and stability analysis to identify those Transmission stations and Transmission substations that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. An entity could remove all lines to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a wide area. Using engineering judgment, the Transmission Owner should develop criteria to identify a contingency resulting in potential widespread instability, uncontrolled separation or Cascading within an Interconnection. For example, the criteria could include post-contingency

facilities loadings above a certain emergency rating or failure of a power flow case to converge. Available remedial action schemes (RAS) or special protection systems (SPS), if any, could be applied to determine if the system experiences any additional instability which may result in uncontrolled separation.

Periodicity

A TO who identifies one or more Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection is required to conduct a risk assessment at least once every 30 months. This period ensures that the risk assessment remains current with projected conditions and configurations in the planned system.

TOs who have not identified any Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection are unlikely to see changes to their risk assessment in the Near-Term Planning Horizon. Consequently, a 60 month periodicity for completing a subsequent risk assessment is specified.

Identification of Primary Control Centers

After completing the risk assessment specified in Requirement R1, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center "operationally controls" a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

Requirement R2

This requirement specifies verification of the risk assessment performed under Requirement R1 by an entity other than the owner or operator of the Requirement R1 risk assessment.

A verification of the risk assessment by an unaffiliated third party, as specified in Requirement R2, could consist of:

1. Certifying that the Requirement R1 risk assessment considers the Transmission stations and Transmission substations identified in Applicability Section 4.1.1.
2. Review of the model used to conduct the risk assessment to ensure it contains sufficient system topology to identify Transmission stations and Transmission substations that if rendered inoperable or damaged could cause widespread instability, uncontrolled separation, or Cascading within an Interconnection.
3. Review of the Requirement R1 risk assessment method, which may include, for example, consideration of factors such as the following system performance criteria:
    a. Thermal overloads beyond facility emergency ratings;
    b. Voltage deviation exceeding ± 10%,

c. Cascading outage/Voltage collapse,

d. Frequency below under-frequency load shed points.

This requirement provides the flexibility for a Transmission Owner to select from unaffiliated registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term unaffiliated means that the selected verifying entity cannot be a corporate affiliate (*i.e.,* the verifying or reviewing entity cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout (*i.e.,* concurrent with) the risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently.

Characteristics to consider in selecting a reviewing entity could include:

- Registered Entity with applicable planning and reliability functions.
- Experience in power system studies and planning.
- The entity's understanding of the MOD standards, TPL standards, and facility ratings as they pertain to planning studies.
- The entity's familiarity with the Interconnection within which the transmission owner is located.

With respect to the requirement that Transmission owners develop and implement procedures for protecting confidential and sensitive information, the Transmission Owner could have a method for identifying documents that require confidential treatment. One mechanism for protecting confidential or sensitive information is to prohibit removal of sensitive or confidential information from the TO's site. Transmission Owners could include such a prohibition in a non-disclosure agreement with the verifying entity.

Requirement R3

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first completing the risk assessment specified by Requirement R1 and the verification specified by Requirement R2. Requirement R3 is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 receive notice so that the Transmission Operator may fulfill the rest of the obligations required in Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include within the notice the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk

assessment under Requirement R1 or as a result of the verification process under Requirement R2.

Requirement R4

This requirement requires owners and operators of facilities identified by the Requirement R1 risk assessment and that are verified under Requirement R2 to conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process. Threats and vulnerabilities may vary from facility to facility based on any number of factors that include, but are not limited to, location, size, function, existing physical security protections, and attractiveness as a target.

In order to effectively conduct a threat and vulnerability assessment, the asset owner may be the best source to determine specific site vulnerabilities, but current and evolving threats may best be determined by others in the intelligence or law enforcement communities. A number of resources have been identified in the standard, but many others exist and asset owners are not limited to where they may turn for assistance. Additional resources may include state or local fusion centers, U.S. Department of Homeland Security, Federal Bureau of Investigations (FBI), Public Safety Canada, Royal Canadian Mounted Police, and InfraGard chapters coordinated by the FBI.

The Responsible Entity is required to take a number of factors into account in Parts 4.1 to 4.3 in order to make a risk-based evaluation under Requirement R4.

To assist in determining the current threat for a facility, the prior history of attacks on similarly protected facilities should be considered when assessing probability and likelihood of occurrence at the facility in question.

Resources that may be useful in conducting threat and vulnerability assessments include:

- NERC Security Guideline for the Electricity Sector: Physical Security.
- NERC Security Guideline: Physical Security Response.
- ASIS International General Risk Assessment Guidelines.
- ASIS International Facilities Physical Security Measure Guideline.
- ASIS International Security Management Standard: Physical Asset Protection.
- Whole Building Design Guide - Threat/Vulnerability Assessments.

Requirement R5

This requirement specifies development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Requirement R5 specifies the following attributes for the physical security plan:

- *Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the assessment conducted in Requirement R4.*

While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site.

- *Law enforcement contact and coordination information.*

  Examples of such information may be posting 9-1-1 for emergency calls and providing substation safety and familiarization training for local and federal law enforcement, fire department, and EMS.

- *A timeline for implementing physical security resiliency or security measures specified in the physical security plan.*

  Entities have the flexibility to prioritize the implementation of the various resiliency or security measures in their security plan according to risk, resources, or other factors.

- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

  A registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various sources. Some of these sources could include the ERO, ES-ISAC, and US and/or Canadian federal agencies. This information should be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in R5.

Requirement R6

This requirement specifies review by an entity other than the TO or TOP with appropriate expertise for the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5. As with Requirement R2, the term unaffiliated means that the selected reviewing entity cannot be a corporate affiliate (*i.e.,* the reviewing entity cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Operator). A reviewing entity also cannot be a division of the Transmission Operator that operates as a functional unit.

The Responsible Entity can select from several possible entities to perform the review:

- *An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.*

  In selecting CPP and PSP for use in this standard, the drafting team believed it was important that if a private entity such as a consulting or security firm was engaged to conduct the third party review, they must tangibly demonstrate competence to conduct the review. This includes electric industry physical security experience and either of the premier security industry certifications sponsored by ASIS International. The ASIS certification program was initiated in 1977, and those that hold the CPP

certification are board certified in security management. Those that hold the PSP certification are board certified in physical security.

- *An entity or organization approved by the ERO.*
- *A governmental agency with physical security expertise.*
- *An entity or organization with demonstrated law enforcement, government, or military physical security expertise.*

A third party that contributes to the threat assessment and development of the security plan may also serve as the reviewer. As with Requirement R2, the Responsible Entity has the flexibility to work with the reviewing entity throughout (*i.e.,* concurrent with) the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5, which for some Responsible Entities may be more efficient and effective. In other words, a TO or TOP could coordinate with their unaffiliated reviewing entity to perform an evaluation of potential threats and vulnerabilities (Requirement R4) and develop a security plan (Requirement R5) concurrently with review to satisfy Requirements R4 through R6 simultaneously.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Project 2014-04

April 9, 2014

Approvals Requested
CIP-014-1 Physical Security

Prerequisite Approvals
None

Effective Date

New or Revised Standards
CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Standards for Retirement
None

Initial Performance of Periodic Requirements
The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard. Subsequent risk assessments shall be performed according to the timelines specified in CIP-014-1, Requirement R1.

The initial performance of CIP-014-1, Requirements R2 through R6, must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows:

- Requirement R2 shall be completed as follows:
    - Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard.
    - Part 2.3 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2.

- Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2.
- Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2.
- Requirement R6 shall be completed as follows:
    - Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5.
    - Part 6.3 shall be completed within 60 calendar days of Requirement R6 part 6.2.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project Overview for Project 2014-04 Physical Security

April 9, 2014

At a Glance: The Top Items to Know about Proposed Reliability Standard CIP-014-1

- Proposed CIP-014-1 Physical Security is drafted pursuant to the framework directed by the March 7, 2014, FERC order[1] directing a Physical Security Standard be filed by June 5, 2014. Consistent with the order, proposed CIP-014-1 includes a risk assessment (transmission analysis) for identification of critical facilities (as describe by FERC), evaluation of physical threats, and development of a physical security plan – with the assessment verified by a third party and the evaluation/plan reviewed by a third party.
    - The framework includes only those Transmission stations and Transmission substations (and associated primary control centers) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.
    - NERC will not request an extension of time to file the Standard, which is supported by the leadership of the Standards Committee (SC) and the Standards Drafting Team (SDT).
- Only a relatively small number of Transmission Owners and Transmission Operators will need to comply with the entire Standard.
    - Generator Operators and Generator Owners are not included as applicable entities.
    - Loss of generation connected to an applicable Transmission station or Transmission substation is considered in the risk assessment conducted by the Transmission Owners.
- The draft Standard was vetted at the April 1, 2014, NERC-sponsored technical conference and during the SDT meetings later that same week.
- The SC has approved a waiver to shorten the initial comment period to 15 days and the ballot period to the last five days of the comment period.
- There will be webinars to explain the Physical Security Standard on April 15 and April 17, 2014.
- **Your vote counts!** If you have registered in the ballot body, we need you to vote, and you must vote by the close of business on April 24, 2014. If you do not vote and quorum is not met on April 24, 2014, this will negatively impact the ability of the SDT to expeditiously move forward.
- Please review the FERC order, the draft Standard and associated guidance, the FAQ, and the RSAW posted on the 2014-04 project page. If you have any questions, please contact Stephen Crutchfield via email or by telephone at stephen.crutchfield@nerc.net or 609-651-9455 as soon as possible.

[1] *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Frequently Asked Questions
Project 2014-04 Physical Security and Draft Standard CIP-014-1

April 9, 2014

1. Why are NERC and the Standards Committee pursuing a Physical Security Reliability Standard?

On March 7, 2014, the Federal Energy Regulatory Commission (FERC or Commission) issued an order directing NERC to file one or more Reliability Standards addressing physical security of certain critical facilities by June 5, 2014.[1] The Commission stated that the physical security Reliability Standard(s) should require entities to take a least the following three steps: (1) perform a risk assessment of their systems to identify their facilities that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System; (2) evaluate the potential threats and vulnerabilities to those identified facilities; and (3) develop and implement a security plan designed to protect against physical attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Commission stated the Reliability standard(s) should also: (i) include a procedure that will ensure confidential treatment of sensitive or confidential information; (ii) include a procedure for a third party to verify the list of identified facilities and review the threat evaluation and security plan(s); and (iii) require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness.

In terms of the scope of the standard, FERC stated:

> . . . we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard.

[1] *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

NERC, the NERC Standards Committee (SC), and the Project 2014-04 Physical Security Standard Drafting Team (SDT) have been working diligently, with the assistance of stakeholders through an April 1, 2014, technical conference and SDT meetings, to draft a Reliability Standard that addresses all of the directives issued by FERC in the March 7, 2014, order. Proposed Reliability Standard CIP-014-1 is consistent with the scope of the Commission order and satisfies each directive described above.

NERC does not intend to request an extension of time for filing the proposed Reliability Standard and is committed to meeting the June 5, 2014, filing deadline. The SC and SDT leadership support this decision because they believe the framework in the FERC order is sufficiently clear to develop and file a Reliability Standard by the June 5, 2014, deadline.

2. Why does the proposed Reliability Standard's applicability section start with Transmission stations and Transmission substations identified under the medium impact criteria in CIP-002-5.1?

The SDT developed a technical guidance document appended to the end of CIP-014-1 that explains the applicability section and the requirements of the Reliability Standard in more detail.

In brief, the SDT concluded that FERC's March 7 order is reasonably understood to focus on the most critical Transmission facilities and determined that the CIP-002-5.1 bright line medium impact criteria for Transmission stations and Transmission substations was the appropriate place to start. The CIP-002-5.1 bright line medium impact criteria has been vetted with stakeholders, NERC, and FERC, and provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment under proposed Reliability Standard CIP-014-1. The SDT considered and rejected higher bright line thresholds because the SDT determined that higher bright lines could not be technically justified and may inadvertently exclude Transmission Owners that could have Transmission stations and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

The SDT understands that many of the Transmission Owners that have Transmission stations and Transmission substations that meet CIP-002-5.1's medium impact criteria are unlikely to have a Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. To that end, if a Transmission Owner's risk assessment does not identify any such Transmission stations or Transmission substations and that risk assessment has been verified by a third party, the Transmission Owner has no further obligations under the proposed Reliability Standard, except to conduct subsequent risk assessments every five years to confirm that it continues to have no such facilities.

The SDT estimates that relatively few Transmission Owners (perhaps 30 or less) will have Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. In turn, only a small number of Transmission Owners will actually have performance obligations under the entire proposed Reliability Standard. While the applicability section may include additional Transmission Owners subject to Requirements R1 and R2 only, the SDT found that the slightly broader applicability is necessary given the FERC directives, the inability to technically justify a higher bright line, and the importance of being conservative on applicability given the nature of the Reliability Standard's important topic.

The SDT also does not believe more study or time will justify another or higher bright line, given the diversity of Transmission Owners and the highly confidential nature of information related to the applicable Transmission stations and Transmission substations.

3. Why were Generator Operators and Generator Owners not included?

The SDT considered whether to include Generator Operators and Generator Owners in the proposed Reliability Standard and decided not to include them as applicable entities. First, the FERC order does not explicitly mention generation assets, and the order is reasonably understood to focus on the most critical Transmission Facilities. Second, the proposed Reliability Standard accounts for the loss of generation resources. A determination of whether a Transmission station or Transmission substation that meets CIP-002-5.1's medium impact criteria could, if rendered inoperable or damaged, result in widespread instability, uncontrolled separation, or Cascading within an Interconnection must consider the impact of the loss of generation. Specifically, the transmission analysis or analyses conducted under Requirement R1 will take into account the impact of the loss of generation. As such it is not necessary to include Generator Operators and Generator Owners to ensure that the impact of loss of generation is considered.

4. Why are only those primary control centers that have operational control of a Transmission station or Transmission substation that is identified in Requirement R1 and verified in Requirement R2 included in the proposed Reliability Standard? And what does "has operational control" mean?

The FERC order in footnote 6 specifically mentions control centers as a type of critical facility to be subject to the physical security Reliability Standard. Consistent with the order, the SDT found that it is important to include in the proposed Reliability Standard those primary control centers that have operational control over Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Specifically, the SDT concluded that in order to fully protect the Transmission stations and Transmission substations from causing

widespread instability, uncontrolled separation, or Cascading within an Interconnection as a result of a physical attack, it was imperative that these primary control centers be subject to the threat evaluation and development/implementation of physical security plans similar to the Transmission station(s) and Transmission substation(s) they operationally control.

There are two scenarios that the Standard recognizes related to identified primary control centers. In the first scenario, the registered Transmission Owner of the identified and verified Transmission station or Transmission substation is also the entity that operates the primary control center. In scenario two, the registered Transmission Owner is not the same registered entity that operates the primary control center. In this latter instance, the Transmission Operator would be the entity that operates the primary control center that has operational control of the Transmission Owner's identified and verified Transmission station or Transmission substation. Under scenario two, formal notice is required to the Transmission Operator, and that is covered in Requirement R3.

The phrase "has operational control" is specifically used to exclude from the Standard control centers that have no physical control over Transmission stations and Transmission substations, but only have the capability to monitor Transmission stations and Transmission substations, such as is the case with many, if not all, Regional Transmission Organizations and Independent System Operators. In other words, to have a primary control center in the scope of this Reliability Standard, the primary control center must have the ability to take electronic actions that can cause direct physical actions at the identified and verified Transmission station and Transmission substation, such as opening a breaker.

5. Why are unaffiliated third party verifications (of Transmission station and Transmission substation identification under Requirement R1) and unaffiliated third party reviews (of the evaluations under Requirement R4 and the security plans under Requirement R5) required in the proposed Reliability Standard?

The FERC order requires that the risk assessment be verified by an entity other than the owner or operator, and, similarly that the evaluation of threats and physical security plan be reviewed by someone other than the owner or operator. The order used the term "verify" in the context of identification of facilities and the term "review" in the context of physical threat evaluations and security plans. Therefore, the SDT decided to also use those terms in similar contexts in the proposed Reliability Standard.

a. What does unaffiliated mean?

The term unaffiliated means that the selected verifying and reviewing entities cannot be a corporate affiliate (*i.e.,* the verifying or reviewing entity cannot be an entity that corporately controls, is controlled by, or is under common control with, the Transmission Owner or

Transmission Operator). The verifying and reviewing entities also cannot be a division of the Transmission Owner or Transmission Operator (only applicable for the reviewer) that operates as a functional unit.

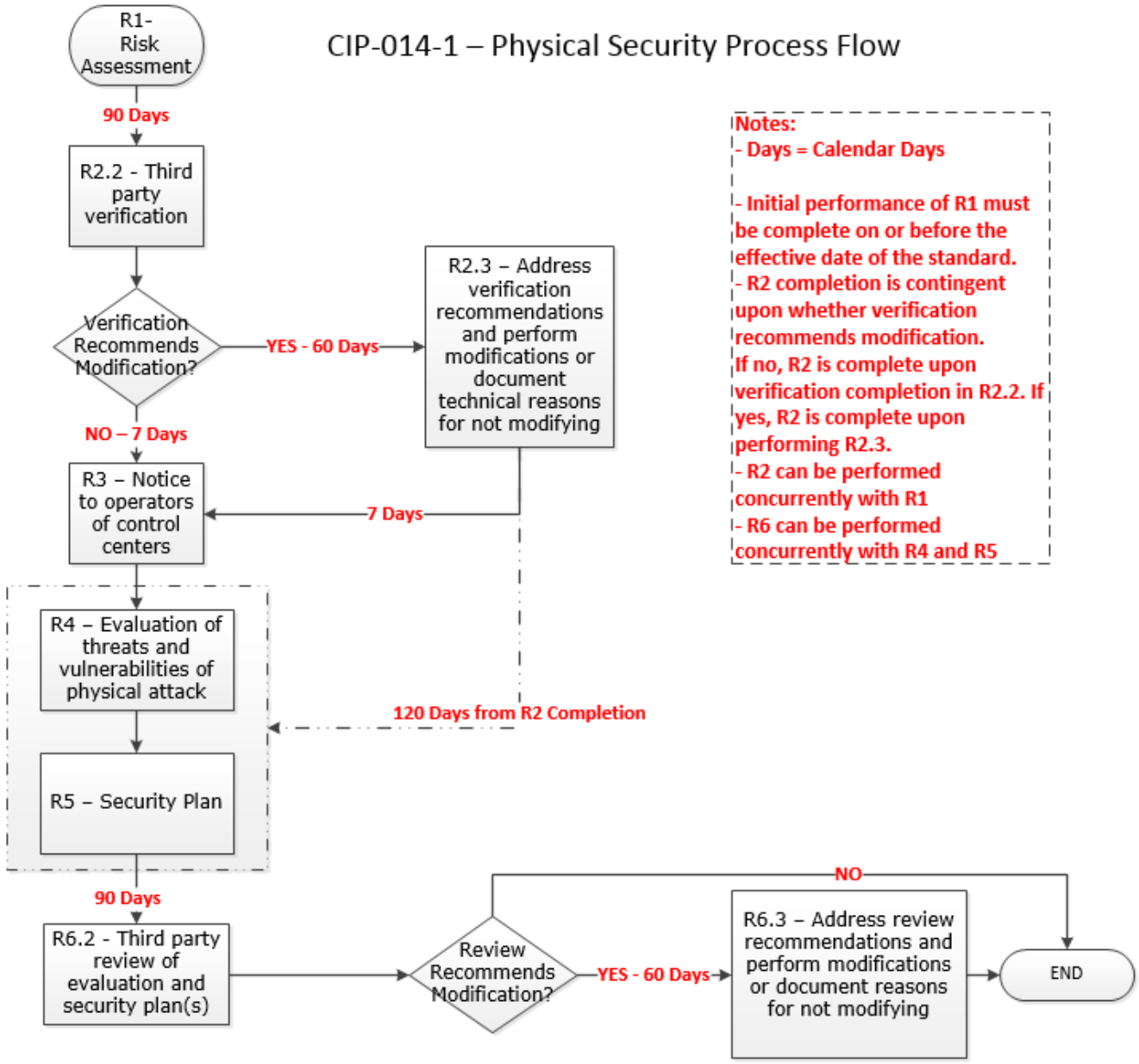
b. Why not "require" unaffiliated Reliability Coordinators, Transmission Planners, and Planning Coordinators to be the verifier of the Requirement R1 risk assessment?

The SDT considered whether to require Reliability Coordinators, Transmission Planners, and Planning Coordinators to be the verifier and decided against such a requirement. The SDT does not believe it is appropriate to require Reliability Coordinators, Transmission Planners, and Planning Coordinators to be the verifier. This conclusion is based the following: (i) unless necessary for reliability there should not be a requirement that requires one functional entity to require another functional entity to perform a task; (ii) there are sufficient entities qualified to verify the risk assessment without mandating additional tasks on Reliability Coordinators, Transmission Planners, and Planning Coordinators, and (iii) Requirement R2 provides Transmission Owners the flexibility to consider from many qualified entities.

c. Why is NERC or the Regional Entities not included as a verifier or reviewer?

Similar to reasons provided above for not mandating Reliability Coordinators, Transmission Planners, and Planning Coordinators to be the verifier, the SDT decided against a requirement that would specify NERC or Regional Entities to be the verifier or reviewer. The proposed Reliability Standard, however, does not preclude an entity from requesting NERC or its Regional Entity to be the verifying or reviewing entity under Requirements R2 and R6, respectively.

6. There are several deadlines in the proposed Reliability Standard to complete the risk assessment, third party verification, security plan(s), and third party review of the evaluation of threats and the security plan – can you illustrate this timeline?



7. Why does the proposed Reliability Standard state that the Transmission Owner can work concurrently with the verifier of the risk assessment or reviewer (and the Transmission Operator of the review) of the evaluation of threats and the security plan(s)?

The SDT recognized the value, effectiveness, and efficiency that may result in the Transmission Owner working side-by-side with its verifier, and the Transmission Owner and Transmission Operator, respectively, working side-by-side with its reviewer. Thus, for example, the Transmission Owner may first perform its Requirement R1 risk assessment for identification of Transmission stations and Transmission substations on its own, and then, in a second step, have the verifier conduct its verification of the risk assessment. If more efficient, the Transmission Owner may combine those steps by working side-by-side with the verifying entity to complete the risk assessment and the verification at the same time. It is expected that the selection of this concurrent approach will lessen misunderstandings, and likely be more effective and efficient. This side-by-side approach is equally applicable for conducting the risk assessment and verification under Requirements R1 and R2 and the evaluation of threats, development and implementation of physical security plan(s), and review under Requirements R4 through R6.

8. Given that the TO and TOP will be subject to unaffiliated third party review, does that change how compliance and enforcement will be conducted for this proposed Reliability Standard?

The SDT expects auditors will use their professional judgment to assess the third party reviews and rely on them to avoid duplication of efforts as is permitted by auditing standards. However, some degree of auditor due diligence related to the third party review is necessary to provide a sufficient basis for reliance on the work of others. Documentation regarding the qualification of third parties and the scope and nature of their reviews will help facilitate reliance for compliance auditors. The Notes to Auditor sections of the draft RSAW associated with proposed CIP-014-1 supports the concept of considering the effect of third party verifications and reviews on audit risk and related rigor of compliance procedures.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2014-04 Physical Security

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments on the draft CIP-014-1 Reliability Standard. The electronic comment form must be completed by 8:00 p.m. Eastern on **Thursday, April 24, 2014.**

If you have questions please contact Stephen Crutchfield via email or by telephone at or (609) 651-9455.

The project page may be accessed by clicking here.

Background Information

On March 7, 2014, the Federal Energy Regulatory Commission (FERC) issued an order directing NERC to submit for approval, within 90 days of the order, one or more Reliability Standards to address physical security risks and vulnerabilities of critical facilities on the Bulk Power System (BPS).[1]

In the order, FERC stated that the proposed Reliability Standard(s) should require entities to take a least the following three steps:

- Perform a risk assessment to identify facilities that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or cascading failures on the BPS.
- Evaluate the potential threats and vulnerabilities to those identified facilities.
- Develop and implement a security plan designed to protect against physical attacks to those identified facilities based on the assessment of the potential threats and vulnerabilities to their physical security.

Additionally, FERC directed that the proposed Standard(s) should also: (1) include a procedure that will ensure confidential treatment of sensitive or confidential information; (2) include a procedure for a third party to verify the list of identified facilities and allow the verifying entity, as well as FERC, to add or remove facilities from the list of critical facilities; (3) include a procedure for a third party to review the evaluation of threats and vulnerabilities and the security plan; and (4) require that the identification of the facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. The proposed Physical Security Reliability Standard(s) must be filed with FERC by June 5, 2014.

In response to the order, NERC staff and the Standards Committee (SC) worked together in order to develop an action plan for meeting the June 5, 2014 filing deadline. The SC approved several waivers to facilitate meeting the required timelines and seated the Standard Drafting Team (SDT) on March 21, 2014.

[1] *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

This posting solicits comment on proposed Reliability Standard CIP-014-1 Physical Security. The proposed standard responds to the directives from the FERC order, and a summary of those directives with explanation of how the approach addresses them is available in the "Consideration of Issues and Directives" document on the project page.

You do not have to answer all questions below. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained. Due to the expected volume of comments, the SDT asks that commenters consider consolidating responses and endorsing comments provided by another.

Questions

1. **Applicability**: The applicability of proposed CIP-014-1 starts with those Transmission Owners that own Transmission facilities that meet the bright line criteria in Reliability Standard CIP-002-5.1 for a "medium impact" rating. The drafting team did not modify these criteria in their use under CIP-014-1, as they have been previously approved by stakeholders, NERC, and FERC. The SDT sought to ensure that entities could apply the same set of criteria to assist with identification of facilities under CIP Version 5 and proposed CIP-014-1. The team determined that slightly modified criteria could possibly result in confusion in application. The drafting team considered several other alternatives to refine the scoping in the applicability section, such as a particular kV threshold in addition to the other criteria; however, after significant discussion, the team found no technical or reliability basis for providing such limitiation. Importantly, by virtue of application of Requirement R1, the scope of the standard only applies to Transmission Owners that have Transmission stations and Transmission substations that meet the "medium impact" criteria from CIP-002-5.1, and their associated primary control centers. Furthermore, the standard drafting team expects many who are "applicable" to the standard will not identify facilities through their Requirement R1 risk assessment and Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. In those cases, the entity only performs Requirements R1 through R2. When that results in a null set, Requirement R1 additionally provides that subsequent risk assessments may occur less frequently. Similarly, while Transmission Operators are also listed in the applicability section, by virtue of application of the requirements, only certain Transmission Operators that are notified under the standard's Requirement R3 have obligations under the standard. Do you agree with the applicability section? If not, please provide specific recommendations, ensuring to articulate how your suggested approach would not limit the applicability in such a manner as to inadvertently miss a facility that should be covered under the standard as specified in the FERC order on physical security.

☐ Yes
☐ No

Comments:

2. **Requirements R1 through R3**: The first three requirements of CIP-014-1 require Transmission Owners to: (1) perform risk assessments to identify through transmission planning analysis those Transmission stations and Transmission substations that meet the "medium impact" criteria from CIP-002-5.1, and their associated primary control centers, that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; (2) arrange for a third party verification (as directed in the order) of the identifications; and (3) notify certain Transmission Operators of identified primary control centers that operationally control the identified and verified Transmission stations and Transmission substations. The requirements provide the periodicity for satisfying these obligations. Only an entity that owns or operates one or more of the identified facilities has further obligations in Requirements R4 through R6. If an entity identifies a null set after applying Requirements R1 through R2, the rest of the standard does not apply. Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security.

☐ Yes
☐ No

Comments:

3. **Requirements R4 through R6**: The final three requirements of CIP-014-1 require (1) the evaluation of potential threats and vulnerabilities of a physical attack to the facilities identified and verified according to the earlier requirements, (2) the development and implementation of a security plan(s) designed in response to the evaluation, and (3) a third party review of the evaluation and security plan(s) (as directed in the order). Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security.

☐ Yes
☐ No

Comments:

4. Do you have input on other areas of the standard or implementation plan not discussed in the questions above? If so, please provide them here, recognizing that you do not have to provide a response to all questions. Please limit your response to 300 words or less.

☐ Yes
☐ No

Comments:

Consideration of Issues and Directives

Project 2014-04 - Physical Security

April 9, 2014

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
6. The Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the Bulk-Power System. First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities." A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards. Instead, the Commission is directing NERC to develop Reliability	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that each Transmission Owner perform a risk assessment of its Transmission stations and substations that meet the criteria in Attachment 1 of CIP-002-5.1 for a Medium Impact rating to identify which of those Transmission stations and substations, if rendered inoperable or damaged as a result of a physical attack, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Transmission Owner must also identify the primary control centers that operationally controls each identified Transmission station or Transmission substation. The standard drafting team (SDT) determined that the CIP-002-5 bright line was appropriate because it has been vetted with stakeholders, and approved by NERC and FERC. The SDT concluded it was a technically sound basis to determine which Transmission Owners should conduct the risk assessment. If the Transmission Owner does not have any Transmission stations or substations that meet the Medium Impact rating, it is not subject

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System and thereby warrant the directive imposed here.		to the proposed Reliability Standard and, in turn, would not have to conduct the risk assessment. Consistent with the Commission's directive, Requirement R1 does not require a specific methodology for identifying facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; rather, the requirement mandates that the risk assessment shall consist of a transmission analysis or transmission analyses to ensure that the methodology is based on objective analysis, technical expertise, and experienced judgment. Lastly, Requirement R1 identifies the periodicity for conducting the risk assessments.
7. Issuance of this directive will help provide for the resiliency and reliable operation of the Bulk-Power System. To that end, the proposed Reliability Standards should allow owners or operators to consider resilience of the grid in the risk assessment when identifying critical facilities, and the elements that make up those facilities, such as transformers that typically require significant time to repair or replace. As part of this process, owners or operators may consider elements of resiliency such as how the system is designed,	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 provides Transmission Owners the flexibility to consider the resilience of their system when conducting their risk assessments. As noted above, Requirement R1 does not require a specific methodology for identifying their critical facilities and, in turn, allows an entity to use a methodology that considers how their system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
operated, and maintained, and the sophistication of recovery plans and inventory management.		
8. In the second step, the Reliability Standards should require owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities. The threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target. Thus, the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R4 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that each Transmission Owner and Transmission Operator that owns or operates facilities identified in accordance with Requirement R1 (and verified under Requirement R2) conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive to "tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated," Requirement R4 states that the evaluation must consider: (1) the unique characteristics of the identified facilities; (2) prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and (3) intelligence or threat warnings from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U. S. federal and/or Canadian governmental agencies, or their successors.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Consistent with the Commission's statement that NERC should consider requiring owners and operators of identified facilities to consult with entities with appropriate expertise, Requirement R6 requires applicable Transmission Owners and Transmission Operators to select a third party to review their evaluation. This review may occur concurrently with or after the evaluation.
9. Third and finally, the Reliability Standards should require those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Reliability Standards themselves need not dictate specific steps an entity must take to protect against attacks on the identified facilities. However, the Reliability Standards need to require that owners or operators of identified critical facilities have a plan that results in an adequate level of protection against the potential physical threats and vulnerabilities they face at the identified critical facilities.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R5 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that each Transmission Owner and Transmission Operator that owns or operates facilities identified in accordance with Requirement R1 (and verified under Requirement R2) develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive, Requirement R5 does not dictate specific steps an entity must take to protect against attacks on the identified facilities but requires applicable entities to develop a security plan that includes the following attributes to help ensure an adequate level of protection: (1) resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4; (2) law enforcement contact and

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		coordination information; (3) a timeline for implementing the physical security enhancements and modifications specified in the physical security plan; and (4) provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).
10. All three steps of compliance with the Reliability Standard described above could contain sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure. Therefore, NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information that is needed to ensure compliance with the Reliability Standards.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	To protect confidential or sensitive information, the Compliance Monitoring section of the standard provides that evidence demonstrating compliance with the standard must be retained at the applicable entities' facilities. Additionally, Requirements R2 and R6 require applicable entities to implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information exchanged with the third party verifier under Requirement R2 or the reviewing entity under Requirement R6. These steps will help ensure that lists of critical facilities or other sensitive documents remain confidential.
11. In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a	*Reliability Standards for Physical Security*	Requirements R2 and R6 respond to this directive. Under Requirement R3 Transmission Owners must have an unaffiliated entity verify the risk assessment performed under Requirement R1. The third party verifier must be either (1) a registered

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Reliability Coordinator, or another entity. The Reliability Standards should include a procedure for the verifying entity, as well as the Commission, to add or remove facilities from an owner's or operator's list of critical facilities. Similarly, the determination of threats and vulnerabilities and the security plan should also be reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise. Finally, the Reliability Standards should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. NERC should establish a timeline for when such reevaluations should occur.	*Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Planning Coordinator, Transmission Planner, or Reliability Coordinator; or (2) an entity that has transmission planning or analysis experience. The requirement provides that the verifying entity shall either verify the Transmission Owner's risk assessment or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). The verification may occur concurrently with the Requirement R1 risk assessment but must be completed within 90 calendar days of the risk assessment. The Transmission Owner is required to either modify its identification based on the verifier's recommendation or, if it disagrees with the verifier's recommendations, document the technical basis for not modifying its identification. Similarly, under Requirement R6, applicable Transmission Owners and Operators must have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The reviewing entity must be either (1) an entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification; (2) an entity or organization approved by the ERO; (3) a governmental agency with physical security expertise; or (4) an entity or organization with demonstrated law

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		enforcement, government, or military physical security expertise. The third party review must be completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The applicable Transmission Owners and Transmission Operators are required to either modify their evaluation or security plan(s) consistent with the reviewer's recommendations or, if they disagree with the recommendations, document the reasons for not modifying. Consistent with the directive to establish a timeline for periodic reevaluation of the identification of facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection, the assessment of the potential risks and vulnerabilities, and the security plans, the standard provides that Requirement R1 risk assessment should be performed at least once every 30 calendar months for those Transmission Owners that identified facilities in their previous risk assessment and once every 60 calendar months for those Transmission Owners that did not identify facilities in their previous risk assessment. Upon completion of each subsequent risk assessment, the applicable entities must satisfy the obligations under the remaining requirements.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
12. Under the Reliability Standards, we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard. We also recognize that the industry has engaged in longstanding efforts to address the physical security of its critical facilities. Thus, NERC should develop an implementation plan that requires owners or operators of the Bulk-Power System to implement the Reliability Standards in a timely fashion, balancing the importance of protecting the Bulk-Power System from harm while giving the owners or operators adequate time to meaningfully implement the requirements. NERC should file the plan with the Reliability Standards for Commission review.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	The proposed Implementation Plan addresses this directive. As provided in the Implementation Plan, the standard becomes effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows: - Requirement R2, Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard. Requirement R2, Part 2.3 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2. - Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		- Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2. - Requirement R6, Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5. Requirement R6, Part 6.3 shall be completed within 60 calendar days of Requirement R6 part 6.2.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Reliability Standard Audit Worksheet[1]

CIP-014-1 – Physical Security

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements ***[RSAW developer to insert correct applicability]***

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1												X[3,4]			
R2												X[3,4]			
R3												X[3,4]			
R4												X[3,4]	X[4]		
R5												X[3,4]	X[4]		
R6												X[3,4]	X[4]		

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC orders, and the language included in this document, FERC orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

[3] Applicability is further defined to owners of transmission Facilities operated at 500 kV or higher (see section 4.1.1.1 of the Standard) and owners of certain transmission Facilities operating between 200 kV and 499 kV where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations, per section 4.1.1.2 of the Standard. In addition, sections 4.1.1.3 and 4.1.1.4 bring additional transmission Facilities identified as either critical to the derivation of Interconnection Reliability Operating Limits and Nuclear Plant Interface, respectively, within the purview of the standard. Please see the referenced sections of the Standard for additional details regarding applicability of the Requirements to Transmission Owners.

[4] Facilities regulated by the Nuclear Regulatory Commission or Canadian Nuclear Safety Commission are not subject to this Standard.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

DRAFT

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

DRAFT

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Note to Auditors Concerning Third Party Verifications and Reviews

Requirements R2 and R6 prescribe, respectively, unaffiliated third party verifications for Requirement R1 and unaffiliated third party reviews for Requirements R4 and R5. Auditors are encouraged to rely on the verifications and reviews performed in cases where the verifying or reviewing entities are qualified, unaffiliated with the audited entity, and the scope of their verification or review is clear. The concept of reliance means using the work of others to avoid duplication of efforts and is consistent with recognized professional auditing standards, which are required for Compliance Audits per NERC's Rules of Procedure. Reliance in the context of this Reliability Standard means using the Requirement R2 verifications and Requirement R6 reviews to reduce audit risk and the related rigor of audit testing for Requirements R1, R4, and R5. However, in cases where the verifying or reviewing entity lacks the qualifications specified in Requirement R2 for verifications or Requirement R6 for reviewers, the required unaffiliation from the audited entity, or where the scope of the third party entity's verification or review is unclear, auditors may need to apply audit testing of Requirements R1, R4, or R5. For this reason, the Evidence Requested and Compliance Assessment Approach Sections are still present in this RSAW for Requirements R1, R4, and R5. We anticipate those sections will also facilitate expectations for entities and their unaffiliated third party verifiers and reviewers, assist Electric Reliability Organization (ERO) auditors to understand the audit procedures applied by unaffiliated third party verifiers and reviewers, and provide transparency between ERO auditors and Industry, should circumstances require audit testing of Requirements R1, R4, or R5. Further, it is an objective of the ERO to have transparent Evidence Requests and Compliance Assessment Approaches for every enforceable standard, whether they are in audit scope or not.

DRAFT

R1 Supporting Evidence and Documentation

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1.The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify any Transmission station(s) and Transmission substation(s) that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2)one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or
- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1.

Registered Entity Response (Required):

Question: As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1? ☐ Yes ☐ No

☐ This entity does not have any applicable Transmission stations/substations.

☐ Other: [Provide explanation below]

[Include additional information regarding the question here, including the type of response and format of the response requested, as appropriate.]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R1) Provide the current and the immediately preceding risk assessments conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant).
(R1) List of existing Transmission stations/substations that meet the criteria specified in Section 4.1.1.
(R1) List of Transmission stations/substations planned in the next 24 months that meet criteria specified in Section 4.1.1.
(R1 Part 1.2) List of primary control centers that operationally control each identified Transmission station/substation.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R1

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R1) Review entity's process for determining Transmission stations/substations subject to identification in accordance with Requirement R1, including weighting described in Section 4.1.1.2.
	(R1) Review entity's risk assessment process to determine the Transmission stations/substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection.
	(R1) Ensure entity's risk assessment process includes Transmission stations/substations planned in the next 24 months.
	(R1) Ensure a risk assessment was performed for each Transmission station/substation meeting applicability described in Section 4.1.

	(R1 Part 1.1) If applicable, review any prior risk assessments and verify whether or not Transmission stations/substations were identified.
	(R1 Part 1.1) Review evidence that risk assessment was performed and verify that it occurred within the past 30 months where items were identified in the previous risk assessment and 60 months where no items were identified in the previous risk assessment.

Note to Auditor: Review entity's answer to the above Question and if the auditor can verify the answer is 'no,' Requirements R3-R6 do not apply and no further audit testing of Requirements R3-R6 is necessary.

See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement.

Auditor Notes:

DRAFT

R2 Supporting Evidence and Documentation

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1.

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator;
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated verifying entity shall either verify the Transmission Owner's risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a s Transmission station or Transmission substation::

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information exchanged with the unaffiliated verifying entity.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R2) Dated evidence of third party verification of the entity's risk assessment performed under Requirement

R1.
(R2 Part 2.1) Documented qualifications of the verifying party.
(R2 Part 2.3) Recommendations, if any, of the verifying party related to Requirement R1 risk assessments.
(R2 Part 2.3) Documentation of modifications and implementation of recommendations or technical basis for not implementing recommendations of the verifying party.
(R2 Part 2.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R2

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R2) Review evidence of third party verification of the entity's risk assessment and verify the following:
	(R2 Part 2.1) The reviewing entity is registered in accordance with Part 2.1 or has transmission planning or analysis experience.
	(R2 Part 2.2) Verification was completed with 90 calendar days of risk assessment.
	(R2 Part 2.3) Verifying entity's recommendations, if any, were used to modify the entity's Requirement R1 identification or the technical basis for not modifying the Requirement R1 identification is documented within 60 calendar days of completion of the verification.
	(R2 Part 2.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between the entity and third party were implemented.
Note to Auditor See Guidelines and Technical Basis section of the standard and Rationale for Requirement R2 associated with the Standard for additional details regarding the term 'unaffiliated.' The third party verification may occur concurrent with or after the risk assessment performed under Requirement R1.	

Auditor Notes:

DRAFT

R3 Supporting Evidence and Documentation

R3. For the primary control center(s) identified by the Transmission Owner according to Requirement R1 and verified according to Requirement R2 that is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2.

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Registered Entity Response (Required):

Question: Are any primary control centers identified in Requirement R1, Part 1.2 not under operational control of your NERC registration? ☐ Yes ☐ No

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R3) If applicable, dated communications with Transmission Operators demonstrating notification and the date of completion of Requirement R2.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R3

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R3) For each applicable primary control center identified in Requirement R1 Part 1.2 not under the control of the entity's registration, verify notification exists and contains the date of completion of Requirement R2.
	(R3 Part 3.1) For each Transmission station/substation removed under Part 3.1, ensure the responsible Transmission Operator was notified of the removal within seven calendar days of removal from identification.
Note to Auditor: Note the entity's response to the above Question. If auditor can verify the entity's answer of 'No,' then Requirement R3 is not applicable and no further audit testing is required.	

Auditor Notes:

.

R4 Supporting Evidence and Documentation

R4. Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R4) A description of the entity's process for executing the evaluation prescribed in Requirement R4.
(R4) Dated evidence of the evaluation prescribed in Requirement R4.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R4

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R4) Review evidence of evaluation and verify it considers the following:
	(R4) Potential threats as described in Requirement R4.
	(R4 Part 4.1) Unique characteristics as described in Requirement R4 Part 4.1.
	(R4 Part 4.2) Prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events.
	(R4 Part 4.3) Intelligence or warnings as described in Part 4.3.
Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement. Auditor should cross reference the Transmission stations/substations and primary Control Centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 to ensure it is complete.	

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following attributes:

5.1. Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for implementing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating implementation of the physical security plan.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R5) Dated physical security plan(s).

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R5

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R5) Review evidence and verify the physical security plan(s) covers the Transmission stations/substations and primary controls identified in Requirements R1 and/or R2, and verify plan was implemented within 120 calendar days following the completion of Requirement R2. In addition, verify the plan includes the following attributes:
	(R5 Part 5.1) Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of Requirement R4.
	(R5 Part 5.2) Law enforcement contact and coordination information.
	(R5 Part 5.3) A timeline for implementing physical security enhancements and modifications specified in the physical security plan.
	(R5 Part 5.4) Provisions to evaluate evolving physical threats, and their corresponding security measures in accordance with R5 Part 5.4
	(R5) Verify implementation of physical security plan(s). See 'Note to Auditor' for details.

Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement.

Auditor should cross reference the Transmission stations/substations and primary Control Centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 and the security plan(s) prescribed in Requirement R5 to ensure the plan addresses vulnerabilities that would facilitate physical attacks that have a high probability or likelihood of occurrence.

Requirement R5 includes implementation of the security plan(s), which is not within the scope of the third party review described in Requirement R6. Auditors can gain reasonable assurance security plan(s) was/were implemented by determining if specific actions prescribed by the plan(s) have taken place within the timelines established by the plan(s). For example, if the plan calls for certain procedures to occur, then auditors could ask for evidence demonstrating the procedure has been implemented within the timeline established in the security plan. Also, if the plan calls for construction of a barrier, an auditor could verify evidence that such a barrier was constructed in accordance with the entity's timeline. As auditors should obtain reasonable, not absolute, assurance the plan(s) was/were implemented, testing implementation on a sample basis may be appropriate.

Auditor Notes:

DRAFT

R6 Supporting Evidence and Documentation

R6. Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

6.1..1. An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.

6.1..2. An entity or organization approved by the ERO.

6.1..3. A governmental agency with physical security expertise.

6.1..4. An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated reviewing entity recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its security plan(s) consistent with the recommendation; or
- Document the reason for not modifying the security plan(s) consistent with the recommendation

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information exchanged with the unaffiliated reviewing entity.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3..

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R6) Dated Evidence of unaffiliated third party review of entity's Requirement R4 evaluation and Requirement R5 security plan(s).
(R6 Part 6.1) Evidence that reviewing entity staff meets qualifications identified in Part 6.1.
(R6 Part 6.3) Recommendations of reviewing party related to Requirement R4 evaluation and Requirement R5 security plan.
(R6 Part 6.3) Dated documentation of modifications and implementation of recommendations or reasons and compensating mitigating measures for not implementing recommendations of the reviewing party.
(R6 Part 6.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R6

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R6) Review evidence and verify the physical security plan(s) and the Requirement R4 evaluation have been reviewed by an unaffiliated third party. Also, review evidence and verify the following:
	(R6 Part 6.1) Reviewing party has the qualifications identified in Part 6.1.
	(R6 Part 6.2) Review is dated within 90 calendar days of completion of the Requirement R5 security plan.
	(R6 Part 6.3) Reviewing entity recommended changes to security plan(s) were made by entity or the reason(s) for not making the change(s) was/were documented within 60 calendar days of the completion of the unaffiliated third party review.
	(R6 Part 6.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between entity and third party were implemented.
Note to Auditor: The third party review may occur concurrent with or after the evaluation performed under Requirement R4 or the security plan develop under Requirement R5. See Guidelines and Technical Basis associated with the Standard for additional details related to qualifications of reviewing entities that may inform audited entities selection of a reviewing entity.	

Auditor Notes:

Additional Information:

Reliability Standard

The RSAW developer should provide the following information without hyperlinks. Update the information below as appropriate.

The full text of CIP-014-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology [If developer deems reference applicable]

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language [Developer to ensure RSAW has been provided to NERC Legal for links to appropriate Regulatory Language – See example below]

E.g. FERC Order No. 742 paragraph 34: "Based on NERC's…….

E.g. FERC Order No. 742 Paragraph 55, Commission Determination: "We affirm NERC's…….

Selected Glossary Terms [If developer deems applicable]

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
1	04/09/2014	Physical Security RSAW Task Force	New Document

[i] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

DRAFT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security
CIP-014-1

Formal Comment Period Now Open through April 24, 2014
Ballot Pools Forming Now through April 19, 2014

This email distribution list may include individuals subject to ex parte communication restrictions pursuant to Rule 2201 of the Federal Energy Regulatory Commission's regulations governing off-the-record communications (18 C.F.R. § 385.2201 (2014)). Please refrain from using this distribution list for any substantive communications related to Project 2014-04, Physical Security.

In an order issued March 7, 2014, the Federal Energy Regulatory Commission directed NERC to file a physical security standard within 90 days of the order (*i.e.*, by June 5, 2014). On March 21, 2014, the NERC Standards Committee (SC) authorized a waiver of the standard development process, in accordance with Section 16 of the Standard Processes Manual, to meet this pending regulatory deadline. The SC approved to shorten this comment period from 45 days to 15 calendar days, with a concurrent ballot conducted during the last 5 days of the comment period. The waiver also provided for ballot pool formation to begin immediately upon approval of the waiver, with closure of the ballot pool 10 days after the initial formal comment and ballot period begins. (Sections 4.7-4.9)

Now Available

A 15-day formal comment period for **CIP-014-1 – Physical Security** is open through **8 p.m. Eastern on Thursday, April 24, 2014.**

If you have questions please contact Stephen Crutchfield via email or by telephone at (609) 651-9455.

Background information for this project can be found on the project page. Please refer to the 1-page Project Overview to learn more about the Physical Security standard and project at a glance.

Instructions for Commenting

Please use the electronic form to submit comments on the standard. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Instructions for Joining Ballot Pool

Ballots pools are being formed for Project 2014-04 – Physical Security and the associated non-binding poll on this project. Registered Ballot Body members must join the ballot pools to be eligible to vote in the balloting and submittal of an opinion for the non-binding poll of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs). Registered Ballot Body members may join the ballot pools at the following page: Join Ballot Pool

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list servers for this project are:

Initial Ballot: bp-2014-04_CIP-014-1_in@nerc.com
Non-Binding poll: bp-2014-04_CIP-014-1_NB_in@nerc.com

Next Steps

An initial ballot for the standard and non-binding poll of the associated VRFs and VSLs will be conducted **April 20-24, 2014.**

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security
CIP-014-1

Formal Comment Period Now Open through April 24, 2014
Ballot Pools Forming Now through April 19, 2014

This email distribution list may include individuals subject to ex parte communication restrictions pursuant to Rule 2201 of the Federal Energy Regulatory Commission's regulations governing off-the-record communications (18 C.F.R. § 385.2201 (2014)). Please refrain from using this distribution list for any substantive communications related to Project 2014-04, Physical Security.

In an order issued March 7, 2014, the Federal Energy Regulatory Commission directed NERC to file a physical security standard within 90 days of the order (*i.e.*, by June 5, 2014). On March 21, 2014, the NERC Standards Committee (SC) authorized a waiver of the standard development process, in accordance with Section 16 of the Standard Processes Manual, to meet this pending regulatory deadline. The SC approved to shorten this comment period from 45 days to 15 calendar days, with a concurrent ballot conducted during the last 5 days of the comment period. The waiver also provided for ballot pool formation to begin immediately upon approval of the waiver, with closure of the ballot pool 10 days after the initial formal comment and ballot period begins. (Sections 4.7-4.9)

Now Available

A 15-day formal comment period for **CIP-014-1 – Physical Security** is open through **8 p.m. Eastern on Thursday, April 24, 2014.**

If you have questions please contact Stephen Crutchfield via email or by telephone at (609) 651-9455.

Background information for this project can be found on the project page. Please refer to the 1-page Project Overview to learn more about the Physical Security standard and project at a glance.

Instructions for Commenting

Please use the electronic form to submit comments on the standard. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Instructions for Joining Ballot Pool

Ballots pools are being formed for Project 2014-04 – Physical Security and the associated non-binding poll on this project. Registered Ballot Body members must join the ballot pools to be eligible to vote in the balloting and submittal of an opinion for the non-binding poll of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs). Registered Ballot Body members may join the ballot pools at the following page: Join Ballot Pool

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list servers for this project are:

Initial Ballot: bp-2014-04_CIP-014-1_in@nerc.com
Non-Binding poll: bp-2014-04_CIP-014-1_NB_in@nerc.com

Next Steps

An initial ballot for the standard and non-binding poll of the associated VRFs and VSLs will be conducted **April 20-24, 2014.**

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security
CIP-014-1

Initial Ballot and Non-Binding Poll Results

Now Available

An initial ballot for **CIP-014-1 – Physical Security** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels concluded at **8 p.m. Eastern on Thursday, April 24, 2014.**

The standard achieved a quorum and sufficient affirmative votes for approval. Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results for the ballot.

Approval	Non-Binding Poll Results
Quorum: 88.60%	Quorum: 84.62%
Approval: 82.07%	Supportive Opinions: 83.83%

Background information for this project can be found on the project page.

Next Steps

The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the standard. If the standard does not show the need for significant revisions, it will proceed to a final ballot

For information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller (via email), Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results	
Ballot Name:	2014-04_CIP-014-1
Ballot Period:	4/20/2014 - 4/24/2014
Ballot Type:	Initial
Total # Votes:	404
Total Ballot Pool:	456
Quorum:	**88.60 % The Quorum has been reached**
Weighted Segment Vote:	82.07 %
Ballot Results:	**The ballot has closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	121	1	85	0.787	23	0.213	0	2	11
2 - Segment 2	8	0.6	6	0.6	0	0	0	1	1
3 - Segment 3	105	1	79	0.919	7	0.081	0	7	12
4 - Segment 4	38	1	27	0.871	4	0.129	0	2	5
5 - Segment 5	101	1	70	0.843	13	0.157	0	5	13
6 - Segment 6	60	1	49	0.907	5	0.093	0	0	6
7 - Segment 7	5	0.2	2	0.2	0	0	0	0	3
8 - Segment 8	6	0.6	2	0.2	4	0.4	0	0	0
9 - Segment 9	3	0.1	1	0.1	0	0	0	2	0

10 - Segment 10	9	0.6	4	0.4	2	0.2	0	2	1
Totals	**456**	**7.1**	**325**	**5.827**	**58**	**1.273**	**0**	**21**	**52**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke		
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Negative	COMMENT RECEIVED
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Hudson Gas & Electric Corp.	Frank Pace	Negative	COMMENT RECEIVED
1	Central Iowa Power Cooperative	Kevin J Lyons	Negative	COMMENT RECEIVED
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	COMMENT RECEIVED
1	Cleco Power LLC	Danny McDaniel	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	East Kentucky Power Coop.	Amber Anderson	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Edison Electric Institute	David Batz	Affirmative	
1	El Paso Electric Company	Pablo Onate	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Negative	COMMENT RECEIVED
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	COMMENT RECEIVED
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Negative	COMMENT RECEIVED
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	

1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Negative	COMMENT RECEIVED
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	COMMENT RECEIVED
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Brett Holland)
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John Chin	Abstain	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Los Angeles Department of Water & Power	John Burnett	Affirmative	
1	Lower Colorado River Authority	Martyn Turner		
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Negative	COMMENT RECEIVED
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Please see comments submitted by me on behalf of the New Brunswick Power Corporation)
1	Network & Security Technologies	Nicholas Lauriat		
1	New York Power Authority	Bruce Metruck	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Negative	COMMENT RECEIVED
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	COMMENT RECEIVED
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Chelan County	Chad Bowman	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	

1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Southwestern Power Administration	Angela L Summer	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES/SPP)
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blue Ridge Electric	James L Layton		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	Central Hudson Gas & Electric Corp.	James J McCloskey		
3	City of Anaheim Public Utilities Department	Dennis M Schmidt	Abstain	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Mark Schultz	Abstain	

3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Negative	COMMENT RECEIVED
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Abstain	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	East Kentucky Power Coop.	Patrick Woods	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
3	El Paso Electric Company	Rhonda Bryant	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	Entergy	Kevin Weber	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes		
3	Kansas City Power & Light Co.	Joshua D Bach		
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Mace D Hunter	Affirmative	
3	Lee County Electric Cooperative	David A Hadzima		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Negative	COMMENT RECEIVED
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	National Rural Electric Cooperative Association	Patricia E Metro	Abstain	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	North Carolina Municipal Power Agency #1	Kathy Moyer	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mahmood Safi - OPPD)
3	Orange and Rockland Utilities, Inc.	David Burke		

3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Negative	COMMENT RECEIVED
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Chelan County	Steve Wickel	Affirmative	
3	Public Utility District No. 1 of Clallam County	Doug Adams	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Southern Indiana Gas and Electric Co.	Fred Frederick	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	SUPPORTS THIRD PARTY COMMENTS - (Please see TVA's comments submitted through the electronic comment form)
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott		
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave		
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell	Affirmative	
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Negative	COMMENT RECEIVED
4	DTE Electric	Daniel Herring	Affirmative	
4	Eugene Water & Electric Board	Dean Ahlsten	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	COMMENT RECEIVED
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas	Affirmative	
4	Garkane Energy	Mike Avant		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Negative	COMMENT RECEIVED
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative	Barry R. Lawson	Abstain	

	Association			
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
4	Southern Minnesota Municipal Power Agency	Richard L Koch		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	Acciona Energy North America	George E Brown	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke		
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Negative	SUPPORTS THIRD PARTY COMMENTS - (Black Hills Corporation on behalf of 4 entities)
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Calpine Corporation	Hamid Zakery	Abstain	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Negative	COMMENT RECEIVED
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	East Kentucky Power Coop.	Stephen Ricker	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	El Paso Electric Company	Gustavo Estrada	Affirmative	

5	Electric Power Supply Association	John R Cashin		
5	Empire District Electric Co.	mike I kidwell	Affirmative	
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Hydro-Québec Production	Roger Dufresne	Negative	SUPPORTS THIRD PARTY COMMENTS - (in support of HQT)
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lafayette Utilities System	Jamie B Webb		
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Manitoba Hydro	Chris Mazur	Negative	COMMENT RECEIVED
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	COMMENT RECEIVED
5	Ontario Power Generation Inc.	David Ramkalawan	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Chelan County	John Yale	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Illinois Power Coop.	Alvis D Lanton		
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	

5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	El Paso Electric Company	Luis Rodriguez	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson		
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw		
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Negative	COMMENT RECEIVED
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley		
6	New York Power Authority	Saul Rojas	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative	
6	Northern California Power Agency	Steve C Hill	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mahmood Safi)
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp	Affirmative	
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	

6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	COMMENT RECEIVED
6	Westar Energy	Grant L Wilkerson		
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Wisconsin Public Service Corp.	David Hathaway	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Eastman Chemical Company	David L Moore		
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Praxair Inc.	David Meade		
7	Siemens Energy, Inc.	Frank R. McElvain	Affirmative	
7	Valero Services, Inc.	Lee W Morris		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner	Negative	COMMENT RECEIVED
8		David L Kiguel	Negative	COMMENT RECEIVED
8	Foundation for Resilient Societies	William R Harris	Negative	COMMENT RECEIVED
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	COMMENT RECEIVED
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Idaho State Public Utilities Commission	Johanna Bell	Affirmative	
9	National Association of Regulatory Utility Commissioners	Jerry M Maio	Abstain	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC CIPC comments)
10	Southwest Power Pool RE	Bob Reynolds	Negative	COMMENT RECEIVED
10	Texas Reliability Entity, Inc.	Derrick Davis	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Copyright © 2014 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Non-Binding Poll Results

Project 2014-04 Physical Security CIP-014-1

Non-Binding Poll Results	
Non-Binding Poll Name:	2014-04_CIP-014-1
Poll Period:	4/20/2014 - 4/24/2014
Total # Opinions:	363
Total Ballot Pool:	429
Ballot Results:	84.62% of those who registered to participate provided an opinion or abstention; 83.84% of those who provided an opinion indicated support for the VRFs and VSLs that were proposed.

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	Comments
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Abstain	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke		
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Abstain	
1	Baltimore Gas & Electric Company	Christopher J Scanlon		
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Hudson Gas & Electric Corp.	Frank Pace	Negative	COMMENT RECEIVED
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Garland	David Grubbs	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	COMMENT RECEIVED

1	Cleco Power LLC	Danny McDaniel	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	East Kentucky Power Coop.	Amber Anderson	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Edison Electric Institute	David Batz		
1	El Paso Electric Company	Pablo Onate	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Negative	COMMENT RECEIVED
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	COMMENT RECEIVED
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Negative	COMMENT RECEIVED
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Brett Holland)
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John Chin	Abstain	
1	Lincoln Electric System	Doug Bantam	Affirmative	

1	Los Angeles Department of Water & Power	John Burnett	Abstain	
1	Lower Colorado River Authority	Martyn Turner		
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Negative	COMMENT RECEIVED
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton	Negative	SUPPORTS THIRD PARTY COMMENTS - (See comments from New Brunswick Power Corporation)
1	Network & Security Technologies	Nicholas Lauriat		
1	New York Power Authority	Bruce Metruck	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Negative	COMMENT RECEIVED
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Chelan County	Chad Bowman		
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	

1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa		
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Southwestern Power Administration	Angela L Summer	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES/SPP)
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		

3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Abstain	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blue Ridge Electric	James L Layton		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt	Abstain	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Mark Schultz	Abstain	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Negative	COMMENT RECEIVED
3	CPS Energy	Jose Escamilla	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	East Kentucky Power Coop.	Patrick Woods	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
3	El Paso Electric Company	Rhonda Bryant	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	Entergy	Kevin Weber		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	

3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes		
3	Kansas City Power & Light Co.	Joshua D Bach		
3	Kissimmee Utility Authority	Gregory D Woessner	Abstain	
3	Lakeland Electric	Mace D Hunter	Affirmative	
3	Lee County Electric Cooperative	David A Hadzima		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Negative	COMMENT RECEIVED
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Abstain	
3	Muscatine Power & Water	John S Bos		
3	National Grid USA	Brian E Shanahan	Affirmative	
3	National Rural Electric Cooperative Association	Patricia E Metro	Abstain	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	North Carolina Municipal Power Agency #1	Kathy Moyer	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mahmood Safi - OPPD)
3	Orange and Rockland Utilities, Inc.	David Burke		
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	COMMENT RECEIVED
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	

3	Public Utility District No. 1 of Chelan County	Steve Wickel	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Abstain	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Southern Indiana Gas and Electric Co.	Fred Frederick	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott		
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Negative	COMMENT RECEIVED
4	DTE Electric	Daniel Herring	Affirmative	
4	Eugene Water & Electric Board	Dean Ahlsten	Abstain	
4	Flathead Electric Cooperative	Russ Schneider	Negative	COMMENT RECEIVED
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Garkane Energy	Mike Avant		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen		
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		

4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Abstain	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	Acciona Energy North America	George E Brown	Abstain	
5	Amerenue	Sam Dwyer	Abstain	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke		
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Negative	SUPPORTS THIRD PARTY COMMENTS - (Black Hills Corporation on behalf of 4 entities)
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Calpine Corporation	Hamid Zakery	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Negative	COMMENT RECEIVED
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		

5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	East Kentucky Power Coop.	Stephen Ricker	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	El Paso Electric Company	Gustavo Estrada	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper		
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Hydro-Québec Production	Roger Dufresne	Negative	SUPPORTS THIRD PARTY COMMENTS - (in support of HQT)
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lafayette Utilities System	Jamie B Webb		
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Manitoba Hydro	Chris Mazur	Negative	COMMENT RECEIVED
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	

5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	COMMENT RECEIVED
5	Ontario Power Generation Inc.	David Ramkalawan	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Abstain	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Illinois Power Coop.	Alvis D Lanton		
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Abstain	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (See SPP Group)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson		
6	Duke Energy	Greg Cecil	Affirmative	
6	El Paso Electric Company	Luis Rodriguez	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson		
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw		
6	Luminant Energy	Brenda Hampton	Abstain	
6	Manitoba Hydro	Blair Mukanik	Negative	COMMENT RECEIVED
6	Modesto Irrigation District	James McFall	Abstain	
6	Muscatine Power & Water	John Stolley		
6	New York Power Authority	Saul Rojas	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative	
6	Northern California Power Agency	Steve C Hill	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mahmood Safi)
6	PacifiCorp	Sandra L Shaffer	Abstain	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp	Affirmative	
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Abstain	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	

6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Westar Energy	Grant L Wilkerson		
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
7	Eastman Chemical Company	David L Moore		
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Praxair Inc.	David Meade		
7	Siemens Energy, Inc.	Frank R. McElvain	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner	Abstain	
8		David L Kiguel	Negative	COMMENT RECEIVED
8	Foundation for Resilient Societies	William R Harris		
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	COMMENT RECEIVED
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Idaho State Public Utilities Commission	Johanna Bell	Affirmative	
9	National Association of Regulatory Utility Commissioners	Jerry M Maio	Abstain	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC CIPC comments)
10	Southwest Power Pool RE	Bob Reynolds	Negative	COMMENT RECEIVED
10	Texas Reliability Entity, Inc.	Derrick Davis	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Individual or group. (137 Responses)
Name (97 Responses)
Organization (97 Responses)
Group Name (40 Responses)
Lead Contact (40 Responses)
IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE. (35 Responses)
Comments (137 Responses)
Question 1 (94 Responses)
Question 1 Comments (102 Responses)
Question 2 (96 Responses)
Question 2 Comments (102 Responses)
Question 3 (93 Responses)
Question 3 Comments (102 Responses)
Question 4 (95 Responses)
Question 4 Comments (102 Responses)

Individual
Jennifer Wright
San Diego Gas & Electric
Yes
San Diego Gas & Electric (SDG&E) agrees that it is appropriate to start with those Transmission Owners that own Transmission facilities that meet the bright line criteria in Reliability Standard CIP-002-5.1 for a “medium impact” rating. However, SDG&E believes that it would be prudent to simply refer to the CIP-002-5.1 Impact Rating Criteria rather than restating it in CIP-014 Standard. Being more specific that this Standard is applicable to Transmission Owners that have any facilities identified as “medium impact” facilities under CIP-002-5.1 Attachment 1, Inpact Rating Criteria 2.4, 2.5, 2.6 and 2.7, would be clearer and more consistent with the general way that CIP-003-5 through CIP-011-5 are built upon the identification of “critical” facilities made in CIP-002-5.1. Linking the two explicitly, rather than simply restating the same language, would prevent the possibility that differences could creep into the rules over time as each Standard is modified.
Yes
SDG&E agrees with this approach. A facility’s identification as “medium impact” does not necessarily mean that the facility, if rendered inoperable or damaged could result in widespread instability, uncontrolled separation or Cascading within an Interconnection. Application of a risk assessment will ensure that CIP-014-1 is focused on the facilities that are most critical to the system.
Yes

SDG&E agrees that an evaluation of potential threats and vulnerabilities of a physical attack to the facilities identified in R1 through R3 of the Standard is appropriate. Security threats and vulnerabilities can, and will vary from location to location and such differences must be accounted for in a robust security plan. It is appropriate and necessary that the Standard not mandate a one-size-fits-all approach, but requires entities to take into account the unique characteristics of each facility. SDG&E understands the Federal Energy Regulatory Commission's concern addressed by its Paragraph 11 directive that the Standard must have the analysis verified by an independent third party. While SDG&E believes it has in-house experts capable of performing such an analysis (as required by R4) and developing a Physical Security plan (as required by R5) adequately, SDG&E appreciates that verification by a third party, essentially a "second opinion," can serve to ensure a robust analysis of the physical security threats and vulnerabilities of facilities identified in Requirements R1 through R3. SDG&E appreciates the broad definition under R6.1 of what qualifies as a "unaffiliated third party reviewer." A list that unnecessarily limits possible reviewers could: 1) result in a bottleneck as too few potential reviewers are available for the industry to use; and 2) result in increased costs and a tight market for reviewers results in higher prices for their services.
No
Individual
Debra Horvath
Portland General Electric
Yes
Yes
The following comments relate to suggested modifications for Requirements 1-3 – PGE believes the 90-day period to ensure verification of the risk assessment is too short. It will be difficult for every Transmission Owner to establish a contract with an unaffiliated verifying entity during the implementation time period. In addition, the current wording of the standard puts the obligation on the Transmission Owner to make sure that the assessment is done within 90 days, even though by definition they cannot have control over that timeline. Therefore, PGE proposes replacing the R2.2 language, "[t]he Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment," with the language, "[t]he Transmission Owner shall ensure that any agreement executed with the unaffiliated verifying entity stipulate that the verification be completed by a date that is not later than 90 calendar days from the completion of the Requirement R1 risk assessment." In addition, Requirement R3 provides no mechanism for the Transmission Operator who operates a primary control center identified by a different Transmission Owner to disagree with that identification. PGE proposes including similar language to that in R2.3 to allow for the Transmission Operator to document the technical basis for not identifying its primary control center as an asset to be protected.
Yes

In Requirement R4 the phrase “owns or operates” is used for the first time. If Transmission Owner Entity A is also a Transmission Operator of a line it does not own, and that line was identified by Transmission Owner Entity B in Requirement R1 and verified according to Requirement R2, Entity A could be responsible for evaluating and protecting that line under this wording. However, there is no mechanism built into the standard to communicate this information or to allow the Transmission Operator to dispute the decision. In addition, Requirement R4.2 should be changed to “[p]rior history of attack.” In addition, in Requirement R4.3, the current wording places an unrealistic and unclear burden on every Transmission Owner to monitor intelligence or threat warnings from an open-ended list of sources. We recommend changing the wording from “[i]intelligence or threat warnings from sources” to “[i]intelligence or threat warnings received from sources” to narrow the obligation to information that the Transmission Owner actually received from its monitoring activities. In addition, in Requirement R5, the phrase “owns or has operational control over” is used for the first time. It’s not clear why this needs to be different from the “owns or operates” in Requirement R4. Consistent terms should be used to decrease potential confusion. In addition, as above, PGE believes that the 90-day period to review each entity’s evaluation and security plan is too short. Again, we propose replacing the R6.2 language, “[t]he Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5,” with the language, “[t]he Transmission Owner or Transmission Operator, respectively, shall ensure that any agreement executed with the unaffiliated verifying entity stipulate that the verification be completed by a date that is not later than 90 calendar days from completing the security plan(s) developed in Requirement R5.”
No
Group
Tennessee Valley Authority
Brian Millard
Yes
Yes
No
Comment: Proposed language to be added to the end on Requirement 6: This Requirement shall not apply to any Federal corporation or agency that meets any of the criteria in Requirement 6.1 and that has an Inspector General, pursuant to the Inspector General Act Amendments of 1988, appointed by the President of the United States and charged with oversight responsibility for such Federal corporation or agency. Comment: Recommend adding “with electric utility experience” as a reviewer qualification to 6.1.3 and 6.1.4.

Rationale: There should be a common standardizing qualification such as PSP, CPP, or electric utility experience that applies across the sub requirements of R6 that entities and the ERO can use as criteria to qualify unaffiliated third party reviewers.
No
Individual
Guy Zito
Northeast Power Coordinating Council
No
The applicability of the draft standard should be expanded to incude Planning Coordinators in addition to Transmission Owners and Transmission Operators. While NPCC agrees that TOs and TOPs simple application of the screening criteria to determine which facilities need analysis, they may not be able to conduct a complete analysis. The SDT should consider that Transmission Owners in some cases do not have the ability to conduct an analysis with a "wide area" view of consequences. Smaller TOs or TOPs only have an outside equivalent representation of the BES and could need help conducting their analyses. Consideration should be given to allow them to conduct the studies in conjunction with PCs.
No
The Rationale Box for Requirement R2 stipulates that "'unaffiliated' means that the selected verifying entity cannot be a corporate affiliate (i.e., the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission o(O)wner)." This conflicts with Requirement R2 Part 2.1 which lists "A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or An entity that has transmission planning or analysis experience" as those qualifications for an unaffiliated verifying entity. Clarification is needed that an Independent System Operator that has operating authority over an entity is eligible to be the unaffiliated verifying entity.
No
Regarding Part 5.1, the requirement states that the security measures should be designed to deter, detect, delay, assess, communicate and respond to potential physical threats. NPCC suggests removing the obligation to 'deter' from this Part and establish a separate Part that addresses deterrence and very basic specifics regarding what constitutes deterrence. The new Part could describe how an entity should implement deterrence and consider some minimum auditable criteria; for example, Consider and Implement measures designed to deter potential physical threats including 1) perimeter control 2) motion detection 3) lighting 4) access control. In this manner the ambiguity surrounding the term 'deter' is eliminated. Part 5.3 should allow flexibility to modify the time line. Suggest that Entities should 1) have a master Physical Security Plan; 2) have the flexibility to accomplish mitigation activities associated with the results of the vulnerability assessment, and 3) capture those mitigation plans under a separate mitigation plan (similar to the action plans for Cyber Assets vulnerability assessments) or include "associated modifications to the time line".

Yes
It is NPCC's expectation that RAI concepts will be applied to the operating and enforcement of this standard.
Individual
Greg Froehling
Rayburn Country Electric Cooperative
No
Overall comment is this is too complicated of a draft standard for a 90 day consensus! Keep it simple. I agree with the functional entitiy that is identified however, I would add GO to address any "critical" switchyards that may exist that are not owned by a TO. I also agree with the scoping of the facilities similar to the CIP V5 criteria with the following exception, apparently a list already exists for the substations that should be considered "high" do they deserve an alternative approach to what is within this standard? Altering the existing basic approach as follows: Since the FERC order allowed for "One or More Reliability Standards", it would be appropriate to address the "High " facilities separate from the "Medium Facilities". This approach would make it an easier task to file the "high standard" within the 90 days then follow with the "medium later". Thus giving more time, latitude and maneuverability to address issues that arise specific to those facilities.
No
I agree with the risk assessment in concept, the standard has far too many requirements and sub requirements to accomplish the task. Since initial analysis apparently this has already been done for the "High Risk" stations, a more efficient approach would be for the RC to perform the analysis based on the criteria mentioned to validate findings and find any second contingency facilities that may not have been identified. Since the RC is the "Reliability Coordinator", this is your third party identifying facilities without bias… Determinations will be based on an engineering basis utilizing standard uniform criteria across North America. The same analysis occurs for all entities within all regions, no variations this would yield consistency! Then the RC notify the entities that they have facilities that have been identified. (much like other NERC standards) Thus the information on which facilities have been identified would disseminated and controlled in a much more secure and better controlled environment while still maintaining the quality and consistency of the study needed.
No
Once the in scope facilities have been identified, it would be best for the entites to use the same resources for the evaluation of "Potential Threats" since this language has endless possibilities. i.e. Aerial attack, induced seismic events to name a few to illustrate "Potential". I favor the wording of "reasonable risks" The FBI, DOE or DHS should be involved in the discussion with the entities in lieu of a third party who is only subject to confidentiality agreements and also has interests beyond mitigating the true risks.
Yes

I think the standard IF broken up into 2 standards (High, Med) should provide clearer guidance as to the expectations of the plans content. Similar to the issues that arose with the Low assets in CIP V5 . Give basic structure and content to be addressed to give FERC the assurance the specific concerns have been met.
Individual
William H. Chambliss, member Operating Committee
Virginia State Corporation Commission
Yes
Yes
There does not seem to be any timeframe within which the initial assessment is to be completed under R1, nor when the 30 and 60 month periods for subsequent reassessments under R1.1 are to begin and conclude.
No
R4.2 requires each Transmission Owner of an identified facility to "consider" and "Prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events." Is such consideration to be given to other "similar facilities" of the specific Transmission Owner or of any Transmission Owner anywhere in North America? How will such "consideration" be possible if the scope of such consideration is intended to be the latter? R5 is fine, but R6 suffers from the same ambiguity as R4.
No
Group
None
Terry Volkmann
Yes
No
The SDT has not factored in the resiliency concerns stated in the FERC order. Many of the facilities selected by the initial screening process will have long lead time equipment that if damaged will be out of service for several months. The assessment process needs to consider the operational risks during the time that the TO is waiting for replacement equipment. R1 should be amended to include the following sub-requirement. If the facility being studied has long lead time items, i.e. 4 months or greater, the study must include an N-1 analysis for the widespread instability, uncontrolled separation, or Cascading within an Interconnection test. In addition, the premise for this standard is a physical attack resulting in faulted equipment. There is no mention of the assessment being conducted for the Facilities under fault

conditions and in many cases under delayed clearing. R1 should be amended to include the following sub-requirement. The analysis of the subject Facility must include dynamic simulation of faulted conditions with delay cleared for the most severe contingency within the Facility. The phrase "instability, uncontrolled separation, or Cascading" is core to the definition of Interconnected Reliability Operating Limit (IROL). Every RC and PC has an IROL methodology under the FAC standards. R1 should be amended to include the following sub-requirement. The test for instability, uncontrolled separation, or Cascading must be consistent with the IROL methodology established by PCs and RCs under FAC-010 and FAC-011.
No
It is recognized that a one–size–fits all approach is not practical. However the proposed directives as to what should be included in physical security plans are so general that little is likely to change from current practices that are insufficient to protect very critical high risk substations. The only language directive in CIP-01401 is listed on Pg. 10, R5 para 5.1. More definitive guidelines must be outlined if improvements are to really be achieved. The utility industry has used real-time remote monitoring of substation equipment for reliability purposes for decades. Similar technology is available for the very important physical security function. The following sentence needs to be added at the end of paragraph 5.1. “Security measures must include isolation zones of sufficient size covering approaches to substations, in addition to monitoring inside substation fenced areas, to detect both attempted and actual penetration of critical sites and the surrounding buffer areas. The areas must be patrolled with real time monitoring & assessment equipment designed to provide live and playback/recorded video that must be automatically presented to alarm station operators. Detection equipment must include gunshot detectors. Sufficient real-time surveillance must be provided to allow sufficient time to implement a tactical response plan to minimize and interrupt threats.”
No
Individual
Steve Hamburg
Encari
Historically, FERC and NERC have taken the position that redundancy is not an acceptable criterion to exempt a Critical Cyber Asset from mandated physical or cyber controls. Redundancy is not supposed to be a factor in the determination of the criticality; instead redundancy is used to improve reliability and availability. This principle should be extended to the protective measures applicable to control centers under CIP-014-1. So long as both the primary control center and backup control centers meet the bright line criteria for a medium impact rating under CIP-002-5.1, the protections under CIP-014-1 should apply equally to both the primary and backup control centers.
No

There should be a strong, rebuttable presumption that an applicable Transmission Facility requires physical protection owing to its classification under the bright-line "medium impact" rating criteria under CIP-002-5.1 (which is repeated in the Applicability section of CIP-014-1 for Transmission Facilities). The utility of a risk assessment could be recognized, however, as justification for rebutting the presumed need for a set of mandated physical security measures.
No
The approach taken by the Nuclear Regulatory Commission, which prescribes specific physical protections for nuclear plants and materials in 10 CFR Part 73, is instructive. Applicable Transmission Facilities, which are subject to common potential threats and vulnerabilities, warrant minimum physical security protective measures. Physical security plans should incorporate those prescribed protective measures unless a responsible entity can establish that its validated security plan provides a comparable level of protection required by the Standard.
Yes
CIP-014-1 should expressly permit one well-coordinated physical security plan for a Transmission Facility. As proposed, there could be a separate physical security plan under CIP-006-5 for BES Cyber Systems within an applicable Transmission Facility and potentially another physical security plan for the Transmission Facility as whole under CIP-014-1.
Individual
David Ramkalawan
OPG
No
In the applicability section of the proposed standard, does the exemption refer to the Nuclear Generation Facility or the Transmission facility to which the Nuclear Generation Facility is connected? In Canada the Canadian Nuclear Safety Commission has no jurisdiction over the Transmission Owner/Operator; therefore the intent of the standard has to be made clear on this point.
Yes
Yes
Yes
Individual
Ralph Meyer
The Empire District Electric Company
Yes

EDE feels this is the right approach on selecting a threashold for applicability to this standard.
Yes
Yes
No
Individual
Kalem Long
The Empire District Electric Company
Yes
Yes
Yes
Yes
Individual
Mike Kidwell
Empire District Electric Company
Yes
Yes
Yes
Yes
Individual
Candace Morakinyo
We Energies
Agree
Edison Electric Institute (EEI)
Individual
Ronnie C. Hoeinghaus

City of Garland
Yes
Yes
No
Clarification - R6.2: Need to clarify that “completing the security plan(s)” does not include completing the tasks outlined in the time line developed in R5.3 – the time line is required to be complete as part of the plan but not the tasks in the time line.
Yes
Recommendation # 1 – Include the timeline diagram located in the FAQ document titled “CIP-014 Physical Security Process Flow” in the Guideline and Technical Basis section of the standard. This diagram clearly demonstrates the timing between the different requirements. Because of the subsequent risk analysis’s in R1, verifications in R2, and potentially the processes outlined in R3, R4, R5, & R6, questions on timing (answered by the diagram) potentially will arise throughout the life of the standard. Recommendation # 2 – Add the words “catastrophic failure” to the Purpose statement. On a webinar, there was discussion concerning the Purpose statement and it was stated a number of times that “widespread instability, uncontrolled separation” meant to convey the concept of “catastrophic” – there will be a lot of folks involved in the implementation of the standard who did not hear the webinar comments. Recommendation # 3 – Rather than the term “primary control center” used in all the proposed requirements, use a different term or phrase such as the “facility that has direct Supervisory Control”. The word “direct” in the recommendation of “direct Supervisory Control” should replace the need for the word “primary” - primary makes one think of primary and backup (which is not addressed in the standard). The concern with using primary control center, even though “control center” is not capitalized, brings up a mental picture of primary (and backup) Control Centers as defined in the NERC glossary. The standard should be straight forward, not using terms that can be confused.
Individual
David Rudolph
Basin Electric Power Cooperative (BEPC)
Yes
Yes
R2 – A concern to consider is whether there is an adequate pool of unaffiliated third party verifiers to meet the 90 day timeframe. Possible solutions would include (1) increase the 90 day requirement to six months; or (2) Revise the requirement to allow the NERC Registered Entity to notify the appropriate Regional Entity of the verifier pool constraint and request the Regional Entity act as the verifier or specify an acceptable alternative.

Yes
Yes
The SDT should be applauded for the diligent work performed in short order to meet the requirements of the FERC order RD14-6-000 while allowing flexibility in the manner the Registered Entity may be compliant.
Group
Edison Electric Institute
David Dworzak
Yes
Yes
Yes
Yes
EEI supports the draft standard CIP-014-1 as fully responsive to the FERC March 7 order. The project has moved along a very aggressive timeline and naturally raises a broad range of practical and implementation issues. Based on extensive discussions with member companies, EEI recommends that the standard drafting team (SDT) consider additions or changes to the implementation guidance that will clarify for companies several questions on the timing of the various implementation stages of the standard, including especially that security plans are subject to change over time for a broad range of reasons. In addition, EEI asks the SDT to consider clarifications in implementation guidance that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work. Observing the many meetings and webinars that have taken place recently, EEI also recommends that the SDT consider adding language in the implementation guidance around the application of the terms 'control center,' 'primary control center,' and 'transmission station' in the draft standard. Obviously, there are a wide variety of understandings on these terms and additional clarity will help companies' ability to perform under the requirements. Considering that these terms have generic application to bulk power system reliability, the project timeline does not afford time for careful consideration of various facts and circumstances that might inform content of formal NERC defined terms.
Group
Southwest Power Pool Regional Entity
Bob Reynolsa
No

SPPRE does not agree with the applicability because it excludes certain facilities that could pose a significant risk to the BPS reliability if rendered inoperable or damaged as a result of a physical attack. Other facilities that should be applicable are those where high impact BES Cyber Systems are found. Additionally, any Special Protection System and automatic load shedding system capable of shedding 300 Mw or more should be included. Reference CIP-002-5 Attachment 1 (Impact Rating Criteria 1.1, 1.2, 1.4,2.9, and 2.10). SPPRE also disagrees with the decision to limit applicability to only the primary control center.
No
SPPRE believes that greater clarity is required with respect to the risk assessment to be performed. At a minimum an extreme contingency study needs to be performed that takes out the entire facility, all voltages present. The study should also not consider any operating guides or other mitigation when evaluating the impact of the outage. In Section 2.3 technical basis should be changed to engineering basis. Additionally, the unaffliated verifying entity should not be the party performing the original study, under the principle that an auditor cannot audit ones own work; to do so would not be consistent with the expectation of verification by an unaffiliated entity.
No
SPPRE disagrees with the inclusion of Requirement 4.2. Prior history is not a predictor of future events and could result in critical facilities not being protected until after a sucessful first damaging attack with adverse BES reliability impact. Requirement 5.3 should be a project plan with measurable milestones for implementing the physical security enhancements and modifications.
Yes
SPPRE recommends that subsequent risk assessments should be peformed at least every 36 calendar months regardless of whether previous risk assessments had identified critical facilities. It is more important to identify facilities that should be on the list than those that might not need to be on the list anymore.
Individual
Randi Nyholm
Minnesota Power
Yes
Yes
Yes
Overall Minnesota Power agrees with the approach laid out by the Standard Drafting Team in Requirements 4-6, but requests that the SDT consider modifying the wording of R5.1 as follows. Resiliency or security measures designed to deter, detect, delay, assess, communicate, or respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4. An auditor could interpret the use of “and” in

"…deter, detect, delay, assess, communicate, and respond…" to mean that each resiliency or security measure be designed to meet all of these, where we believe and hope that the intent of the sub-Requirement is that the resiliency or security measure identified in the physical security plan be designed to "…deter, detect, delay, assess, communicate, or respond…", while recognizing that it may meet more than one.
No
Individual
Bob Thomas and Kevin Wagner
Illinois Municipal Electric Agency
Agree
Florida Municipal Power Agency American Public Power Association
Individual
Jack Stamper
Clark Public Utilities
No
Section 4.1.2 of the Applicability section states "Transmission Operator." This reference in the Applicability section should be more specific based on the the actual conditions under which CIP-014 would be applicable to a Transmission Operator. Clark suggests the reference should be revised to "Transmission Operators that have operational control over the primary control center of a Transmission station or Transmission substation identified in section 4.1.1."
Yes
Yes
No
Individual
Frank Pace
Central Hudson Gas & Electric Corporation
Yes
No
In regards to R2.2 as currently drafted, the unaffiliated verifying entity should have to ensure verification within 90 days and not the TO, since it is that entity performing the verification. In regards to R2.3 as currently drafted, there appears to be a lack of an appeals process in cases

of disagreement between the unaffiliated verifying entity and the TO concerning the recommendations formulated by the unaffiliated verifying entity.
Yes
No
Individual
Earl F. Cass
EF Cass Consulting Inc.
No
the applicability section table should be modified by either removing the 500kV line or making it a 3000 value. By giving it a 0 value in the table it send a different message than the text indicating all 500kV facilities are in. Also, in the draft RSAW Compliance Assessment approach for R1, it would appear that a Transmission Owner needs to comply with R1 and R2 in order to determine if the standard applies to them. If an entity is required to have a process for determining applicability then it needs to be a requirement. The applicability section should produce a yes or no answer. I spoke with Nick Webber of WECC and his response back was "Much like the requirement of all entities to apply CIP-002, all entities registered as for the TO function must complete CIP-014-1 R1 and R2. Each TO must complete R1 to determine if R3-R6 apply. The TO then must subsequently have that R1 assessment reviewed as required in R2." An entity should not have to comply with 2 of the requirements in order to determine if the standard applies to them. If all TOs are expected to comply with R1 and R2, then move the criteria into the requirement, if that is not the intent, clarify that once an entity reviews the applicability section and determines the standard does not apply they are finished. The rationale for requirement R1 indicates the criteria is in R1 when it is actually in the Applicability section.
Yes
This standard has the perceived importance of protecting national security and being so critical as to expedite its development through modification of nearly all associated controls. I agree physical security of critical facilities is of paramount concern but not at the expense of producing a sound standard. After listening to two of the webinars it is clear to me that the majority of the entities responsible for ultimately complying with this standard and those that will enforce the requirements are unclear as to what is required. I would suggest running it past the "Experts" for their review prior to the first vote.
Group
Tampa Electric Company
Ronald L Donahey

Yes
Yes
Yes
Comments to R5 Tampa Electric Company appreciates the excellent work of the standard drafting team (SDT). They and their support staffs have evidently worked very hard to produce in a very short time a family of documents that create a workable framework for improving the physical security of Transmission substations and primary Control Centers. We also commend NERC and the SDT for reaching out to the industry through a live a technical conference and by conducting a series Webinars in local and national venues. Moreover, we fully support the intent of the SDT as it has been articulated so well in the technical conference, in NERC and FRCC Webinars and in EEI and NATF conference calls. Unfortunately, there is a critical ambiguity in the text of requirement R5 that is problematic and needs to be addressed by the SDT. Our main concern is that requirement R5 literally reads that all provisions of the security plans for our primary control center and for all our substations and switchyards, including the installation and construction of any physical security upgrades, must be completed "within 120 calendar days following the completion of Requirement R2." Such a requirement may well be impossible to meet depending on the extent of the upgrades, the need for facility outages, and the number of locations that are affected. Members of the SDT have made it very clear in the Webinars and conference calls that they did not intend this result. Instead, the SDT intended to require registered entities, "within 120 calendar days following the completion of Requirement R2," to develop and document plans that include definite timelines for completing any security upgrades that are necessary to protect against the vulnerabilities and threats that are identified under requirement R4. Given that the text of R5 is contrary to the intent of the SDT, Tampa Electric urges the SDT to clarify that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work. This clarification can be accomplished in the guidance document to the standard or by our preference, editing the text of the standard and issue a revised standard for a second ballot. Removing "and implement" from the text of requirement R5 should remove the ambiguity and conform the text to the intent of the SDT. This edit, combined with R5.3 expresses the SDT's intent on this issue: R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following

attributes: [VRF: High; Time-Horizon: Long-term Planning] 5.3. A timeline for implementing the physical security enhancements and modifications specified in the physical security plan.

Yes

Comments: Comments to Definitions Tampa Electric also urges the SDT to define certain terms that appear in the standard: 1) “Transmission substation” and “Transmission station,” 2) “collector bus,” and 3)“primary control center. There terms are not defined in the NERC Glossary and may not have definitions that are universally accepted by the industry. “Transmission substation” and “Transmission station” Many industry practitioners use the term “Transmission substation” generally, whether or not any transformers are installed in the facility they are describing. Other practitioners apply the term “Transmission substation” only to facilities that include transformers. The standard implicitly uses the term “Transmission station” in reference to transmission switching arrangements that do not involve transformers. However, the more commonly used term for a transmission switching arrangement that does not include transformers is “Transmission switchyard.” NERC addressed this issue in the Guidelines and Technical Basis section of CIP-002-5. The SDT could easily carry that text over to the Guidelines and Technical Basis section of CIP-014-1. However, it would be better to add definitions for “Transmission substation” and “Transmission station” to the Glossary of Terms Used in NERC Reliability Standards. The relevant text in CIP-002-5 is copied below for the convenience of the SDT. CIP-002-5 Guidelines and Technical Basis clarifications of “Transmission stations” and “Transmission substations” The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist. “Collector bus” “Collector bus” is another term that is not defined in the NERC Glossary and that may not have a definition that is universally accepted by the industry. “Collector bus” appears in 4.1.1.1 and in 4.1.1.2. of CIP-014-1 in text that was carried over from CIP-002-5. 4.1.1 Transmission Owner that owns any of the following: 4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. [Underlines added] 4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. [Underlines added] If “Collector bus” is not defined or clarified, some TOs may conclude that some part of

every transmission substation or switchyard that receives the output of a generator(s) is excluded from the scope of the standard. However, that is not the case nor the intent of the SDT. Therefore, the drafting team should consider whether it should define or clarify in the guidance document, the term “collector bus” “Primary control center” The NERC Glossary defines “Control Center” in this manner: One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations. What might not be clear for the purposes of CIP-014-1 is what exactly distinguishes a “primary control center” from other alternate “Control Centers.” Some registered entities can operate substations from multiple locations. Often, there is one self-designated “main control center” or “primary control center” for which there might be multiple alternate or “backup control centers.” Given that alternate or backup control centers have capabilities that are comparable to so-called main control centers, it might not be clear in some systems whether “primary control center” in CIP-014-1 applies to more than one Control Center. The SDT can solve this problem by adding a definition of “primary control center” to the NERC Glossary or by adding text to CIP-014 that for each critical substation the TO or TOP can designate any Control Center as the “primary control center.”

Group

Black Hills Corporation Entities

Bob Case - NERC Compliance Manager , Bob.Case@blackhillscorp.com

No

Black Hills Corporation (referred to as BHC hereafter) believes that Section 4.1.1 has appropriate applicability specifics, but Section 4.1.2 only says “Transmission Operator”, which initially implies a much greater scope. Request that similar to Section 4.1.1 styling, Section 4.1.2 alternatively state “Transmission Operators notified by a Transmission Owner according to Requirement R3.”

No

Although BHC agrees with the overall approach, it has significant concerns regarding the use of the term “risk assessment” without a clear definition of intent. CIP-002 regulatory expectations in the Western interconnect for RBAM have consistently referred to the classic risk definition as “risk” times “probability”. However, the further expectation is that the probability of an event is assumed to be 100%, such that the “risk” them becomes equal to the “impact”. CIP-014 does not currently lay out the same expectations, which could allow Transmission Owners and other affected (or unaffiliated) parties to disagree over the role of “proabability” in defining risk. This problem can be resolved in the CIP-014 draft by: 1. leaving the risk assessment language as is, but adding the above statements about “probability” of occurrence being 100%, or 2. changing all references of ‘risk assessment’ in the standard, to ‘impact assessment’, or 3. leave the risk assessment language as is, but make it clear that CIP-014 is deviating from the historical CIP-002 RBAM definition of risk, such that the probability

of the event can change the perceived risk (and that such an interpretation is congruent with the FERC order. This last option seems to be closest to the intent of Paragraph 8 in the FERC directive, but represents a significant departure from past NERC CIP guidance, and needs to be highlighted as such. As written, the TO has exclusive determination say in identifying applicable Transmission stations, substations and primary control centers. R2 speaks to a third party verification of that assessment, but Black Hills believes that coordination of the BES would be better served by having the TO & TOP reach a consensus on the assessment, prior to having the assessment validated by a third party. Requirement 2.1 directs the Transmission Owner to select an unaffiliated Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment. Firstly, Planning Coordinator does not appear in the NERC functional registry and should not be casually equated with the TP and RC functions; without first equating the Planning Coordinator to the PA function per the NERC glossary. Secondly, none of these NERC functional entity designations appear in the applicability section of the standard. Therefore, it can be assumed that the unaffiliated PC, TP, or RC are not obligated to conduct the assessment themselves, but rather the assessment is conducted by mutual agreement of the TO and unaffiliated PC, TP, or RC acting as third-party assessor. If this is not the correct assumption, then the PC, TP, and RC functions should be noted in the applicability section. If the Transmission Owner is affiliated with the Transmission Planner and Planning Coordinator, then the third-party review should be performed by the entity's Reliability Coordinator. The reference to "primary control center" is adequately explained in the rationale section of R1, but confusion between it and "back-up control centers", "emergency dispatch center", and those control centers that can only monitor status seem to justify an up-front definition in the standard. Recommend that a special definitions section be added, or the term be clearly defined at its first instance in Section 3. R2.4 could benefit from some added guidance regarding the protection of sensitive or confidential information. Is the intent to employ the entity's baseline confidentiality banner, or something more robust such as that required by CIP-003-3 R4 or CIP-011-1. The latter seems more appropriate for this CIP standard.

No

BHC has the same concern with R4 as expressed in the opening comment of the previous section regarding the definition risk assessment. The tailored evaluation required by FERC directive paragraph 8 introduces a probability of less than 100%, which is in conflict with prior NERC guidance on risk definition. As previously noted, if the unique probability of a threat is to be taken into consideration along with the impact, this change from CIP-002-3 expectation should be clearly highlighted. In addition, the inclusion of probability in the risk assessment will increase disagreements between unaffiliated entities, which will require a mechanism for resolution. BHC questions R4.2: The current language states "Prior history or attack". BHC believes this opening should state "Prior history of attack" because the current language does not provide an indication of what 'prior history' is being referred to. BHC agrees with the AZPS suggestion that a sector specific threat source be utilized to aggregate and disseminate threat information to ensure that relevant and timely data is analyzed consistently across the regions, which would also improve the auditability of the standard as well by removing the subjectivity associated with an unbounded number of threat sources. BHC believes that the

120 day requirement for R5 should be limited to the development of the security plan, and that full implementation should be dependent on the complexity of the plan. Implementation timing of the entity's plan should be approved by the applicable RC. Provisions could be added for temporarily derating the facility, if the implementation timing were considered by the RC to be excessively long. By mandating a 120 day implementation, entity's security plans may be down-sized to meet the 120 day implementation window, rather than to meet the potential threats and vulnerabilities at the facility. If "implementing" only means the specific deliverables of R5.1, R5.2, R5.3, and R5.4 (i.e. the timeline required by R5.3 is created, but not executed), then "implementation" needs to be more clearly defined. BHC has a further concern that R5.1 language reads too close to the "Identify, Assess, Correct" language already remanded by FERC in the CIP v5 standards. Alternative language for R5.1 might be "Resiliency or security measures designed to prevent potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4." This simplification is not expected to change entities efforts, but could be more appealing to FERC. BHC agrees with the reasoning of AZPS to simplify R6.1 to read: "Each Transmission Owner and Transmission Operator shall select an unaffiliated third-party reviewer with electric industry physical security expertise." If this language consolidation is not acceptable, then alternatively recommend that Section 6.1.1 be expanded to include other similar certification providers, e.g. the National Sheriffs' Association Institute for Homeland Security offers a Certified homeland protection Professional (CHPP) designation (https://ndpci.us/certification/CHPP_Certifications.php), so as not to appear preferential.
No
Individual
Ayesha Sabouba
Hydro One
Yes
We agree with the Applicablity. R1 has provided flexibility in the assessment method.
Yes
Subsequent risk assessments should be performed every 36 months (to align with CIP requirements) instead of every 30 months. The FERC Order allows for the verification to be completed by NERC, the Regional Entity, an RC or another entity. The standard only identifies that the verification can be completed by a registered Planning Coordinator, Transmission Planner, or Reliabity Coordinator, or an entity with transmission planning and analysis experience; it does not mention NERC or the regional entity.
Yes
The Standard allows the TO and TOP sufficient flexibility to complete R4, R5 and R6.
Yes
Will FERC accept R2.3 and R6.3, which allows the TO or TOP to document why they are not following the recommendations from the verification? The FERC Order did not suggest this. It

is extremely important that all jurisdictions follow the same standard, so that the mitigation of risk to physical security is consistent. Having some jurisdictions who follow a more stringent standard will increase costs to ratepayers in those jurisdictions. The standard should provide a definition for “unaffiliated”.
Group
ERTF
Joe Tarantino
Agree
The following comments are in agreement with LPPC and ERTF as well as comment from our own entity LCRA: • Use of “primary control center” is ambiguous (R1.2 and others); • Unaffiliated third party review needs to be longer than 90-days, suggestion to be 180-days (R2.2); • Issue with non-disclosure agreement vs. Public Power’s obligation to disclose information (R2.4); • Expansion of the Security Plan third-party reviewer to include those functions that are identified in Requirement 2.1 (R6.1). • The standard does not address substations/stations that are owned by multiple Transmission Owners. LCRA TSC recommends adding language describing NERC’s expectations associated with jointly-owned substations/stations or substation/stations with multiple asset owners.
Individual
John Falsey
Invenergy LLC
Agree
NPCC
Individual
David Kiguel
David Kiguel
No
1. For clarity suggest that the word “verify” be changed to “confirm” in sub-requirement 2.2 so that it reads: “The unaffiliated verifying entity shall either confirm the Transmission Owner’s risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). 2. Sub-requirement 3.1 should cover both, addition and removal of elements from the identified facilities list. Suggest changing to: “In the case of addition(s) to, or removal(s) from the identified Transmission stations or Transmission substations list developed under Requirement R1 and verified/modified according to Requirement R2, the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the change(s).”
No

Sub-requirement 6.1.1: While Certified Protection Professional (CPP) or Physical Security Professional (PSP) might be recognized certifications in the U.S.A., that is not necessarily the case across the Canadian Provinces. Recommend to add: “or equivalent in those jurisdictions where such certifications are not recognized.” Sub-requirement 6.4: In addition to the non-disclosure agreements referred to in this sub-requirement, the standard should specify that the reviewing individuals having access to the confidential information must have security clearance and training, similar to the requirement in other CIP standards. Also, the security clearance must be obtained according to the established procedures in the respective jurisdiction.
Yes
The Implementation Plan obligates applicable entities to complete the initial risk assessment in Requirement R1, on or before the effective date of the standard. While performing and completing the vulnerability assessment before the effective date of the standard may constitute a recommended good practice, from a statutory perspective, compliance with the standard before its effective date may not be enforceable in all jurisdictions. An entity cannot be found in violation of the standard at a time when the standard is not yet effective. Recommend changing the implementation plan to require completion of the assessment after the effective date of the standard.
Group
JEA
Tom McElhinney
Agree
APPA
Individual
Michael Haff
Seminole Electric Cooperative, Inc.
National Rural Electric Cooperative Association (NRECA)
Yes
Seminole supports the comments by NRECA. Additionally, Seminole supports the use of CIP-002-5 medium impact criteria for use in CIP-014. CIP-002-5 has at least one issue that will apply to CIP-014 as well. There are multiple ways to interpret the phrase Transmission Facility. One example is clarifying what is in the scope of a Transmission Facility. The definition or other documentation should state that the substation is exclusive of the criticality of any connected substation and clarify that a Transmission Facility as used here does not include Transmission Lines.
Yes
Seminole supports the comments by NRECA. Additionally, Seminole agrees with this approach. As this standard is based on the same standards as the impact ratings in CIP-002, it would be cleaner to identify any facility that is determined critical under the Assessment with a separate (non-exclusive) impact rating such high physical impact and use this term for applicability for R3-R6. If an entity has a qualified third party perform the R1 assessment on

behalf of or in cooperation with the registered entity, does this also meet the requirement R2? Note that the draft RSAW, not under review here, states that R1 and R2 may occur concurrently. R2.4 is redundant with the information protection requirements in CIP-011-1. It would be appropriate to note that this information is included in the materials subject to enforcement under CIP-011-1 R1.
Yes
Seminole supports the comments by NRECA. Additionally, Seminole agrees with this approach. Requirements R4.1, 4.2, and 4.3 should be moved to the guidelines and technical basis as there is excessive flexibility provided to the auditor for concluding whether the evaluation is adequate and potential that an auditor may choose to determine that identification of events was inadequate. R5.2 requiring law enforcement contact information is redundant with EOP-004-2 R1. If an entity has a qualified third party perform the R5 security planning on behalf of or in cooperation with the registered entity, does this also meet the requirement R5? R6.4 is redundant with the information protection requirements in CIP-011-1. It would be appropriate to note that this information is included in the materials subject to enforcement under CIP-011-1 R
No
Group
Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing
Marcus Pelt
Yes
Yes
Yes
Yes
Clarification should be made in the implementation guidance for CIP-014-1 that Verifiers who are also Registered Entities in functions applicable to CIP-014, are not subject to penalty under the requirements of CIP-014 due to verification duties performed at the request of a responsible Transmission Owner and/or Operator.
Group
Arizona Public Service Company
Janet Smith
Yes

See related comments under Requirement 2 below.
Yes
AZPS generally agrees with the approach of the standard as drafted. The following comments relate to suggested modifications for Requirements 1-3. AZPS suggests that the drafting team modify the term “risk assessment” to “BES impact assessment” in Requirements 1-3. The term risk assessment is not a defined term in the NERC Glossary of Terms. It is used in other CIP standards (CIP-002, and CIP-004) each with a different context. Changing the term to “BES impact assessment” ensures that the risks will be categorized and evaluated correctly. Requirement 2.1 directs the Transmission Owner to select a Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment. However, none of these NERC functional entity designations appear in the applicability section of the standard. Thus it is assumed that the entities listed above are not obligated to conduct the assessment once selected but rather the assessment is conducted by mutual agreement. AZPS suggests that the drafting team provide clarifying language in the requirement to indicate that the assessment is conducted by mutual agreement between the Transmission Owner and the third-party assessor. AZPS is concerned that the term “primary control center” will be confused with the NERC Glossary Term “Control Center.” The definition of Control Center is partially defined as “monitor and control the BES…”. The rationale for Requirement 1 introduces the term “operationally control” in its definition of primary control center which is further defined to mean “causing direct physical action”. The concept of monitoring is explicitly excluded from this definition. To avoid confusion, AZPS suggests that the drafting team define the term primary control center or adopt a new term that clearly differentiates itself from the common term “control center”.
Yes
AZPS generally agrees with the approach of the standard as drafted. The following comments relate to suggested modifications or clarifications for Requirements 4-6. AZPS is concerned that Requirement 4.3, which requires the Transmission Owner to evaluate threat warnings from a myriad of sources, will result in inconsistent application by entities. The threat sources need to be consistent, and the threats evaluated must be relevant. AZPS suggests that a sector specific threat source be utilized to aggregate and disseminate threat information to ensure that relevant and timely data is analyzed consistently across the regions. This would also improve the auditability of the standard as well by removing the subjectivity associated with an unbounded number of threat sources. Requirement 6 requires Transmission Owners to secure a third-party review of the security plan developed under Requirements 4 and 5. AZPS strongly supports the development of security measures to protect critical substations. However, AZPS believes that requirements 6.1.1 through 6.1.4 add a level of specificity that does not provide an improved reliability benefit and has the potential to create a bottleneck that would make compliance within the short 90-day timeframe very difficult. AZPS contends that the most important quality of the third party reviewer is electric industry physical security expertise. Further, AZPS does not believe that the CPP or PSP certifications provide additional value from a realiability standpoint since neither certification has a sector specific focus. For these reasons AZPS would suggest that 6.1 be simplified to read: “Each

Transmission Owner and Transmission Operator shall select an unaffiliated third-party reviewer with electric industry physical security expertise.”
No
Individual
David Jendras
Ameren
Yes
No
(1) Regarding R3 and R3.1, we believe that the 7 day requirement is too short and 30 days would be more appropriate to notify other utilities. (2) R4 should have wording added to the requirement that the R4 evaluation is to be completed 120 days after the completion of R2. Then, the R5 wording should be changed so that the R5 physical security plans should be completed 120 days after the R4 evaluation is completed.
Yes
No
We recommend adding language in the implementation guidance around the application of the terms ‘control center’, ‘primary control center’, and ‘transmission station’ in the draft standard. Obviously, there are a wide variety of understandings on these terms and additional clarity will help companies’ ability to perform under the requirements. Considering that these terms have generic application to bulk power system reliability, the project timeline does not afford time for careful consideration of various facts and circumstances that might inform content of formal NERC defined terms. Also, we recommend that the standard drafting team (SDT) consider additions or changes to the implementation guidance that will clarify several questions on the timing of the various implementation stages of the standard, including particularly that security plans are subject to change over time for a broad range of reasons. In addition, we ask the SDT to consider clarifications in implementation guidance that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work.
Individual
Kayleigh Wilkerson
Lincoln Electric System
Yes

R1 - It appears the intent of R1 is for a TO (which meets the applicability section 4.1.1) to perform a risk assessment (as defined in the standard) on only those substations that meet the applicability section 4.1.1, not all substations owned by a TO which meets the applicability section 4.1.1 description; however this is not 100% clear. The verbiage of the second sentence in R1 states “The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify any Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.” The use of the word “any” in this sentence has led some to believe that a TO (which meets the applicability section 4.1.1 description) will have to assess all of their substations, even those that do not meet the section 4.1.1 description. To address this possible issue, LES recommends replacing the word “any” in R1 with “applicable”. R2 - Smaller TOs may not have the in-house resources to perform the risks assessments required in R1, and may need to contract with a third party to perform these assessments. If the performing third party is not affiliated with the TO, is a second unaffiliated third party verification required as stated in R2? Please revise the requirement to address this situation.
Individual
Gary Kruempel
MidAmerican Energy Holding Company
Yes
MidAmerican Energy Holdings Company (MEHC) agrees with the applicability section.
Yes
MEHC agrees with the R1 through R3 approach. However, MEHC suggests the following changes to improve the standards as written: The term “unafilliated third party” is used in R2 and in R6, but in parts 2.1, 2.3 and 2.3. “unaffiliated verifying entity” and in part 6.3 “unaffiliated reviewing entity” is used. Unless the intent was that the terms have different meanins, it is suggested that “unafilliated third party” be used throughout the standard.
Yes
MEHC agrees with the R4 through R6 approach. However, MEHC suggests the following changes to improve the standards as written: The following rewording of R5 is recommended to clarify that the “build out” of security enhancement schedule. R5 Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator’s primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The plan shall be completed within 120 calendar days following the completion of Requirement R2. Implementation of the plan shall be as documented in the plan.
Yes

1. The standard anticipates the potential for joint responsibility in involving transmission operator control centers for substations identified by transmission owners. It is suggested that additional guidance be provided regarding joint ownership of substations The following addition to the first paragraph under the Requirement R1 heading which is similar to an aswer to this questions in the webinars is suggested: For substations that are jointly owned the owners may jointly designate one of the joint owners to perform the risk assessment for that substation. 2. It is suggested that a clarification be made to the RSAW with regard to the following question: " As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?" By referring to risk assessment this seems to imply the stations/substations identified after the completion of the requirement R1 risk assessment rather than just the applicability requirements. It is suggested that the words "as a result of your risk assessment" be deleted from this question. 3. Item 3. in the guidance for Requirement R2 seems to actually be guidance for Requirement R1. However, it does not provide useful guidance for Requirement R1; therefore, it should be removed. The guidance for Requirement R1 that gives the TO discretion to choose its own methods and criteria is preferred. 4. The following modification to one of the sentences in the "Performing Risk Assessment" section of the guidance document is suggested: "Using engineering judgment, the Transmission Owner should develop criteria (e.g. imposing a fault near the removed substation) to identify a contingency resulting in potential widespread instability, uncontrolled separation or Cascading within an Interconnection."
Individual
John Canavan
NorthWestern Energy
Agree
Arizona Public Service, Bureau of Reclamation, Portland General Electric, WECC
Group
Western Electricity Coordinating Council
Steve Rueckert
No
WECC questions why generation assets are exempt from analysis and verification required by Requirements R1 and R2. It is possible that some generation assets, if rendered inoperable, could result in widespread instability, uncontrolled separation, or Cascading. WECC recommends removing the 500 kV line in the Weighted Value table. All 500 kV facilities are to be assessed per Applicability Section 4.1.1.1 and including 500 kV lines in the table in applicability section 4.1.1.2 with a zero value seems more likely to add confusion than to provide clarifying information. Applicability section 4.1.2 makes it look like the standard is applicable to all Transmission Operators. WECC suggests adding some clarifying language to indicate that the standard is only applicable to Transmission Operators notified per Requirement R3. This may serve to make the standard more acceptable to Transmission Operators in general.

No
The periodicity for risk assessments and the forward looking time frame for including planned substations do not match. Entities are only required to consider stations planned in the next 24 months, while the risk assessment is applied on a 30 month cycle, or a 60 month cycle if the entity previously identified a null list of applicable stations. This potentially leaves a 6 to 36 month gap. We would encourage the SDT to match the periodicity of the application to the planned implementation window or include language requiring any new asset be evaluated under R1. WECC notes that the time frame for completion of the initial risk assessment required in Requirement R1 is not identified in the standard, only in the implementation plan. This may be a point of confusion for entities that fail to fully read and understand the implementation plan. WECC suggests that at a minimum NERC and the Regions engage in extensive outreach to ensure that the Transmission Owners are aware of this and that if possible the drafting team revise the language of Requirement R1 to make this clear. Requirement R2, part 2.2 appears to be assigning responsibilities to the unaffiliated verifying entity (registered Planning Coordinator, Transmission Planner, or Reliability Coordinator) yet these entities are not included in the applicability section. If these entities are to be held accountable in the standard for actions, why are they not included in the applicability section?
No
From a compliance perspective, WECC notes that the criterion identified in R4 is too vague to enable a consistent approach across regions or even entities. Identifying a basic set of attack vectors that must be considered (ie: direct fire ballistic attack, indirect fire attack, explosive device attack, vehicle-borne attack, arson/incendiary attack) fosters a far more consistent approach while allowing the entity the flexibility to tailor their assessment and security plan to the unique characteristics and threat landscape of their asset(s). WECC is concerned that the language of Requirement R5 is confusing or contratictory. Requirement R5 requires the applicable entity to “develop and implement” a documented physical security plan…within 120 calendar days following the completion of Requirement R2. However, part 5.3 requires a timeline for “implementing” the physical security enhancements and modifications specified in the physical security plan. WECC questions whether Requirement R5 requires the physical security plan to be “developed” or “developed and implemented” within 120 calendar days following the completion of Requirement R2. If Requirement R5 requires “development and implementation” within 120 calendar days following the completion of Requirement R2, what is the purpose of the timeline for implementing the physical security enhancements and modifications specified in the physical security plan required by part 5.3?
Yes
WECC believes that the proposed standard addresses the FERC Order and has voted affirmative to approve CIP-014-1. However, as noted in our comments above we believe there is opportunity for enhancements and clarification that if implemented would improve the standard and still meet the FERC Order. WECC encourages the drafting team to consider implementation of these suggestions prior to the final ballot or NERC to submit a SAR for consideration of these suggestions immediately after approval of the standard.
Group

NCPA Compliance Management Operating Committee
Steve Hill
No
The Standard Drafting Team (SDT) estimates that relatively few Transmission Owners (perhaps 30 or less) will have Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability or uncontrolled separation. The Applicability section creates a lot of work for many TOs an TOPS to identity those 30 or less transmission stations out of the 55,000 substations. The SDT might consider a higher level of applicability as was done for EOP-010-1, Geomagnetic Disturbance Operations i.e. apply the standard to Reliability Coordinators (RC) and only the Transmission Operators the RCs deem critical.This would be a more efficeint filtering process. Benefits of such an approach would be (1)Simplification and tighter security of critical information and informaton sharing (2) streamling and simplicaton of requirements for unaffiliated third party review, for example one reviewer could handle the risk assessment, vulnerability and threat assessment and review of security plans (combines requirements R2 & R6 together) (3)Time and resources of the entity could be more efficiently and economically managed as all reviews could be handled by a single Reviewer in a continuous manner rather than starting a stopping for different phases. (4) Saves many entities who would fall out of the process after going through the first three requirements. I expect RCs, ISOs and Regional Entities already know this
No
Applicability is a key issue here. Comments to question 1 apply here as well. Why subject all Transmission Owners who may meet the "medium impact under CIP-002-5.1 to a third pary review for all medium impact stations and substations when only 30 stations will be affected (please define the difference between a Transmission station and Transmission substation. A third party review is appropriate for the 30 or so stations involved, but seems excessive for all owners to obtain third party review when the expectation is that 30 out of 55,000 are te ones of real concern. NCPA elected to have an independent third party risk asssessment and vulnerability assessment performed at its 5 generation facilities and control center. The assessment cost is approximately $150K and takes about 9 months to complete. NCPA'a assets are also low impact. The risk assessment, vulnerability and threat assessments and development of the security plans are able to performed by the same third party reviewer that flows together without interruption. The way in which the requirements are structured creates alot of consultants or third party reviewers running around, with 99% of them stopping work after R3. How much money will be spend for that and for what purpose? There has to be a better way segregate the 99% from the 1% where the real concern is.
No
Same line of reasoning as given in the response to the question 2. If the Applicability Section were changed R1, R3, R4,and R5 could be combined together and R2 and R6 could be combined together. This simplifies the standard and gets to the heart of the Reliability

Concern without creating a Consulting industry to perform third party reviews. (If you don't like the suggestion, maybe I found a new business opportunity)
Yes
The Implementation Plan is too agressive. I cite NCPA experience as described in our response to question 2. I find it interesting the the CIP-version 5 standards have essentially a two year implementation plan for medium and high assets and yet this proposed standard has a 6 month implementation plan.
Individual
Joe O'Brien
NIPSCO
In R2 we are not sure who would do the verification. On one of the webinars a member of PJM suggested that another PJM member could be a candidate. However it is likely that a PJM member is not a PC, TP or RC as prescribed in the requirement; that role is performed by PJM itself. Any further guidance would be welcome; we do not consider this a "show stopper". The hard work that went into putting this project together in such a short time frame is appreciated, thanks.
Individual
Wayne Sipperly
New York Power Authority
Agree
APPA
Individual
Megan Wagner
Westar Energy
Yes
No
The Standard intentionally does not provide specific methodologies regarding the type of analyses needed to be conducted for the assessments in R1. This leaves the door open to very different interpretations across the industry. We suggest the drafting team consider specifying analyses such as those contained in the TPL standards. This would eliminate confusion within the industry and provide clear direction for those conducting the analyses. We suggest adding the following sentence at the end of R1. “These analyses will include consideration of the entire loss of the Transmission stations and Transmission substations specified in Applicability Section 4.1.1 taken individually, one at a time.” While not specifically

referencing the TPL standards (currently enforceable TPL-004-0a, R1 and TPL-001-4, R3 to be enforced in 2016) which cover the loss of switching stations and substations, this language provides guidance regarding the type of analyses to be conducted in the assessments.
Yes
Yes
Effective Date: The use of the term 'implement' needs clarification . To some implement means installed and in-service. To others it could mean a work in progress. The SDT recognized this confusion in the webinars on April 17 and we encourage them to modify the language to more clearly indicate the intent of the drafting team. VSLs: Capitalize Part 2.3 in the Lower, Moderate and High VSLs for R2. Insert 'and verified according to Requirement 2' following the reference to Requirement R1 in all the VSLs for R5. Delete 'and modify or' in the last High VSL for R6. Guidelines and Technical Basis: Replace 'drafting team' with 'SDT' in the last paragraph under Section 4 Applicability on Page 27. Make the same change in the last paragraph on Page 32 under Requirment R6. Capitalize Remedial Action Schemes (RAS) and Special Protection Systems (SPS) in the paragraph at the top of Page 29. These are defined terms in the Glossary. Insert 'Transmission', capitalize 'Owner' and delete 'or operator' in the 1st paragraph under Requirement R2 on Page 29. Make 'outage' plural in Bullet c. at the top of Page 30. Capitalize 'Transmission Owner' in the 4th bullet in the middle of Page 30. Capitalize 'Owner' in the 1st line of the paragraph immediately preceeding Requirement R3. Insert 'Requirement' in front of R5 in the last line of the paragraph immediately preceeding Requirement R6. Spell out TO and TOP throughout the document. RSAW: The parenthetical statement in the 1st row of the table under Evidence Requested for R1 that states '…any risk assessments conducted prior to the effective date of this standard are not relevant…' is inconsistent with the statement on the Consideration of Issue or Directive in response to paragraph 12 of the FERC order. It states there 'This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard.' We believe the latter is consistent with the view expressed by SDT members on the two webinars conducted on April 17. This is also inconsistent with the posted Implementation Plan in which it states "The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard." Additionally, this is inconsistent with others standards in that action is sometimes taken prior to the effective date of the standard in order to be compliant when the standard becomes effective. Replace 'with' with 'within' in the 3rd row of the table under Compliance Assessment Approach Specific to CIP-014-1, R2. This is the row for R2, Part 2.2. Use lower case control center in the Note to Auditor box at the bottom of the table under Compliance Assessment Approach Specific to CIP-014-1, R4. The phrase 'and compensating mitigating measures' in the 4th row in the table under Evidence Requested for R6 goes beyond the requirement in the standard. The requirement only calls for the reasons for not modifying the security plan according to the reviewer recommendations. It doesn't require the Responsible Entity to specify how it will mitigate the discrepancy.
Individual

Amy Casuscelli
Xcel Energy
Yes
Yes
Overall Xcel Energy agrees with the approach, but we offer the following items for consideration of the Standard Drafting Team. R1 requires an assessment of facilities, including those to be in service within the next 24 months, followed by an additional review every 30 or 60 months. If a facility is brought into service, it is unclear when the review should be performed due to the 6 month gap between the in service date and the review. R2 requires a Transmission Owner to have an unaffiliated third party "verify" the risk assessment performed under R1. By contrast, R6 requires each Transmission Owner to have an unaffiliated entity "review" the evaluation performed under R4 and the security plan under R5. Xcel Energy recognizes that use of "verify" and "review" reflects the Commission's wording, but it would be helpful if the standard explained the difference between the two terms, if there is a difference. The 90 days prescribed by R2 to obtain third party verification may be too restrictive due to the availability and/or capacity of applicable resources. The standard requirement which imposes the action/deliverable by a third party, but the accountability to the TO/TOP, is also a cause for concern. It might be better to have the timing of R1 and R2 combined as this would enable flexibility of performing the assessment and completing the third party verification within the overall timeframe desired. We also suggest the Regional Entities or NERC be considered as parties that can provide third party verification and contract out if desired. It would also be helpful to expressly clarify in R2.1 that an "entity with transmission planning or analysis experience" could include a peer TO/TOP or a panel of employees from peer TO/TOPs, for example from the North American Transmission Forum. Allowing peer review would assist in identification and dissemination of best practices, we believe. R2.3 requires documentation of any recommendation to add or remove facilities as recommended by the verifying entity, but does not specify if any actions are required if no recommendations are made. Since the VRFs reference various levels of severity based upon documentation of recommendations, it would seem beneficial to allow a "no recommendations" option. Also, it is unclear if there are specific criteria the third party reviewer should utilize to review/verify and make recommendations if facilities are to be added or removed. While an entity could indicate why recommendations were or were not adopted, it would be useful to have verification criteria defined more clearly. R3 seems to be unclear in whether TOs or TOPs have operational control over facilities. In order to more clearly identify that TOPs have operational control, R3 should indicate that the TO shall notify the TOP of the identified facility.
Yes
Overall Xcel Energy agrees with the approach, but we offer the following items for consideration of the Standard Drafting Team. The rational for R4 and R5.1 indicate that there is no required timeframe to complete the evaluation of the potential threats and

vulnerabilities to identified facilities, but it does indicate the linkage of completing this when the physical security plan developed as part of R5 and within 120 days of completion of R2. We suggest that it might be more efficient to combine R4 and R5 or clearly show the linkage to reduce confusion about the timing of these two activities. Maybe the standard should require entities to develop a physical security plan after the risk assessment is completed, not after a verification of facilities as specified in R2. If R2 returns a null set, this seems ambiguous as we may still be required to have a physical security plan, even if blank. Since R4 would only be considered applicable if the R2 risk assessment process identifies facilities, referencing R4 in R5 would seem more intuitive. R5.2 states that the physical security plan must include law enforcement's contact and coordination information. However, guidance on law enforcement and coordination has already been established with the adoption of EOP-004-2. It is also unclear by what is meant by "coordination". Since reporting a physical threat to a Facility is a requirement of EOP-004-2 and in order to remove ambiguity around the word coordination, we propose changing R5.2 to read "notification of law enforcement consistent with EOP-004-2". This would avoid potential confusion whether the R5.2 requirement is different than the EOP-004-2 requirement. R6.1, While there will be some regional variances, if an entity spans multiple regions or even some governmental agency jurisdictions, what protection does an entity have against reviewer discrepancies or differences? For example, the Xcel Energy registered entities anticipate using a common risk assessment methodology, and similar security plans. It would be efficient to have a single evaluator provide the review for all three Xcel Energy registered entities. It would also be important for Regional Entities to apply consistent criteria when auditing the risk assessments and security plans. R6.1.2, if the ERO does not meet any or some parts of the criteria established in R6.1, it is uncertain how the ERO will be able to determine and approve an organization that does. Our security department, like the departments at other utilities of similar size, consists of a mix of multiple CPP and/or PSP holders, prior law enforcement professionals and several career military experts, including nuclear military asset security. It would seem that resources within the industry are the most knowledgeable resources available to evaluate physical security plans, given the criteria, and would have more utility specific knowledge than outside entities. Similar to our comments regarding R2.1, since the industry has the most knowledge on threats and vulnerabilities, and means to prevent them, we again propose adding an option to allow for industry (but non-affiliated) peer review of the physical security evaluation, either directly or through a group organization such as the North American Transmission Forum. Allowing peer review is likely to assist in identifying and disseminating best practices, thereby improving security. R6.3. Similar to our comments regarding R2.3, if no recommendations are made for changes to the evaluation by the unaffiliated reviewing entity, does this conclusion need be documented? Since some of VRFs are built off this requirement, it would seem to follow that all aspects be included to ensure certainty for the industry.

Yes

Since existing criteria from CIP-002-5.1 is used to identify facilities in scope, Xcel Energy suggests the addition of the proposed requirements be incorporated to CIP-006-5 (rather than in an entirely new standard) to more closely align and standardize the oversight of R3 and R6. In addition, this would centralize all physical security requirements within a single

Standard. Additionally, there is a significant amount of language in the requirements to specify the affected parties. We suggest the Standard Drafting Team seek opportunities to more concisely outline the applicability and the subsequent obligations in the requirements, to improve ease of understanding. We see an opportunity for the audit or risk functions of the Regional Entities to align with the third party review criteria established in the proposed standard. Although the expertise to perform this function may not currently be in place, the Regional Entities could easily develop the knowledge and expertise, and the reviews could naturally integrate within their other review and assessment activities. Overall, the standard is very comprehensive as drafted and it is balanced in a manner that allows for maximum flexibility. Consistent with NERC's evolution to results-based standards, it is appropriate for the standard to focus on the desired results of increased security of critical facilities, rather than mandating rigid actions that may or may not be suitable for individual facilities and entities. Allowing industry the latitude to design its own mitigating measures ensures those measures will be the most practical and cost effective as appropriate for the particular nature of each facility. The flexibility of this proposed standard is the best opportunity for the industry to execute a comprehensive solution based on assessments and security that relies on the unique design and characteristics of the operating systems of each utility.
Individual
Mahmood Safi
Omaha Public Power District
No
The Omaha Public Power District (OPPD), suggests replacing the term "primary control center", using the NERC defined term "Control Center", with "primary Control Center".
No
OPPD, in general, is in agreement with the approach taken in CIP-014-1 for identifying critical Transmssion stations and substations. We agree that risk assessment be conducted using transmission planning analysis, however, we suggest that this standard identifies what applicable planning analysis is used. We think the TPL standards provide the ability for the Transmission Owners to determine the worst case extreme event for identifying critical transmission stations and substations. OPPD believes that leaving R1 open and vague would encourage various interpretations of the term 'transmission planning analysis' as it applies to a 'risk assessment'. This may place the industry and the ERO in the same position as they were with the ealier versions of CIP-002 and the associated RBAM. Referencing the applicable TPL standards attemptes to remove some of this ambiguity by providing a more concise framework to evaluate those worst case extreme events. Furthermore, since TPL standards associated transmission planning analyses are performed in coordination with the PCs, risk assessment verification by PCs/RCs will not require a re-assessment of a study that has already been performed. We suggest that the SDT consider specifically defining 'transmission planning analysis' to avoid repeat of the uncertainty and vagueness associated with the CIP-002 RBAM. OPPD asks the SDT to consider revising requirement R1 as following: R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments

of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify any Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The transmission planning analysis shall be based on the applicable portion(s) of the TPL standards and specifically referenced. [VRF: High; Time-Horizon: Long-term Planning] 1.1. Subsequent risk assessments shall be performed: • At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or • At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. 1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.
Yes
Yes
OPPD believes that the third-party verifications in requirements R2 and R6, to be performed once every 60 calendar months, not each time when a risk assessment analysis or security plan is changed that does not significantly change the facilities identified or the associated security plan. The transmission entity can still perform analysis and update security plan accordingly as required by this standard, however, the third-party verification should be reserved for major changes to the assessment or the plan or otherwise be done every 60 calender months.
Individual
Bruce Metruck
New York Power Authority
Agree
APPA
Individual
Russell Noble
Public Utitliy District No. 1 of Cowlitz County, WA
American Public Power Association
No

We strongly disagree with applicability statements being outlined in the requirement. We support APPA's recommendation to further define TOP applicability in section 4.1.2 to avoid nuisance compliance certifications.
Yes
However, the TOP does not receive any relief from R1-R2 null set(s) and will be required to provide attestations to auditors and yearly certification of the absence of any notice from Transmission Owners.
No
We are very concerned with the preferential endorsement this Standard affords to ASIS International. We know of at least one other security organization that offers a security certification: the Certified Homeland Protection Professional (CHPP) designation form the National Sheriffs' Association Institute for Homeland Security. If this requirement is left unchanged, FERC's statutory obligation in determining a proposed reliability standard is "not unduly discriminatory or preferential" may trigger the standard to be remanded back to NERC. It is for this concern, and only this concern Cowlitz votes negative. However, Cowlitz plans to vote affirmative in the final Ballot, regardless of any concerns to allow NERC to meet FERC requirements.
Yes
Cowlitz commends the SDT's effort in a very difficult situation.
Individual
Dennis Minton
Florida Keys Electric Cooperative
No
• Stations and substations should be clearly understood within the standard, not just through a guidance document or rationale. It is FKEC’s understanding that a “station” equates to a switchyard that does not include transformers; and a “substation” is a facility that does include transformers. This should be addressed at the beginning of the standard document to ensure clear understanding throughout the standard. • Do stations and substations focus only on certain key assets or all assets within the facility? Some assets could be those used for local distribution and/or be below 100kV. Clarity on this is required in order to understand the full scope and appropriateness of the standard.
No
• Comments: R1.1 – FKEC recommends that the 30 months timeframe be revised to 36 months as an annual focus is more straight forward than a 2.5 year focus and it’s easier to track for internal programs and controls. 60 months should also be increased to 72 months to maintain the double timeframe that currently exists in the draft requirement. • R2 – The March 7 FERC order does not require an owner or operator to select an entity to verify its critical facilities assessment. The order uses the word “should,” not “shall” or “require.” The rationale for R2 is not accurate in this sense and should be revised to match the language in the order. Additional clarity is needed regarding what “verify” means in the standard.

Guidance and rationale is helpful, but does not carry to legal weight of the standard language. • R2.1 – This section should explicitly include NERC and the Regional Entity (RE) as a potential verifying entity. NERC and the RE should be obligated to perform this role if the owner or operator requests them to do so under this standard. There should not be a direct or indirect requirement to mandate the registered entity to hire a third party to verify the assessment portion of the standard. If a registered entity wants to hire a third party, that should be a decision the registered entity makes, but is not required for standard compliance. If a third party, other than NERC or the RE, verification of the assessment is required by the standard, then this is effectively two audits on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the standard is currently drafted. o Are there enough non-NERC/RE third parties available for what is likely to be a high demand for services, especially if there's a short time period as currently drafted? This is similar to the shortage of vendors that industry faced in theNERC facility ratings alert responses. o How is "transmission planning or analysis experience" judged by NERC compliance and enforcement? This language could be very difficult to comply with depending on the purview of the auditor. o If a registered entity hires a third party to develop and complete an assessement as required in the standard, can that third party also verify the registered entity's assessment? As drafted, the current standard could be read to require two third party entities to be hired – this would be unreasonable and the standard should be revised to clarify that only one third party would be needed to comply with the standard. • R2.2 – This requirement appears to require the third party entity to comply with language in the requirement. This does not seem to be appropriate or legal. The drafting team should revise the language to redirect the compliance burden to the NERC registered entity. In addition, the 90 day requirement could be difficult to comply with if there is a shortage of third party entities to contract with. Consideration should be given to revising this requirement to prevent a registered entity being found in violation of a requirement due to circumstances not under its control. • R2.4 – The words "exchanged with" should be changed to "made available to" in order to clarify that information may not be exchanged, but rather presented for viewing only, to a third party entity • R3.1 – The 7 day requirement appears to be unnecessarily short and not immediately necessary for BES reliability. FKEC believes 30 days is more appropriate timeframe for this requirement.

No

• It's unclear how an auditor will judge compliance with R4 and its subrequirementsas it will be uncertain what an owner or operation is aware of regarding prior history, intelligence information, etc. The language should be revised to clarify the compliance expectations and also taking into consideration that each TO and TOP may have a varied exposure to the items identified in the requirements. • R5.1 – FKEC strongly recommends the removal of "Resiliency or security" as this is not needed for the requirement and resiliency will be next to impossible to audit. • 5.3 – After the word "modifications " add ",if any," as this is a possibile outcome. • R6 – Same as comments on R2 in Question 2 above. and R2.1. • R6.1.1 – NERC standards should not endorse, or appear to endorse, ASIS or its certifications in a requirement. This should be removed. There could be other certifications that an entity may have that provides

for the necessary skills under this standard. • R6.1.2 – It is highly unlikely that the ERO is not going to approve consultants for industry use. This should be removed. • R6.1.3 – All government agencies have physical security expertise for their own facilities; that doesn't mean they can be an adequate reviewer under this standard. This should be removed. • R6.1.4 – It is unclear and not auditable whether an entity has demonstrated expertise. This language should be removed.
Yes
Under the implementation plan for R1, how can compliance with a standard be required prior to the effective date of the standard? The drafting team should reconsider this element of the implementation plan. If included in future drafts, a legal opinion from the NERC General Counsel should accompany this issue for stakeholder consideration.
Individual
Bill fowler
City of Tallahassee
Agree
APPA
Individual
Chris Scanlon
Exelon
Yes
Yes
R2.1 Drafting Team could consider adding a note to R2 Guidance section similar to that which is included in the recently approved MOD-032 standard. "Planning Authority and Planning Coordinator" (hereafter collectively referred to as "Planning Coordinator")combines "Planning Authority" with "Planning Coordinator" in the list of applicable functional entities. The NERC Functional Model lists "Planning Coordinator" while the registration criteria lists "Planning Authority" and they are not yet synchronized. Until that occurs, the proposed standard applies to both Planning Authority and Planning Coordinator."
Yes
No
Individual
Linda Jacobson-Quinn
FEUS
Agree
APPA WECC

Individual
Dean Ahlsten
Eugene Water & Electric Board
Agree
American Public Power Association (APPA)
Individual
Russ Schneider
Flathead Electric Cooperative, Inc.
Yes
No
Do not support the third party requirements, seems like a full employment effort by security consultants and others. Administratively burdensome and time-consuming at the expense of actual security improvements.
No
Again, do not support the third party review requirements. Already an auditable standard approach.
No
Individual
Steven Wickel
Public Utility District No. 1 of Chelan County
Agree
LPPC and APPA
Individual
John Yale
Public Utility District No. 1 of Chelan County
Agree
LPPC and APPA
Individual
Hugh Owen
Public Utility District No. 1 of Chelan County
Agree
APPA and LPPC comments
Group
Con Edison and Orange & Rockland
Peter Yost

No
Reliability Coordinator, Planning Coordinator and Transmission Planner should be added to the Applicability Section. That will obligate these entities to meet the 90 day review period stipulated in R2.2, if they are identified as a verifying entity by the Transmission Owner.
Yes
Yes
Yes
Section: Purpose Comment: Use of term “primary control center” should be clarified. If an entity has a primary control center and a redundant back up control center, is the back up control center also in scope for CIP-014? Requirement 1: is the intent of the Standard that the R1 risk assessment be applied to transmission stations or substations identified under Applicability 4.1.1.4, as meeting NPIRs? Requirement 4: If under Requirement R4 a Transmission Owner owns or operates a single substation that employs multiple voltage levels, then which portions of that substation would be covered by CIP-014-1 and the Entity’s physical security plan, and which would not be covered? Requirement 5: Consideration of transmission system “resiliency” is more appropriate to be applied during the R1 risk assessment, as opposed to the R5 physical security plan. Recommend moving references to resiliency to R1.
Individual
Mike Marshall
Idaho Power Co.
Yes
4.1.2. Seems vague in its description lending the reader to believe that TOPs are in scope at all times which is inconsistent with guidance later in the standard which states they are only required to perform actions when informed they are in scope by a TO. Further Clarification is needed in this section.
Yes
Further clarification is needed on several points. There is no specificity to provide consistency with how the "risk assessment" should be performed or what methodology or components to the methodology should be used. Additionally, there is no defined meaning of "widespread instability, uncontrolled separation, or Cascading within an Interconnection." Does this refer to regionally identified IROLs or some other objective criteria or only based on the analysis performed? Additionally, there is no mechanism built into R3 to allow for a dispute between a TO and a TOP if they disagree on a particular station or substation as there is in the third party reviews under R2 and R6 where there is a mechanism to disagree with the reviewer.
Yes

Further clarification is needed on several points. 4.2 & 4.3 leave open much room for interpretation under audit to say you did or didn't consider a particular source or threat. There is also some consternation over the use of "potential threat" in this requirement. There are a great many potential threats many that are so remote and nearly impossible to protect against that the risk does not outweigh the cost. It seems like these sub-requirements are a potential audit findings trap by the way they are worded. There are also no criteria specified for what the unaffiliated third party will be looking for in their review of the entity's evaluation. There is a great deal of concern for how these third parties will be able to handle or be willing to handle the influx of these reviews especially considering the short 90 day timeframe listed in 6.2.
Yes
There is great concern related to information protection related to turning over information concerning vulnerabilities of the grid and related facilities to outside parties. Even with the use of NDAs, these third parties are not subject to the same NERC reliability standards (i.e. CIP standards, information protection, etc) as the entities, will not be audited on their information protection practices, and may have no accountability to the regulators in the event of a disclosure of sensitive information, inadvertent or otherwise. It is a concern that the TO is responsible for 3rd party verification to be completed within a tight 90 day window, especially considering the critical infrastructure information being exchanged. Contractual exchanges and negotiations could impede upon the 90 day window. Also, TO's may need time to review the R2 study results and possibly mitigate study discrepancies. The date R1 needs to be performed is unclear. Does it need to be performed within a certain amount of time after the effective date? The implementation plan states that the initial risk assessment must be performed on or before the effective date of the standard. However, the RSAW for R1 states that "any risk assessments conducted prior to the effective date of this standard are not relevant." Does this mean the initial risk assessment must be performed “on” the actual effective date of the standard? Is there a basis for the short notification window in R3? The seven calendar days window for the TO to notify the TOP seems quite short. Additionally, there is a discrepancy in the review timeframes in R1 in which a look ahead of 24 months is required for stations and substations that are in the planning process but the risk assessments are performed every 30 months leaving a 6 month gap in the analysis. It would also seem more intuitive and consistent with other CIP standards to have the risk assessment requirement performed on an even year rather than a 30 month basis (i.e. 36 months.)
Individual
Chad Bowman
CHPD
Agree
CHPD is supportive of the comments submitted by APPA
Group
ACES Standards Collaborators
Ben Engelby

Yes
We support a clear and defined “bright line” criteria that has been industry vetted and FERC approved as the starting point for the risk assessment in R1.
No
(1) Conceptually, we agree with this approach but have identified the following issues and concerns. (2) R1 requires additional clarification. The Guidelines and Technical Basis section states that the “bright line” criteria in applicability section is used to identify an initial set of stations and substations that must be further evaluated in R1. It is our understanding that if a TO owns one 500 kV transmission station and no other transmission facilities, then that 500 kV station would meet the applicability section 4.1.1.1 criteria. The TO would be required to perform a risk assessment to identify if that facility was rendered inoperable, it could result in widespread instability, uncontrolled separation, or Cascading in an Interconnection. In other words, if the applicability section is met, the TO must perform a risk assessment, but the remainder of the standard (R4-R6) would not apply unless loss of the Facility would result in widespread instability, uncontrolled separation or Cascading. Please confirm if our understanding of applying the requirements is the correct approach. (3) We see a significant compliance risk created by Requirement R2 and question why the unafilliated third party verification cannot be integrated into the Regional Entity compliance monitoring and enforcement processes to minimize costs and limit access to highly sensitive information. The third party verification creates a compliance problem outside of the TO’s control because the TO is dependent on a third-party for regulatory compliance and there is no obligation on any of the third parties (i.e. RC, PC) identified in the standard to verify the risk assessment. Thus, the TO will have to rely on consultants to perform the verification. Since all TOs will be working towards the same efffective date, there will be a backlog and the reviews may not be completed by the timelines established in the standard. Review by consultants also will increase the number of people with access to highly sensitive information. While this concern can be partially mitigated through confidentiality agreements, the more people that have the information, the higher the probability the information will be released, whether intentional or unintentional, to persons that should not have the information. All of these issues could be resolved if NERC and Regional Entities conducted the review. The review could be performed as part of a spot check of the standard 90 days after the initial effective date. If NERC or the Regional Entity disagree with the approach or believe additional facilities should be added, RAI would give them the flexibility to treat the issue as not impactful to compliance as long as the TO resolved the issue within a certain time period. This approach would result in a reduced cost impact on industry and minimize the distribution of highly confidential information reducing the likelihood of information leaks. As an alternative, we suggest that a companion requirement that compels either the RC or PC to perform the verification. This would also reduce the costs impacts and distribution of sensitive information since these entities will already be familiar with the TOs they are verifying and will already have access to highly sensitive information. (4) Regarding R3, this requirement does not warrant a 7-day timeline. This is not a near real-time issue. We suggest 30 days as a reasonable notification period.
No

(1) We see a significant risk of the compromise of highly sensitive information created by Requirement R6 and question why the unaffiliated third party review cannot be integrated into the ERO compliance monitoring and enforcement processes. There is no compliance obligation on these third parties to complete the review within the required timelines, which could subject the TO to potential compliance violations. Furthermore, there is a limited set of companies with qualified personnel capable of performing this review. Given that all of the Transmission Owners will be working toward the same effective date of the standard, it is highly likely that a backlog of work would occur. Furthermore, review of the evaluations by consultants will increase the the number of people with access to higly senstivie information. While this concern can be partially mitigated through confidentiality agreements, the more people that have the information, the higher the probability the information will be released, whether intentional or unintentional, to persons that should not have the information. To resolve this inssue, NERC and Regional Entities could hire qualified personnel to perform these reviews. NERC and Regional Entities could perform a spot check of the standard 90 days after the initial effective date. If NERC or the Regional Entity disagree with the approach or believe additional facilities should be added, RAI would give them the flexibility to treat the issue as not impactful to compliance as long as the TO resolve the issue within a certain time period. This approach would result in a reduced cost impact on industry and minimize the distribution of highly confidential information reducing the likelihood of information leaks. (2) How can the 'cost to benefit to risk to the BES' be measured consistently across each facility, region and risk? Does a Registered Entity have to authority to not implement a 'recommendation' from a third party based upon a cost to benefit to risk analysis? (3) Given that third parties are required to evaluate critical facility information, further guidance is needed for the required controls to prevent unintended release of highly sensitive and confidential information. What is the risk to the Registered Entity if the information does get leaked? Is this a violation to the Registered Entity, even if the leaked information was not caused by the Registered Entity? We are concerned that if this information were to be leaked, the Registered Entity could be liable for increased risk of attack, additional time and costs to address the leak and could impact the BES due to changes in operations from shutting down those facilities. (4) Part 4.2 has a potential "prove the negative" issue. How do you prove that you considered similar facilities particularly when similar facilities could includes other company's facilities. To resolve this issue we suggest replacing "similar" with "nearby facilities" or "asset owner's other facilities in the area". (5) Part 4.3 could be interpreted as requiring consideration of all threat and intelligence information including information that is not relevant to a given area. To remedy this issue, we recommend using the term "current and local" to describe the types of intelligence and threats that must be considered. (6) We believe that Part 5.2 is redundant to the EOP-004-2 – Event Reporting, especially Attachment 2 Event Reporting Form line 4. Please consider removing and comparing the standard in its entirety to EOP-004-2 to avoid unnecessary duplication. (7) For Part 5.4, please modify the language to clarify that it only applies to facilities identified as a result of application of Requirements R1 and R2. (8) For Part 6.1 please modify "… from the following" to "… from one of the following". This will make it perfectly clear that only one entity must be selected.
No

Thank you for your time and consideration.
Individual
David Thorne
Pepco Holdings Inc.
Yes
Yes
Yes
Yes
There seems to be a conflict between the RSAW, Consideration of Issues or Directives and the Timeline included in the FAQ. To meet the overall timeline for the entire standard, the risk assessment must be started prior to the Effective date of the standard. There should be no prohibition for completion of the Risk Assessment prior to the Effective date of the standard. The FAQ Timeline states: “Initial performance of R1 must be complete on or before the effective date of the standard…” The Consideration of Issues or Directives #12: “…This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard…” The RSAW under R1 Evidence Requested states: “Provide the current and the immediately preceding risk assessments conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant).”
Group
American Public Power Association (APPA)
Allen Mosher
Yes
APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members. CONTROL CENTER - Use the defined term “Control Center” by capitalizing as “primary Control Center” or explain why lower case “primary control center” is different and needs to be used in the standard. Consider inserting “with operational control” after primary Control Center, to express the intent of the text box Rationale for Requirement R1 that the control center must be capable of taking electronic actions that can cause direct physical actions at the identified station or substation. Please also clarify whether the periodic use of a

backup control center as the entity's primary control center would make R4 and R5 applicable to both the primary and backup control centers. UNAFFILIATED - needs to be either defined or a footnote needs to be added to the standard to explain that "unaffiliated means that the selected verifying or reviewing entity cannot be a corporate affiliate," as stated in the guidance section. CONFIDENTIALITY Publicly Owned Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the A. Introduction section, after 6. Background: 7. Critical Facilities Information Records and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. ALTERNATIVE PROPOSED REQUIREMENT LANGUAGE ADDITIONS: R1.3 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under this standard. R3.2 The Transmission Owner will keep confidential all records and information related to the notifications conducted under Requirement R3 and R3.1 of this standard. R4.4 The Transmission Owner and each applicable Transmission Operator will keep confidential all records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1. APPA suggests technical edits to Requirements R2.4 and R6.4 to insert "or made available to" after "exchanged with." This change would clarify that sensitive or confidential information does not have to be actively "exchanged" between entities to be subject to the protections directed under Requirements R2.4 and R6.4. APPLICABILITY 4.1.2 - The applicability section for Transmission Operators under section 4.1.2 should be explicitly limited to each TOP that operates a primary Control Center and receives a verified notification under Requirement R3. As written each TOP would

be required to certify on each compliance contact that it has not been notified that it operates an applicable primary control center. The following edited text would accomplish that objective: 4.1.2 Transmission Operator that operates a primary Control Center and receives notice from a Transmission Owner under Requirement R3. Please also confirm that the Transmission Operator of a primary control center is not responsible for conducting a risk assessment under R1 or arranging for third party verification of the risk assessment under R2.
Yes
APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members. TIMELINES to complete third party verification under R2 and third part review under R6 are both too short. Increase 90 days to 120 days or 180 days. Verifying entities may recommend that the Transmission Owner conduct additional planning studies to confirm asset identifications such as interactions between BES Elements in adjacent Transmission Owner footprints. A short 90-day time limit may not be sufficient time to conduct and verify a revised or supplemental BES assessment. For security reviews, conducting a meaningful review with sound recommendations applicable to a specific TO's or TOP's facts and circumstances may also take time along with necessary discussions with the TO. A short review window is more likely to lead to disagreements with the TO which in turn would lead to discrepancies that would need to be justified – which in turn might cause the reviewer to avoid making proposals that should be considered by the TO or pressure on the TO to accept recommendations that could be improved upon. R1 GUIDANCE - TRANSMISSION PLANNING BASE CASES: Please revise the Guidance for R1 to clarify that TOs should start their initial and subsequent risk assessments with a common regional or area transmission planning base case used for transmission planning purposes. The base case should include existing BES stations and substations and those planned to be in service within 24 months within the region or area, to ensure forward-looking risk assessments and security planning. R2 VERIFICATION - Third party verification of third party risk assessments conducted under R1: some medium sized TOs with applicable transmission stations and substations may contract with a third party consultant to conduct necessary BES risk assessments, to ensure accurate and comprehensive consideration of the risk of widespread cascading, instability and uncontrolled separation. Such entities seek clarification that a single expert risk assessment study, in conjunction with a verification by an unaffiliated PC, TP or RC would suffice.
Yes
APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members. R4 CLARITY - Under R4, combining the applicability of this requirement to both TOs and TOPs with applicable control centers within a single sentence is confusing and could be read to imply that a TOP that is affiliated with a TO must arrange for a separate third party review. We recommend revising R4 to read as follows: R4 Each Transmission Owner that

owns a Transmission station or Transmission substation identified in Requirement R1 and verified according to Requirement R2, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s) and Transmission substation(s), identified in Requirement R1 and verified according to Requirement R2. Each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to their primary control center identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: [VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning] R4.2 TYPO – Please change: "Prior history or attack..." to "Prior history OF attack..." Make conforming edits to the RSAW. 30-MONTH CYCLE - Identification of new threats and vulnerabilities in R5.4 does not change the 30-month cycle for conducting reliability studies and security evaluations: The standard needs to make clear that the security plan needs to take into account threats and vulnerabilities that are known at the time the plan is developed and the approved plan is capable of addressing new threats and vulnerabilities as they emerge, but that there is no NERC requirement to revise the plan between 30 month cycles and for the NERC CEA to audit such revisions. The TO should apply its existing security plans and procedures to evaluate and mitigate evolving security threats. The TO may also revise the security plan in mid-cycle if it so chooses without arranging for a third party review, but that action does not obviate its obligation to conduct the "subsequent" risk assessment and threat evaluation and security plan on the 30 month cycle. The CEA will audit the processes the TO uses to develop its plans, rather than the content of the plans. REQUIREMENT R5 CLARITY – R5 states in part that each TO and TOP "shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2." Please change "implement" to "complete." The use of implement can easily be read to require the actual implementation of physical security measures within 120 days, rather than the completion of the security plan, starting the 90 day clock for unaffiliated third party review under R6. In contrast, R6 states that: "The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5."

Yes

APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members. See comments on definitions under Question 1. RSAW for R1 poses the following question: "As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?" This question combines a multi-step process into a single question that cannot be answered as yes or no by many TOs. Please break the RSAW for R1

into three discrete questions: 1…Do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1? 2…Have you conducted a risk assessment of each applicable station or substation identified under Applicability section 4.1.1.? 3…Did the risk assessment identify one or more Transmission station(s) and/or Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection? RSAW R1 evidence request text from near the top of page 6: (R1) Provide the current and the immediately preceding risk assessments conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant). The draft Implementation Plan states that the risk assessment required by R1 "must be completed on or before the effective date of the standard," yet the RSAW language provided above seems to exclude such an assessment. RSAW R1 "Note to Auditor" on page 7: “Review entity’s answer to the above Question and if the auditor can verify the answer is ‘no,’ Requirements R3-R6 do not apply and no further audit testing of Requirements R3-R6 is necessary.” The text appears to reference the following question from page 6: “As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?” This question is poorly worded, because TOs not meeting the applicability requirements of 4.1.1 are effectively exempt from this standard and do not need to perform a risk assessment. RSAW R3 "Question" on page 11: Please reword to add the following all caps text: “Are THERE any primary control centers identified in Requirement R1, Part 1.2 THAT ARE not under operational control of your NERC registration? RSAW R4 "Compliance Assessment Approach" on page 14: Change “or” to “OF” (R4 Part 4.2) “Prior history OF attack...” See the language used in the Guidelines and Technical Basis on page 31 of the standard. RSAW R5 "Note to Auditor" on page 16 states: “Auditor should cross reference the Transmission stations/substations and primary Control Centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 and the security plan(s) prescribed in Requirement R5 to ensure the plan addresses vulnerabilities that would facilitate physical attacks that have a high probability or likelihood of occurrence.” The requirements of the standard do not address "probability" or "likelihood" of occurrence, so these factors should not be in scope of the compliance audit. Rather, auditors should address whether the security plan is complete and the TO or TOP addresses the issues raised by the third-party reviewer.
Individual
Melissa Kurtz
US Army Corps of Engineers
Agree
Western Area Power Administration
Individual
Shirley Mayadewi
Manitoba Hydro

Yes
Yes
No
(1) Manitoba Hydro has concerns about the need to have a third party to review or verify risk assessments and physical security plans. It is unclear at this point what measures or counter measures are being alluded to here as far as protecting critical assets such as lines and towers. This may potentially be financially burdensome as well as questionably effective. (2) Also missing in the standard is conflict resolution between a TO and this third party reviewer. Clarification should be provided on who weighs in on this and how NERC audits a system that has been verified by a third party. As currently drafted it appears that the third party reviewer/verifier would have no liability under the standard.
Yes
(1) R6.1 – It is not clear whether only one or all of the qualifications in Section 6.1.1 through 6.1.4 must be met. Accordingly, R6.1 should be rephrased to refer to “one of the following”.
Individual
Debra Warner
self
No
While the reqirement for unafflilated third party verification of the security plan is required by the FERC order, I believe the mandate will lead to future security compromises.
Group
FirstEnergy
Doug Hohlbaugh
Yes
Yes
FirstEnergy supports the proposed requirements R1 through R3.
Yes
FirstEnergy supports the proposed requirements R4 through R6 but offers two comments: 1) In regard to the inclusion of “primary control centers,” we suggest the team add language within the Guidelines and Technical Basis section for requirement R4 and potentially the inclusion of an additional FAQ item to document some of the team’s feedback provided

during the webinar sessions. During the webinar the team provided a good explanation of how CIP-014 is uniquely different than physical protections provided under CIP-006 and that CIP-014 provides perimeter protection of the primary control center location or site and not just the subset of the control center that may house cyber assets protected under CIP-006. 2) Regarding requirement R5, during the industry webinars it became evident that there is some confusion associated with the word “implement” as used in the statement “shall develop and implement a documented security plan(s)” and that some industry stakeholders questioned if implement intended completion of all identified tasks stated within the plan(s). While FirstEnergy understood the requirement as described by the team during the webinars, to alleviate any confusion and better clarify the intended application, FirstEnergy suggests changing “implement” to “initiate” or “issue” so that it reads “shall develop and initiate a documented security plan(s)”. This wording may better align with part 5.3 and the guidance provided in the Guidelines and Technical Basis section that states “Entities have the flexibility to prioritize the implementation of the various resiliency or security measures in their security plan according to risk, resources, or other factors.”
No
FirstEnergy supports the proposed standard and appreciates the teams consideration of our comments intended to help clarify a few areas of the standard. FirstEnergy appreciates the team’s efforts in producing a quality standard within an expeditious schedule and believes the team has provided a product that meets the core expectations described by the FERC Order.
Group
Seattle City Light
Paul Haase
Yes
Seattle City Light supports the Question 1 comments of APPA, with one exception in the area of Confidentiality. Seattle's comments about Confidentiality, in place of APPA's comments on this topic, follow. CONFIDENTIALITY The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the Introduction Section: 7. Critical Facilities Information Records and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be

kept confidential by the owner of the records and information, those entities with authorized access to the records and information, and any agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. Proposed Requirement Language: R1.3 Records and information related to the risk assessments conducted under this standard that are designated confidential by the Transmission Owner are [intended to be] exempt from public disclosure. R3.2 Records and information related to the risk assessments conducted under Requirement R1 of this standard that are designated confidential by the Transmission Owner are [intended to be] exempt from public disclosure. R4.4 Records and information related to the evaluation of physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and/or Control Center(s) identified in Requirement R1 conducted under this standard that are designated confidential by the Transmission Owner or Transmission Operator are [intended to be] exempt from public disclosure.

Yes

Seattle City Light supports the Question 2 comments of APPA as well as the additional comments of Salt River Project (SRP) regarding 3rd party verification. Third Party Verifiers (SRP): SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or

fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities. Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers. Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
Yes
Seattle City Light supports the Question 3 comments of APPA.
Yes
Seattle City Light supports the Question 4 comments of APPA.
Group
SPP Standards Review Group
Robert Rhodes
No
We have some concern with the undefined term ‘collector bus facility’. Without a definition for collector bus facility some may consider the entire switchyard at a generating station as a collector bus facility. We do not believe the drafting team intended this to be the case. Therefore, some additional clarification may be needed for the term.
No
The Standard intentionally does not provide specific methodologies regarding the type of analyses needed to be conducted for the assessments in R1. This leaves the door open to very different interpretations across the industry. We suggest the drafting team consider specifying analyses such as those contained in the TPL standards. This would eliminate

confusion within the industry and provide clear direction for those conducting the analyses. We suggest adding the following sentence at the end of R1. “These analyses will include consideration of the entire loss of the Transmission stations and Transmission substations specified in Applicability Section 4.1.1 taken individually, one at a time.” While not specifically referencing the TPL standards (currently enforceable TPL-004-0a, R1 and TPL-001-4, R3 to be enforced in 2016) which cover the loss of switching stations and substations, this language provides guidance regarding the type of analyses to be conducted in the assessments. We strongly suggest that the SDT expand on this addition to R1 in the guidance document to provide needed clarification to the industry.
Yes
Yes
Effective Date: The use of the term ‘implement’ needs clarification . To some implement means installed and in-service. To others it could mean a work in progress. The SDT recognized this confusion in the webinars on April 17 and we encourage them to modify the language to more clearly indicate the intent of the drafting team. VSLs: Capitalize Part 2.3 in the Lower, Moderate and High VSLs for R2. Insert ‘and verified according to Requirement 2’ following the reference to Requirement R1 in all the VSLs for R5. Delete ‘and modify or’ in the last High VSL for R6. Guidelines and Technical Basis: Replace ‘drafting team’ with ‘SDT’ in the last paragraph under Section 4 Applicability on Page 27. Make the same change in the last paragraph on Page 32 under Requirment R6. Capitalize Remedial Action Schemes (RAS) and Special Protection Systems (SPS) in the paragraph at the top of Page 29. These are defined terms in the Glossary. Insert ‘Transmission’, capitalize ‘Owner’ and delete ‘or operator’ in the 1st paragraph under Requirement R2 on Page 29. Make ‘outage’ plural in Bullet c. at the top of Page 30. Capitalize ‘Transmission Owner’ in the 4th bullet in the middle of Page 30. Capitalize ‘Owner’ in the 1st line of the paragraph immediately preceeding Requirement R3. Insert ‘Requirement’ in front of R5 in the last line of the paragraph immediately preceeding Requirement R6. Spell out TO and TOP throughout the document. RSAW: The parenthetical statement in the 1st row of the table under Evidence Requested for R1 that states ‘…any risk assessments conducted prior to the effective date of this standard are not relevant…’ is inconsistent with the statement on the Consideration of Issue or Directive in response to paragraph 12 of the FERC order. It states there ‘This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard.’ We believe the latter is consistent with the view expressed by SDT members on the two webinars conducted on April 17. This is also inconsistent with the posted Implementation Plan in which it states “The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard.” Additionally, this is inconsistent with others standards in that action is sometimes taken prior to the effective date of the standard in order to be compliant when the standard becomes effective. Replace ‘with’ with ‘within’ in the 3rd row of the table under Compliance Assessment Approach Specific to CIP-014-1, R2. This is the row for R2, Part 2.2. Use lower case control center in the Note to Auditor box at the bottom of the table under Compliance Assessment Approach Specific to CIP-014-1, R4. The phrase ‘and compensating mitigating measures’ in the 4th row

in the table under Evidence Requested for R6 goes beyond the requirement in the standard. The requirement only calls for the reasons for not modifying the security plan according to the reviewer recommendations. It doesn't require the Responsible Entity to specify how it will mitigate the discrepancy.
Group
Colorado Springs Utilities
Shannon Fair
CSU agrees with APPA comments with exception to the confidentiality section, please see CSU's comments below. CONFIDENTIALITY Publicly Owned Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the A. Introduction section, after 6. Background: 7. Critical Facilities Information Records and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. ALTERNATIVE PROPOSED REQUIREMENT LANGUAGE ADDITIONS: R1.3 All records and information related to the risk assessments conducted of this standard are exempt from public disclosure. R3.2 All records and information related to the notifications conducted under Requirement R3 and R3.1 of this standard are exempt from public disclosure. R4.4 All records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1 of this standard are exempt from public disclosure. Adding confidential in the standard would create undo compliance burden and auditing challenges.

Yes
Yes
Yes
Yes
Individual
Barry Lawson
National Rural Electric Cooperative Association (NRECA)
No
Stations and substations should be clearly understood within the standard, not just through a guidance document or rationale. It is NRECA's understanding that a "station" equates to a switchyard that does not include transformers; and a "substation" is a facility that does include transformers. This should be addressed at the beginning of the standard document to ensure clear understanding throughout the standard. Do stations and substations focus only on certain key assets or all assets within the facility? Some assets could be those used for local distribution and/or be below 100kV. Clarity on this is required in order to understand the full scope and appropriateness of the standard.
No
R1.1 – NRECA recommends that the 30 months timeframe be revised to 36 months as an annual focus is more straightforward than a 2.5 year focus and it's easier to track for internal programs and controls. 60 months should also be increased to 72 months to maintain the double timeframe that currently exists in the draft requirement. R2 – The March 7 FERC order does not require an owner or operator to select an entity to verify its critical facilities assessment. The order uses the word "should," not "shall" or "require." The rationale for R2 is not accurate in this sense and should be revised to match the language in the order. Additional clarity is needed regarding what "verify" means in the standard. Guidance and rationale is helpful, but does not carry to legal weight of the standard language. R2.1 – This section should explicitly include NERC and the Regional Entity (RE) as a potential verifying entity. NERC and the RE should be obligated to perform this role if the owner or operator requests them to do so under this standard. There should not be a direct or indirect requirement to mandate the registered entity to hire a third party to verify the assessment portion of the standard. If a registered entity wants to hire a third party, that should be a decision the registered entity makes, but is not required for standard compliance. If a third party, other than NERC or the RE, verification of the assessment is required by the standard, then this is effectively two audits on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the standard is currently drafted. Are

there enough non-NERC/RE third parties available for what is likely to be a high demand for services, especially if there's a short time period as currently drafted? This is similar to the shortage of vendors that industry faced in the NERC facility ratings alert responses. How is "transmission planning or analysis experience" judged by NERC compliance and enforcement? This language could be very difficult to comply with depending on the purview of the auditor. If a registered entity hires a third party to develop and complete an assessement as required in the standard, can that third party also verify the registered entity's assessment? As drafted, the current standard could be read to require two third party entities to be hired – this would be unreasonable and the standard should be revised to clarify that only one third party would be needed to comply with the standard. R2.2 – This requirement appears to require the third party entity to comply with language in the requirement. This does not seem to be appropriate or legal. The drafting team should revise the language to redirect the compliance burden to the NERC registered entity. In addition, the 90 day requirement could be difficult to comply with if there is a shortage of third party entities to contract with. Consideration should be given to revising this requirement to prevent a registered entity being found in violation of a requirement due to circumstances not under its control. R2.4 – The words "exchanged with" should be changed to "made available to" in order to clarify that information may not be exchanged, but rather presented for viewing only, to a third party entity R3.1 – The 7 day requirement appears to be unnecessarily short and not immediately necessary for BES reliability. NRECA believes 30 days is more appropriate timeframe for this requirement.
No
It's unclear how an auditor will judge compliance with R4 and its subrequirements as it will be uncertain what an owner or operation is aware of regarding prior history, intelligence information, etc. The language should be revised to clarify the compliance expectations and also taking into consideration that each TO and TOP may have a varied exposure to the items identified in the requirements. R5.1 – NRECA strongly recommends the removal of "Resiliency or security" as this is not needed for the requirement, and resiliency will be next to impossible to audit. 5.3 – After the word "modifications " add ",if any," as this is a possibile outcome. R6 – Same as comments on R2 in Question 2 above. and R2.1. R6.1.1 – NERC standards should not endorse, or appear to endorse, ASIS or its certifications in a requirement. This should be removed. There could be other certifications that an entity may have that provides for the necessary skills under this standard. R6.1.2 – It is highly unlikely that the ERO is going to approve consultants for industry use. This should be removed. R6.1.3 – All government agencies have physical security expertise for their own facilities; that doesn't mean they can be an adequate reviewer under this standard. This should be removed. R6.1.4 – It is unclear and not auditable whether an entity has demonstrated expertise. This language should be removed.
Yes
Under the implementation plan for R1, how can compliance with a standard be required prior to the effective date of the standard? The drafting team should reconsider this element of the implementation plan. If included in future drafts, a legal opinion from the NERC General Counsel should accompany this issue for stakeholder consideration.

Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Yes
Yes
Yes
Yes
ATC supports the draft standard, with the realization that the aggressive time line has raised a broad range of issues or ambiguities resulting from the use of vague language or generic terms. While ATC understands the necessity for this approach, given the compressed timeframe directed by the FERC Order, the project's condensed timeline may not have afforded for the necessary and careful consideration of these terms. Improved guidance around the application of generic terms would increase clarity and help the industry. ATC also supports a follow up effort commensurate with typical standards drafting processes and timeframes to allow for further consideration, improvement, and cleaner language to assure effective implementation of the standard. An example of language like this is in Requirement R1, which includes the vague terminology of "widespread instability, uncontrolled separation, or Cascading." Risk assessment findings can vary significantly depending on the assumptions, criteria, and methodology used for the assessment, and a more thoughtful use of terms could provide for a more uniform risk assessment basis.
Individual
Brian Evans-Mongeon
Utility Services
No
We have seen in the previous versions of the CIP standards that "Risk Assessments" are not performed consistently, and create more problems than they solve, and even violation determinations. The solution in CIP-014 to this inherent problem seems to just add another level of review, but there is no guarantee of consistency within these assessments. Additionally, it seems the drafting team is suggesting a single assessment ("Concurrent with R1 study" specified in R2), this this might eliminate the review stage all together. A clear applicability section with a "brightline" approach would be more appropriate and consistent with the progression of the CIP standards overall. Otherwise, what prevents an auditor from making a determination that the assessment performed was not sufficient or incomplete, even with a 3rd party validation? Entities need a clear definition to avoid the problems of the past. If the drafting team wants to limit the scope of Facilities this could be detailed in the "Exemptions" portion of the "Applicability" section of the standard. 1. The "Exemption"

section needs to be clarified. If this applies to the entire section number it 4.2. If it is only applicable to the last bullet it is under give it the appropriate number (4.1.2.1) Suggested re-write 4. Applicability: 4.1. Functional Entities: 4.1.1 Transmission Owner 4.1.2 Transmission Operator 4.2. Applicable Facilities: The following Facilities, systems, and equipment, owned or operated by each Responsible Entity in 4.1 above are those to which these requirements are applicable. 4.2.1 Transmission Facility operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. 4.2.2 Transmission Facility that operate between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. ADD TABLE HERE 4.2.3 Transmission Facility at a single station or substation location that is identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies. 4.2.4 Transmission Facility at a single station or substation whose unplanned unavailability would result in the loss of at least 3000 MW of generation. 4.2.5 Control Center that controls: 4.2.5.1 Transmission Facilities identified by identification under 4.2.1 through 4.2.4; or 4.2.5.2 Two or more Facilities which contain a Cyber System(s) which have been identified as a High or Medium Impact BES Cyber System. 4.2.6 Exemptions: 4.2.6.1 All facilities regulated by the Nuclear Regulatory Commission or Canadian Nuclear Safety Commission. 4.2.6.2 Transmission station or substation connected to only one other Transmission station or substation. 4.2.6.3 Transmission station or substation that does not operate above 200kV. 4.2.6.4 control centers not designated as a “primary control center”
No
1. What is a Transmission “station”? What is the definition of station and what is it intended to cover that substation does not. Generally in the NERC glossary “station” is associated with Generation, not Transmission. 2. There is a concern between R1 and R5. a. R1 states that substations planned to be in service within 24 months should be identified, which would presumably be for stations under construction. b. R5 will then require a Physical Security plan to be in place within 120 days of identification, regardless of the current status of the station. c. Possibly adjust language to allow sites under construction to have the later of 120 days or the operation date of the station. 3. R1.2 should be reworded: “The TO shall identify the primary Control Center with operational authority of each Facility identified in the R1 risk assessment.” 4. R2, if the assessments are concurrent, could this be a joint effort, with the result being 1 report? 5. R2.1, “unaffiliated” needs some clarification. Is this unaffiliated with the TO in any way? Could the TO use their Planning Coordinator, Transmission Planner or RC for the assessment, or do they need to seek out an entity from another region?
Yes

1. R4, what is the time frame for the evaluations? Is this to be conducted during the 30 or 60 month cycle outlined in R2 or more frequently? 2. R6.1, These are all “or” statements and 6.1.1 through 6.1.4 should be bullets, not numbers (this is outlined in the CIP-002-5 page 6, and should maintain consistency with the CIP standards format). 3. R6, Does the ERO have to approve of the third party reviewer? Is there going to be a criteria to determine “demonstrated physical security expertise”?
Yes
1 “primary control center” is confusing. NERC has a defined term “Control Center” which is intentionally not being used. What is the intent of not using the defined term? If the undefined term remains in use more clarity needs to be given on “primary control center”. 2. what is the definition of “widespread?” Does this mean outside of a Balancing Authority Area, outside of a Region or outside of an interconnection? More clarity is needed in the term. Additionally, TO’s may not have the data required to perform this type of assessment. There needs to be process in place for the TOs to obtain the data required to perform the appropriate assessment. 3. The SDT should review projects such as PRC-006 or MOD C, and define groups within the requirements to reduce the length of requirements. For example R4 could be reduced to the following, making the requirement easier to read and adding much needed clarity: “Each Applicable Entity shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Applicable Facilities as identified in R1 and verified in R2. The evaluation shall consider the following:… “ RSAW Comment: R1 “Evidence Requested” section doesn’t provide a time frame for the first assessment, no assessment prior to effective date will be considered, but there must be an assessment completed before the effective date to be complaint. This is a catch 22.
Individual
Dan Inman
Minnkota Power Cooperative
Yes
Yes
Yes
Yes
In the “Draft_RSAW_CIP-014-1_v1_2014_0409.pdf” document, on page 4 of 22, there is a Note to Auditors Concerning Third Party Verifications and Reviews. In this section there is a mention to the “concept of reliance means using the work of others to avoid duplication of efforts”. While the reference to “duplication” was in regards to unaffiliated third party verifications and reviews, we appreciate the SDT be congnitive of “duplication of efforts” as their developing the Standard and the RSAW. With the very restrictive timeframe for which the development of the Standard was required, this concept can get lost. We did see another

area in the Standard CIP-014-1 R5.2, which may be considered “duplication of efforts”. CIP-014-1 R5.2 states, the TO/TOP should have in their physical security plan(s) law enforcement contact and coordination information. On June 20, 2013, FERC approved Reliability Standard EOP-004-2, which identified types of reportable events and thresholds for reporting, requires responsible entities to have an operating plan for reporting applicable events to NERC and other entities (including law enforcement), and requires reporting of threshold events with a 24 hour period (Docket No. RD13-3-000). This Standard covers the need to incorporate law enforcement contacts in the operating plan. Requesting this type of information in both the operating plan required in EOP-004-2 and physical security plan in CIP-014-1 is a “duplication of efforts”. MPC believes the intent for CIP-014-1 was to identify and mitigate physical security risks, while the intent for EOP-004-2 is to improve reliability of the BES by requiring the reporting of events by Responsible Entities. MPC suggests removing Requirement 5.2 in CIP-014-1.
Individual
John Allen
City Utilities of Springfield, Missouri
Agree
APPA
Individual
kim moulton
Vermont Transco LLC
Yes
While we do agree with the need for the standard and the importance of it we do have comments on the proposed standard. The intention of this standard is to protect those facilities that are most critical to the bulk electric system. The CIP-002-5.1 criteria brings into play many facilities that while deemed critical to an entity are not likely critical to this standards definition and would not cause wide area impact.
Yes
Specifically the filtering of assets. While starting with CIP-002-5.1 as a starting point, the amount of analysis and assessment to determine if these facilities are critical and applicable to this standard may not be possible in the timeline proposed for this standard if a full transmission planning analysis will be needed. Many planning analysis performed previously by entities were not assessed to the specific defininition included in this requirement and therefore could require considerable work to be performed to analyze. The wording suggests that a full transmission planning assessment should be performed for all CIP-002-5.1 facilities and not to just those an entity feels may cause wide area impact. What if you do not agree with the third parties review of your assessment? what evidence will be required to prove that you do not need to agree with their assessment? If an entity identifies a facility as critical does this require that the control center operating this facility must also have a full physical security plan per the requirements later in the standard?

Yes
how long will and entity have to complete their plans designed due to the evaluation of threats? It appears that the standard is saying that you must develop a plan and a timeline to complete your actions associated with the plan. What if a timeline needs to be adjusted at some point, will an entity have to notify their RRO? Or just track all changes and their need to provide to an auditor during a full audit of the standard?
No
Group
Western Area Power Administration
Lloyd A. Linke
Yes
Western agrees with what we understand as the applicability, based on the CIP-014 Workshops. However, we have some concern with the undefined term 'collector bus facility'. Without a definition for collector bus facility we are concerned that some parties may consider the entire switchyard at a generating station as a collector bus facility. Based on the discussion during the CIP-014 Workshops we do not believe the drafting team intended this to be the case. Therefore, some additional clarification may be needed for the term.
Yes
Western agrees with the approach of using Requirements R1 and R2 to identify whether an entity is subject to Requirements R4-R6. However, we suggest that the drafting team modify the term "risk assessment" to "BES impact assessment." In the physical security community, the term "risk assessment" generally refers to "The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel." See ASIS International, General Security Risk Assessment Guideline (2002), http://www.scnus.org/local_includes/downloads/9200.pdf. In its filing to FERC, NERC can explain that it adopted the term "BES impact assessment" so it is clear that the initial evaluation is of risk to the BES if the substation is damaged or rendered inoperable. Western recommends revising R1 1.1 to: "Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment." This would consolidate the two bulleted actions and make them equally applicable. We believe a 60 month interval would be a more appropriate period for this type of assessment. Western suggest the drafting team clarify requirement 2.1, which directs the Transmission Owner to select a Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment; however, these NERC functional entity designations do not appear in the applicability section of the standard. We also suggest reconsidering the short 90-day period to ensure verification of the risk assessment. This may not allow every Transmission Owner to establish a contract with an unaffiliated verifying entity during the standard's implementation time period.

Yes
: We recommend striking the qualifier regarding the ASIS “Certified Protection Professional or Physical Security Professional” from the standard R6-6.1.1 as it is inclusive of only one organization and may not provide the best support for each entity . Simply having these certifications does not guarantee the necessary knowledge to perform this unique work. We believe the language does not support the intent of the FERC Order as identified in paragraph 11. We request the Drafting Team clarify the scope of the third party review process identified in R6 and tie the requirement to a specific and established method as consistent in accepted practices, such as the ISO processes. We recommend the third party review process be clarified as a review of the primary entity’s adherence to their established processes in evaluating threats and vulnerably, as well as their security plan(s). We believe the current audits conducted by the regional entities satisfy the third party review process as identified in the FERC Order, paragraph 11. We do not believe R6-6.4 adequately protects the sensitive information contained in the risk, threat, and vulnerability assessments, or the security plan(s). These reports may contain sensitive and/or classified information, or otherwise information that if released would jeopardize the BES, with little to no penalty for an offending party.
Yes
In the VSL for requirement R5, in all four severity levels, states that the security plans need to be developed for the facilities “identified in requirement R1”. However Requirement R5 only requires the plans to be developed for facilities ‘identified in Requirement R1 and verified according to Requirement R2,”. The VSL should be modified to include the statement ‘and verified according to Requirement R2. The first row in the Table, in the RSAW, describing the evidence required in requirement R1, it states that any risk assessments conducted prior to the effective date of this standard are not relevant. The Implementation Plan states that “The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard.” There appears to be a conflict between these two statements, unless the intent is that the initial risk assessment needs to be completed on the effective date. Also, normally, unless the implementation plan provides a different time line, you need to be compliant by the effective date. In the RSAW for requirement R6 the fourth row in the Evidence Requested table, it asks for evidence that includes the “reasons or compensating mitigating measures for not implementing the recommendations for the reviewing party.” Requirement R6.3 of the standard only requires the Transmission Owner or Transmission Operator to “Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.” These two statements should be clarified in order to ensure consistent enforcement.
Individual
Lynnae Wilson
Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.
Yes

Vectren supports the use of the CIP-002-5.1 medium impact criteria. This approach focuses on the facilities that could have a true adverse impact to the Bulk Electric System and provides consistency with approved standards.

No

Specifically, Vectren recommends that R2 be removed from the draft standard, for the reasons set out in this Comment. And that an approach similar to that used for evaluation of designations under CIP 002 Version 3 be adopted for review of the required risk assessment. Vectren urges FERC and NERC to designate registered Planning Coordinators, Transmission Planners, or Reliability Coordinators as the approved verifiers for entity risk assessments AND to establish clear criteria for verifiers, so that NERC auditors can apply a uniform set of criteria to their after the fact assessment of verifier qualifications. As written, these provisions lack the specificity necessary to provide clear direction to entities, increasing the risk of later non-compliance. Such a risk is ironic and unacceptable in requirements that purport to provide a review of risk assessments. Under these draft requirements entities have no assurance that any third party verifier they might select will be considered "qualified" by FERC, NERC or NERC auditors who might review the results later – leaving entities at grave risk of compliance violations if FERC, NERC or any other regulatory body later disagrees with the entity's selection of a third party verifier. Vectren strongly urges NERC and FERC to establish criteria for those who might seek to be designated third party verifiers, rather than leave assessment of qualifications to an after the fact review during a NERC audit or spot check. A lack of certainty leads here by necessity to a lack of confidence in the result, which Vectren surmises was not the intent of FERC or the drafters.

No

Specifically, Vectren recommends that R6 be removed from the draft standard, for the reasons set out in this Comment. And that an approach similar to that used for evaluation of designations under CIP 002 Version 3 be adopted for review of the required risk assessment. Vectren urges FERC and NERC to establish clear criteria for verifiers, so that NERC auditors can apply a uniform set of criteria to their after the fact assessment of verifier qualifications. As written, these provisions lack the specificity necessary to provide clear direction to entities, increasing the risk of later non-compliance. Such a risk is ironic and unacceptable in requirements that purport to provide a review of risk assessments. Under these draft requirements entities have no assurance that any third party verifier they might select will be considered "qualified" by FERC, NERC or NERC auditors who might review the results later – leaving entities at grave risk of compliance violations if FERC, NERC or any other regulatory body later disagrees with the entity's selection of a third party verifier. Vectren strongly urges NERC and FERC to establish criteria for those who might seek to be designated third party verifiers, rather than leave assessment of qualifications to an after the fact review during a NERC audit or spot check. A lack of certainty leads here by necessity to a lack of confidence in the result, which Vectren surmises was not the intent of FERC or the drafters.

Yes

Vectren recognizes that this drafting effort required significant contraction of drafting and approval processes, and Vectren appreciates the work of the drafting team. Vectren is

supportive of the goals of the standard, supports R1, R3, R4 and R5. Vectren urges the drafting team, NERC and FERC to remove entirely or add detail to the requirements R2 and R6, and to add specific audit criteria in the RSAWs, so that entities can have some confidence that their risk assessments performed in good faith, will be considered compliant with this Standard.
Individual
Venona Greaff
Occidental Chemical Corporation
Agree
Ingleside Cogeneration, LP
Group
Texas RE
Derrick Davis
Yes
The applicability should include the TP, PC, RC, and the unaffiliated entity as they are noted in this standard.
No
1. For R1, the Transmission Owner is not the appropriate entity to conduct the type of transmission analysis that the requirement describes. It seems like a more logical process would be for the Transmission Planner to conduct an analysis of all substations meeting the applicability in 4.1.1.1 thru 4.1.1.4, and then, if the removal of a substation results in Cascading, instability, or uncontrolled separation, the TP will then notify the TO & TOP to conduct the security threat evaluation per R4 at only those substations identified by the TP. 2. R1 - A “risk assessment” pertains to the physical security of Transmission Facilities while a “risk-based assessment” pertains to identification of Critical Assets and Critical Cyber Assets. The two phrases are too similar in meaning to each other, but possess differing meanings and intents. 3. For R2, if the approach described in #1 is accepted, it may also satisfy R2 in those cases where the TP is independent from the TO. The independent verification would also be the responsibility of the TP, utilizing another TP, the PC, the RC, or an unaffiliated entity as described in the current language. 4. For R3, if the approach described in #1 is accepted, the initial notification to the TOP would originate from the TP.
No
1. The sequence and timelines for R5 and R6 need to be reviewed. R5 states the TO “shall develop and implement” the security plan within 120 calendar days of completion of R2. R6 states the 3rd party evaluation can occur concurrently with or after completion of R5. It seems like the 3rd party evaluation should be completed before the plan is implemented in R5, otherwise the entity may be planning for or implementing measures that may not be appropriate for the risk level. 2. R6 also 3. Also, who evaluates the implementation phase of security plan and whether or not it was implemented correctly or if the plan was effective? There should be an entity assigned for this task. There should be an exercise (like GridEx) to

test the plan. 4. The third party reviewer could be the same entity in R2 and R6. This could be a question of independence. It also does not indicate the third party actually verifies the implementation of the security plan(s) in R6. This does not permit the Compliance Enforcement Agency to place reliance upon the work of the third party.
Yes
Several places in the standard refer to notifying the Transmission Operator for stations that meet the higher risk profiles. However, the language is not clear as to what is expected from the Transmission Operators when a physical security incident occurs at one of those substations during real-time operations. Finally, this entire process can exceed four hundred days, which is excessive.
Group
Florida Municipal Power Agency
Frank Gaffney
Yes
No
FMPA commends the efforts of the SDT to lay out an excellent process for risk assessment in accordance with the FERC Order in such a short time frame. We only have few comments. WHAT DOES “CONTROL CENTER” MEAN Is there a signifance for not using the capitalized term of Control Center throughout the standard? It seems to FMPA that the defined term “Control Center” ought to be used. If the intent is that “control center” and “Control Center” mean two different things, then, what does “control center” mean? If the intent is to include large TOs that may be part of a large TOP, such as a large utility in an RTO, that do not have Control Centers; then, FMPA recommends using a different term such as “the location of the SCADA system that has remote control of breakers associated with the identified substation/station” or similar might avoid confusion. WHAT DOES “UNAFFILIATED” MEAN The term “unaffiliated” may be a source of ambiguity and conflict without further definition. For instance, dictionary.com defines affiliated as: “being in close formal or informal association; related” So, this would imply that peer members of the Transmission Forum are affiliated, which we do not believe is the intent of the SDT. FMAP believes the SDT’s intent is as Black’s Law Dictionary defines affiliate: “1. A corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or sibling corporation. 2. One who controls, is controlled by, or is under common control with an issuer of a security.”; which would mean that peers within the Transmission Forum are unaffiliated, but subsidiaries of a company are affiliated, or members of a Joint Action Agency are affiliated. It also aligns with FERC’s definitions for Affiliate in their market based rates regulations 18 C.F.R. 35.36(a)(9) and in the Pro Forma OATT. FMPA suggests using a footnote to clarify use of the term unaffiliated, such as “Use of the term unaffiliated is in relation to Black’s Law Disctionary defition for affiliated: ‘1. A corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or sibling corporation. 2. One who controls, is controlled by, or is under common control with an issuer of a security.’”

PROPER QUALIFICATIONS FOR RISK ASSESSMENT VERIFICATION FMPA appreciates the challenges of defining qualification for independent verifiers while offering registered entities a broad choice for selection. We interpret that requirements R2 and R6 grant the applicable entity sole authority to choose the 3rd party verifier as long as they meet the qualifications contained within those requirements. Is FMPA correct in that interpretation? CHANGE MANAGEMENT OF THE RISK ASSESSMENT The standard is somewhat ambiguous on what happens if the responsible entity chooses to revise it's risk assessment of R1 sooner than the required 30 or 60 calendar months. Does every minor revision to the risk assessment require another 3rd party review? Or would only major system changes (e.g., due to adding a major new investment in the power system like a new 500 kV line) require review? Or regardless of system changes, would the review occur once every 30/60 months? FMPA suggests clarification to R2 to say that minor revisions to the risk assessment due to minor power system changes in between the 30/60 month periods do not need a separate 3rd party verification.

No

Again, FMPA commends the SDT for a job well done. Just a few minor comments. See response to question 1 concerning use of the terms "control center" and "unaffiliated". CHANGE MANAGEMENT OF THE VULNERABILITY ASSESSMENT AND SECURITY PLAN Similar to our comments regarding change management of the risk assessment, it is ambiguous as to how we would implement change management related to the vulnerability assessment and security plans. R4 has no periodicity requirement, but, instead seems to require responsible entities to continuously reevaluate their vulnerability assessments in response to events listed in bullets 4.1, 4.2 and 4.3. If the entity changes their vulnerability assessment to include new threats, does every revision require a new 3rd party review? How do we come to agreement what constitutes a valid "trigger" for a new vulnerability assessment? It seems to imply that each of us would need to have an independent 3rd party on retainer to review our assessment of every intelligence or threat warning from governmental or regulatory agencies, or new attacks that each entity becomes aware of. Is that the intent? If so, what consititues a "warning", e.g., is it an "official" warning through some sort of official channel, such as a NERC Alert? If so, what happens if an entity decided to act on an "unofficial warning", such as a media release, to revise their vulnerability assessment – would that also need a 3rd party review? FMPA suggest clarifying 4.3 with "Official intelligence or threat warnings …". R5 seems overly ambitious. 120 days, or 4 months, is not a lot of time to perform a vulnerability assessment and develop and implement a security plan, especially in response to a newly identified threat vector/warning, and especially considering that a revised security plan may include capital investments in measures like new enclosures, vehice barriers, or the like. Is the intent that a security plan could be a phased approach, e.g., implement an interim security plan within 120 days while future improvements to that plan take longer? If so, then the language of the requirement ought to reflect that intent. FMPA suggest a modification to R5 such as: "… shall develop and implement the first phase of a documented physical security plan(s) … within 120 calendar days …" In addition, R5 does not seem to fit temporally with R2 and R4 well. R2 requires periodic risk assessments every 30/60 months. R4 seems to require changes to vulnerability assessments in response to newly known threat vectors. The timing

of R5 refers to R2: "… within 120 calendar days following the completionof R2" with no reference to a revision to the vulnerability assessment. This causes FMPA to belevie that revisions to the security plan as a result of a new threat vector and a revised vulnerability assessment of R4 would not need to be required until 120 days following the next periodic risk assessment of R2. Is that the intent? If that is the intent, if an entity chooses to revise the security plan earlier, would that then need an 3rd party verification at that time, or at the time of the periodic risk assessment?
Yes
FMPA has concerns for the RSAW and the lack of direction to auditors from the RSAW concerning the scope of their review. The auditor should not have a subjective decision regarding the sufficiency of the risk assessment, vulnerability assessment or security plan of the TO/TOP. The unaffiliated 3rd party is the source of qualified expert subjective opinion on the sufficiency of the risk assessment, vulnerability assessment and security plan. As such, the RSAW ought to clearly define the scope of the auditor's review of the risk assessment, vulnerability assessment and security plan. FMPA suggests rewording the "Compliance Assessment Approach"portions of the RSAW that call for these reviews to read something like the following (specific to R1): Review the entity's risk assessment to answer the following: a. Were all of the entity's assets, existing and planned to be in service within 24 months of the date of the documented risk assessment, and applicable to the standard (Applicability Section 4.1.1), included in the assessment? b. Was a transmission analysis or transmission analyses identified and documented to evaluate whether any applicable Transmission station(s) and Transmission substation(s), if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection? The auditor is not to evaluate the sufficiency of such analyses; but rather whether such analysis was documented. c. Was the assessment conducted within the timeframes identified in bullet 1.1? d. Was the primary control center(s) identified in accordance with bullet 1.2?
Individual
Thomas Foltz
American Electric Power
Yes
Yes
Yes
Yes
It is AEP's understanding that regarding R5, the phrase "develop and implement a documented physical security plan…within 120 calendar days" means that, within 120 days, the physical security plan must be completed and that the entity is working toward implementing the plan and does not mean that the plan must be fully implemented within

120 days. AEP urges the clarification of that expectation within R5 so that the requirement is unambiguous. Regarding R6.4, please clarify whether the procedures for protecting sensitive or confidential information would include suitable terms and conditions within a third party contract.
Group
Duke Energy
Michael Lowman
Yes
Yes
Yes
Yes
(1) Duke Energy suggests that language should be incorporated either in the proposed standard or RSAW to allow for the flexibility in modifying the timeline specified in R5.3. We believe there are unforeseen circumstances that could occur which would result in the proposed timeline shifting from the intended completion date. Examples include, but are not limited to: a. Unplanned outage of transmission or generation facilities that results in canceling scheduled work. b. BES reliability concerns should the facility be out of service for a short or extended period of time. c. Third party vendor's availability in implementing recommendations made by an entity or unaffiliated third party verifier. For these reasons, we believe a provision is needed to allow for this type of flexibility in modifying the timeline specified in R5.3.
Individual
Anthony Jablonski
ReliabilityFirst
Yes
ReliabilityFirst supplies the following comments for consideration: 1. ReliabilityFirst believes there may be a perceived disconnect between the Applicability Section and Requirements 5 and 6. Requirements 5 and 6 introduce new requirements surrounding the Transmission Owners "primary control center" though the "primary control center" is not listed within the Applicability section as an asset the Transmission Owner owns that is included in the standard. Consideration may be given to adding "primary control center" under section 4.1.1. [Note: Since "Control Center" is a NERC defined term, this term should be capitalized throughout the standard.] 2. Applicability section 4.1.1.4 - ReliabilityFirst believes the term "as essential" is ambiguous and may cause unintended compliance monitoring implications. ReliabilityFirst recommends the following for consideration: "Transmission Facilities identified

[in] Nuclear Plant Interface Requirements [which provide offsite power].” ReliabilityFirst believes the recommended language addresses the intent of the SDT.
Yes
ReliabilityFirst supplies the following comments for consideration: 1.Requirement R1 - ReliabilityFirst believes there may be a gap in the timing of performing the risk assessment for new Transmission stations and Transmission substations which are planned outside the 24 month window as required in Requirement R1. For example, as written, if a new Transmission stations or Transmission substation is planned for month 25, it would not be included within the initial risk assessment. Thus, there is a potential for this new Transmission stations or Transmission substation to not be assessed for 30 calendar months (for a Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable …) or 60 calendar months (for a Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability…” With the potential gap in assessing new Transmission stations and Transmission substations being so long, ReliabilityFirst believes reliability may be compromised. For these reasons, ReliabilityFirst recommends the following for consideration: “Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 30 months)…” and including a new bullet under Part 1.1 which states “At least prior to the implementation of all new Transmission stations and Transmission substations (if not assessed within the initial or subsequent risk assessment)” 2. Requirement R3 part 3.1 - From a standards writing perspective, if there is only one sub-part, ReliabilityFirst recommends including it within the Parent requirement R3. Typically sub-parts are only included if there are more than one.
Yes
ReliabilityFirst supplies the following comments for consideration: 1. Requirement R5 - ReliabilityFirst requests clarification on why the term “primary control center” is used throughout the document instead of just “control center”, as it seems both a primary and secondary control center would be of equal importance (and have similar vulnerabilities) to reliability.
Individual
Larry Watt
Lakeland Electric
Agree
Florida Municipal Power Agency (FMPA)
Individual
Donald E Nelson
MA Dept. of Public Utilities
Agree

Agree with the comments made by NPCC.
Individual
Andrew Gallo
City of Austin dba Austin Energy
Agree
American Public Power Association (APPA). In addition, Austin Energy states the following: The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this Standard may be subject to disclosure under state open records laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard designating the produced, gathered, used and maintained records related to compliance with this Standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure.
Individual
Kevin Lyons
Central Iowa Power Cooperative
Agree
ACES
Group
Peak Reliability
Jared Shakespeare
Yes
Yes
Peak believes the RC entity should perform the R2 verification because the RC has the wide-area view in the Western Interconnection. The alternative would be to have individual transmission entities perform varied verifications, which could result in inconsistent methodologies and results.
No
Individual
Robert Trowbridge
Consumers Energy Company

Yes
With Michigan situated as a peninsula, Michigan infrastructure may be at a lesser risk, based on the limited number of interconnect avenues into and out of our system. Meaning the highest level of criticality likely would be identified as those key interconnect points, and not the entirety of our system. From our experience with the blackout of August 2003, BES implications were centered in southeast Michigan and although affected, we were able to successfully minimize/sustain our base load generation requirements. Any substation targeted in Michigan may not have a cascading effect on the BES.
No
We agree to the approach, however, our concern is around protection of information shared between the entity and the third party. There should be a requirement within the standard that requires the third parties to protect the information and not leave it up to the entities.
No
We agree to the approach, however, our concern is around protection of information shared between the entity and the third party. There should be a requirement within the standard that requires the third parties to protect the information and not leave it up to the entities.
Yes
Develop a requirement to protect information shared between entities and third party organizations. Requirement number 6 should be revised to state “…third party reviewer that is either…” 6.1.1 or 6.1.2 or 6.1.3 or 6.1.4. R6 seems vague and should be revised
Individual
Chantal Mazza
Hydro Québec TransÉnergie
Yes
No
Hydro-Quebec TransEnergie (HQT) agrees with this approach but requests that the SDT remove the term "unaffiliated" from Requirements R2 and R6.1 HQT notes that the term "unaffiliated" is not used in FERC Order 146. Paragraph 11 of the Order states "In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator." Moreover, it appears that it is not FERC's intent to introduce this restriction regarding the choice of a third party. HQT therefore believes that the use of the term “unaffiliated” goes above and beyond what was stipulated in the FERC Order. Furthermore, the term "unaffiliated" is not required because the NERC Reliability Functional model already ensures the independence between the TO/TOP and the verifying entities (RC, PC and TP) that the SDT is seeking in the draft standard. The Reliability Model uses the term "functional entity" to apply to a class of entities without making reference to specific organizations that register as functional entities. For some Canadian jurisdictions, the use of the term "unaffiliated" renders the standard more stringent due to the fact that certain Canadian entities such as Hydro-Québec TransÉnergie are simultaneously

registered as TO, TOP, PC and RC. For integrated modeled entities, the restriction of available options that would otherwise be available (such as selecting a PC, TP or RC for the risk assessment verification under R2), makes it difficult to identify an entity with the required expertise capable of performing the reviews stipulated in the standard. HQT believes that the risk assessment of a TO should only be verified by the RC or the PC that has supervision (real-time or planning) over the said TO's assets because only the RC or the PC can ensure a comprehensive approach to critical facility identification that considers the reliability of an entire area. For these reasons, HQT believes that the expression "third party" alone is sufficient and consistent with the expressed concerns in the FERC Order.
No
The same comments regarding the term "unaffiliated" in Question 2 above apply to R6. HQT believes that the SDT should remain general about the security measures that should be put in place. Requirement R5.1 states "Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4." We believe that rather than the standard dictate what type of measures are to be implemented, it should be rephrased to remain general and use similar language that is used in paragraph 9 of the FERC order. Suggest rewording the requirement to "Resiliency or security measures designed to protect against potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4.".
Yes
The following are suggestions to facilitate reading of the standard, as well as its future translation: All requirements: Replace the expression "Transmission stations and Transmission substations" with "Transmission facilities". Otherwise, please explain why such a distinction is necessary. R1: Remove "transmission analysis" from the sentence "The initial and subsequent risk assessments shall consist of transmission analysis or transmission analyses designed to …" We believe this repetition is unnecessary. R2.2: The first part applies to an entity that is not subject to the standard and should be removed from the standard. R2.3: Replace the word "identification" with "assessment". Remove the word "either" Rephrase R4, R5 and R6 (add "a"): " ...a transmission substation, or a primary control center". R4 and R5: Remove the part "…that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation". It only complicates the reading of the requirement (the TOP is not notified by the TO unless it has operational control over an asset identified in R1). If the first parts of R4, R5 and R6 are intended to identify the functional entities to which the requirement applies, we suggest "… and each Transmission Operator notified by a Transmission Owner under requirement R3, shall …" for the TOP portion (line 3 to 6 of R4, R5 and R6). We believe that it would greatly improve clarity and readability of the requirements. R6.1: rephrase to "from one of the following". Furthermore, the numbers 6.1.1 to 6.1.4 should be replaced with bullets as is the case in R1.1, R2.1, and R2.2. Rephrase R6.1 and R6.1.1 to reflect the language used in the rationale. We believe limiting the reviewer to someone with a CPP or PSP certification goes beyond what the FERC order requesting. Suggest rephrasing to "with appropriate expertise of the evaluation performed". Guidelines and Technical Basis on requirement R1: HQT agrees with the fact that the TO has discretion to

choose the specific method to establish the risk assessment, and that it is relevant that the Guidelines proposes examples. However, the proposed example of "removing all lines to a single Transmission station" seems to present a very stringent impact considering a physical attack on a facility. We ask the SDT to propose others less stringent examples that would be more in line with realistic physical attack, such as loss of a large section according to physical organisation of the facility, or loss of all main transformers, etc.
Group
Dominion
Connie Lowe
Yes
No
Measure M1 - R1.2 -- Measure M1 does not address sub-requirement R1.2 which requires the Transmission Owner to identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment. Dominion recommends the SDT determine whether M1 should include the control center. R2.3 - Relative to R2.3, Dominion does not agree that the TO should have to document the technical basis for retaining assets that have been suggested for removal by the third party. R3 - Dominion suggests R3 be revised to strike the words ‘and verified according to Requirement R2’, and changing R2 to R1.2 in the next two instances where R2 is mentioned. This is due to the reason there is nothing included in R2 that requires verifing primary control centers.
No
R5 and R6 are written for the initial risk assessment and don’t necessarily apply for subsequent risk assessments. Is the expectation that 3rd party reviews be performed for R4 and R5 every time R1/R2 is run, particularly if there are no changes? Dominion recommends that the SDT modify this in the event the R1 list changes (ie: add stations) to require a subsequent R4/R5 reassessment. If stations drop off, or no change to R1 list for subsequent assessments, then subsequent R4/R5 reassessment is not required. R6 - Through continuous improvement processes and lessons learned, there will be expected changes to the security plan(s). What changes are allowed to the security plan(s) without triggering a 3rd party review?
No
Individual
Michiko Sell
Public Utility District No. 2 of Grant County, WA
Public Utility District No. 2 of Grant County, WA
Yes

Language contained in R1 does not align the performance of risk assessments of Transmission stations and Transmission substations with the actual commissioning or energization of such facilities. To ensure that risk assessments and subsequent risk assessments address existing and planned Transmission stations and Transmission substations to be in service within a risk assessment window the following edits are recommended to R1: R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 30 months) .. 1.1. Subsequent risk assessments shall be performed at least once every 30 calendar months. (this would apply to all applicable TOs) GCPD also supports comments made by APPA regarding the insertion of the language addressing Confidentiality and treatment of Critical Facilities Information. GCPD's suggested language is as follows: Risk assessments and evaluations of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure.
Yes
R2 references primary control center(s). Since Control Center is a NERC defined term GCPD suggests that all references to the Control Center be capitalized within the Standard and that "primary" be defined within the standard to not include "back-up" Control Center(s).
Yes
GCPD appreciates the flexibility built into the Standard language that allows tailored evaluations of potential threats and vulnerabilities to its own facilities. GCPD supports APPA's suggested edits to the Standard to enhance clarity of requirements under R4, R4.1 & R4.2. In addition, APPA's suggested removal of "and implement" under R5 clarifies that the intent of R5 is to develop the physical security plan, not fully implement the plan within 120 calendar days. This would better align the Standard language contained in R5.3.
Yes
GCPD feels that the implementation schedule is somewhat arbitrary and demonstating compliance with the implementation schedule conflicts with language contained in the proposed RSAW. GCPD supports RSAW edits as proposed by APPA to address these discrepancies. GCPD proposes the following edits to Requirement language addressing implementation timing to allow for enforceable and auditable time lines not dependent upon the unique completion date of the initial risk assessments conducted by the RE. 2.2. ...The Transmission Owner shall ensure the verification of the initial risk assessment performed under Requirement R1 is completed within 90 calendar days following the effective date of this Standard. Subsequent risk assessments shall have verifications completed within 90 calendars days of completion of the risk assessment. R5. ...and primary Control Center(s) within 210 calendar days following the effective date of this Standard. Changes to recognized applicable facilities under this Standard as identified under Requirement R1 and verified according to Requirement R2, shall require review of the physical security plan(s) within 90

calendar days of completion of associated risk assessments. ... General commentary: in October 2012 the Cost Effective Analysis Process (CEAP) was approved for a “pilot”. The NERC CEAP was intended to integrate cost consideration and effectiveness into the development of new and revised standards. The first phase of the CEAP was to be implemented during the SAR stage to determine cost impact and identify “order of magnitude” or potentially egregious costs, to determine if a proposed standard will meet or exceed an adequate level of reliability, and what potential risks are being mitigated. The second phase was to be conducted later in the standard development process and afford the industry the opportunity to offer more cost efficient solutions that may be equally effective to achieving the reliability intent of the draft standard. This report would be posted at the time the standard is balloted. The report was intended to present the data collected in a manner which will provide the industry with representative cost implementation and effectiveness information to allow a more informed choice during balloting. Based upon the urgent nature of this Standard, phase two would need to be applied. The CIP-014 Standard requires costs to be incurred to comply with Requirement R5. In addition, there may be substantial costs incurred to implement the Physicial Security Plan(s). The CIP-014 Standard is an ideal standard upon which to exercise the CEAP. The information resulting from the CEAP would be beneficial not only to government officials, but also the industry as a whole.
Individual
Brett Holland
Kansas City Power & Light
No
There is a use of the term "critical" being used in several NERC Standards, which can cause unintended confusion. Since the applicability of this draft Standard is derived from the approved CIP-002-5.1, can this proposed Standard be added as a revision to CIP-002-5.1?
No
In R1, we have concerns about the ambiguity associated with the term "assessments". Can you provide examples of the types of assessments that would be acceptable to meet R1 and that would be CIP audit worthy in the future. We have the same concern in R2 with the term "third-party". Will there be a list of pre-approved third party contractors or will the RE's review and approve a third-party at the request of the registered entity prior to their use in the verification process as described in R2?
No
Same comments about "third-party" from Question 2.
No
Group
APPA
Joe Tarantino
American Public Power Association (APPA)

SMUD supports the APPA comments and is specifically concerned that records and information developed and maintained under each of the requirements for this standard are afforded the necessary protection through an introduced section, #7 Critical Facilities Information. We respectfully ask the Standard Drafting Team to ensure that AUTHORIZED ACCESS to information pertains to ANY RECORD AND INFORMATION associated with the Physical Security Standard.
Individual
Nick Braden
Modesto Irrigation District
Modesto Irrigation District supports the comments submitted by American Public Power Association/Large Public Power Council
No
MID agrees that maintaining selection criteria consistent with CIP-002-5 is a prudent approach. However, if a facility is worthy of protection against a cyber attack, why is that same facility not worthy of consideration and evaluation for a potential physical attack? Inclusion of 'widespread instability, uncontrolled separation, or Cascading within an Interconnection' as an additional criteria is also prudent. These criteria focus on the immediate impact of the physical attack. What is missing is the longer term impact - if serious physical damage is the result, can the damaged system perform adequately during subsequent peak loading periods? MID understands that these changes would extent the scope of the standards coverage beyond what was included in the FERC order. MID would like to respectfully suggest that the FERC order is a step in the right direction but did not fully consider all of the potential physical attacks that could cause 'widespread instability, uncontrolled separation, or Cascading within an Interconnection' or impair long term reliability of the system. MID feels that in responding to the FERC order, it would be acceptable to ‘do the right thing’ and step up to the challenge and evaluate all facilities identified in CIP-002-5 as high or medium impact the system against possible physical attacks.
Yes
Yes
No
Individual
Dixie Wells
Lower Colorado River Authority
Agree

Lower Colorado River Authority
Individual
Alan Johnson
NRG Energy, Inc.
Yes
This standard should not address generation interconnection facilities because the BES is designed to withstand the loss of generation facilities through the use of regional reserves.
Yes
NRG agrees the approach described in Requirements 1 through 3 address the directives specified in FERC Docket No. RD14-6-000. However, NRG does have concerns with the standard as currently composed and offers the following points it believes will improve the standard if implemented: • Primary control centers are referenced in the “purpose” of the standard, but are not included in the “applicability” section. For clarity, NRG suggests the addition of section 4.1.1.5, stating “Control Centers and backup Control Centers associated with the Transmission stations and Transmission substations identified in requirements 4.1.1.1 through 4.1.1.4.” • R1 directs that the Transmission Owner to perform an initial risk assessment with subsequent studies and include an unaffiliated third party to verify the risk assessment performed. NRG is concerned the standard does not indicate how information shared under this Requirement will be protected and held in confidence. NRG believes the information subject to this standard should be treated as Critical Energy Infrastructure Information (CEII). • R1 is vague in providing guidance as to the criteria to be used in developing the risk assessment. NRG appreciates this is intentional to allow flexibility in developing the assessment. However, this results in the potential for a determination of non-compliance during the audit process. NRG suggests reliance on the CIP-002 standard used for defining Critical Assets, which is based on solid metrics. • R2 seems to allow the same third party to perform both the initial risk assessment and the review of the initial risk assessment, potentially negating the need for a separate review. • R2.2 calls for review of the results of the initial risk assessment by an unaffiliated third party. The standard provides no guidance regarding the criteria (assumptions, contingencies, etc.) to be used for this review, which could provide results differing from the initial assessment. More objective measures should be incorporated.
Yes
NRG agrees the approach described in Requirements 4 through 6 addresses the directives specified in FERC Docket No. RD14-6-000. However, NRG does have concerns with the standard as currently composed and offers the following points it believes will improve the standard if implemented: • R5.1 provides no guidelines or examples of how to combat certain threats, or even what threat thresholds require accounting for. NRG appreciates the flexibility built into the requirement. However, NRG is concerned this flexibility could result in “interpretation” issues during future audits of compliance with the standard. • The ability to meet the time horizon commitment for providing the third party assessment of the vulnerabilities and security plan are contingent upon the availability of certified parties that

can adequately perform these assessments. NRG is concerned there may be a lack of qualified resources available to the industry to complete the necessary reviews within the required time frame. • Because the reliability of the bulk power system depends on numerous susbstations all across the nation, it would be more effective to increase the monitoring of the grid to ensure timely, effective re-routing of power when a disruption occurs. • Minimum physical standards should be established within the security plan that include industrial standard chain link fencing with barbed wire topguards; gates secured with chains and locks (not the alloy metal collar around a post); signage that clearly states No Trespassing every 100 ft., or on each perimeter side at small footprints; cameras that are monitored by the appropriate transmission control center, security control center or a contract central monitoring service and capable night viewing to be able to identify intruders.
No
Individual
Curtis Klashinsky
FortisBC
Yes
No
The audit provides an independent review of an entity's application of the standard and therefore, an additional third party review should not be required as described in R2. It is agreed that if a null set is identifed, the rest of the standard does not apply.
No
The third party review of the security plan does not guarantee an objective evaluation as they would be funded by the requesting entity. The standard could state that the entity should follow an industry standard technical guideline. The audit provides an independent review of an entity's application of the industry standard technical guideline and therefore, an additional third party review should not be required as described in R6.
No
Group
New Brunswick Power Corporation
Alan MacNaughton
No
New Brusnwick Power (NB Power) agrees with the “applicability section” but not with portions of the preamble above, in question 1, which expands beyond applicability and states that “Furthermore, the standard drafting team expects many who are “applicable” to the standard will not identify facilities through their Requirement R1 risk assessment and

Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection." To our knowledge there is no evidence to support the standards drafting teams statement that they expect that many of the applicable entities will not identify facilities through R1 and R2. FERC's statement that "we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System" is not sufficient evidence. NB Power is concerned that the cost impact of this standard may be underestimated as a result of this view that the number of critical facilities will be small. Please see comments below with respect to R1 and R2.

No

In general, a TO may not have the capability to conduct a risk assessment to determine if an identified facility that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Such an assessment requires a wide area view of the Interconnection. It is proposed that the risk assessment be conducted by a PC, or RC for the area in which the facility is located. Doing so would satisfy the third party verification requirement as the TO would not be conducting the analysis. It is the opinion of NB Power that the technical details concerning the transmission analysis, in the proposed standard, are overly vague. This could lead to an inconsistent application of the analysis between entities as well as create obstacles with consensus concerning the proposed 3rd party verification. NB Power suggests a clear analysis methodology be drafted to establish a common basis for study criteria with the ability for each entity to apply additional specific requirements for their respective area. For corporate bodies, such as a vertically integrated utilities, that are registered as the RC, TOP, PC, TP and TO for a particular area, it is the opinion of NB Power that the requirement for unaffiliated 3rd party verification is overly stringent and of little value. The verifying party is limited to entities that have transmission planning or analyses experience, or, are registered as a PC, TP, or, RC from an adjacent area. NB Power is of the view that there are no unaffiliated entities with sufficient knowledge of the local transmission system to provide a meaningful verification within a 90 day period. As a government owned utility, NB Power is required to follow procurement processes which will make it difficult to meet the 90 day period for the third party verification. NB Power is also concerned that it could be non-compliant with the requirement if the third party fails to meet its obligation. While NB Power can mitigate the financial risk of that event it would still result in a recorded non-compliance. It is the opinion of NB Power that the proposed standard does not sufficiently address a disagreement resolution process between the TO and the unaffiliated verifying 3rd party in requirement R2.3. NB Power believes that documenting the technical basis for not following the recommendations of the unaffiliated verifying 3rd party without guidance on what constitutes valid technical reasons presents a compliance and enforcement gap where both the entity and an auditor may not be able to come to consensus. NB Power suggests the SDT develop guidance concerning compliance and enforcement of this requirement indicating acceptable technical reasoning for not following the 3rd parties recommendations.

No

NB Power is concerned with the 120 day timeline to implement a physical security plan that would meet the third party verification requirements. Having limited knowledge of physical security issues NB Power will likely rely on the third party verifier to work with NB Power in developing a security plan. NB Power is not aware of any analysis that was done to ensure that there is enough capacity within the “physical security industry” to support the work load increase resulting from the approval of this standard and as such is concerned that 120 days may be insufficient. NB Power is concerned that it could be non-compliant with R6.2 if the third party fails to meet its obligation. While NB Power can mitigate the financial risk of that event it would still result in a recorded non-compliance. It is the opinion of NB Power that the proposed standard does not sufficiently address a disagreement resolution process between the TO and the unaffiliated reviewing 3rd party in requirement. NB Power believes that documenting the technical basis for not following the recommendations of the unaffiliated reviewing 3rd party without guidance on what constitutes valid technical reasons presents a compliance and enforcement gap where both the entity and an auditor may not be able to come to a consensus. NB Power suggests the SDT develop guidance concerning compliance and enforcement of this requirement indicating acceptable technical reasoning for not following the 3rd party’s recommendations.
No
Individual
Mark Wilson
Independent Electricity System Operator
Yes
We agree with the inclusion of the Transmission Owners and Transmission Operators as they have the obligations to conduct an evaluation of the potential threats and vulnerabilities to a physical attack on each of their respective transmission stations/control centres.
No
While the proposed R1 to R3 collectively meet the FERC requirements for having an entity to identify the critical facilities and having the assessments of such identification verified, we believe it is more appropriate that the 3rd party verification be performed by NERC registered entities only (which could be the Reliability Coordinator, Planning Coordinator or Transmission Planner). An entity that has transmission planning or analysis experience may only have an outside equivalent representation of the BES and their ability to conduct an analysis with a “wide area” view of consequences may not be possible. As such, we suggest to revise Requirement 2.1 by eliminating the second bullet point : “An entity that has transmission planning or analysis experience”.
Yes
Individual

Kenn Backholm
Public Utility District No.1 of Snohomish County
Agree
Salt River Project ("SRP")
Individual
David Grubbs
Ciy of Garland
No
Applicability: The applicability section for Transmission Operators under section 4.1.2 should be explicitly limited to each TOP that operates a primary Control Center and receives a verified notification under Requirement R3. As written each TOP would be required to certify on each compliance contact that it has not been notified that it operates an applicable primary control center. The following edited text would accomplish that objective: 4.1.2 Transmission Operator that operates a primary Control Center and receives notice from a Transmission Owner under Requirement R3. Please state clearly the Transmission Operator of a primary control center is not responsible for conducting a risk assessment under R1 or arranging for third party verification of the risk assessment under R2.
No
R1 - The auditors should be limited to verifying that a study was completed using the assumptions agreed to by both the TO and the reviewer. The auditor should accept any study and assumptions jointly agreed to by the TO and the reviewer without requiring additional engineering justifications as to why one type of study was used instead of the auditor’s preferred methodology. To summarize and echo FERC Commissioner Norris in his clarifying statement, included with the FERC Order that is the basis of the CIP-014 Standard, that if the Planning Studies indicate a transmission solution that would cause the substation to no longer cause the cascading outage that the transmission project could be initiated in lieu of the security plan. The additional transmission solution would potentially add other operational benefits other than just “security” and therefore may be more practical than the security plan in R4 through R6. In the guidance document, statements should be made that a TO may make additional planning studies at any time prior to the 30 months and if the third party reviewer concurs the updated study no longer shows a cascading event, whether due to changing grid conditions or system improvements, the standard would no longer apply including the continued implementation of the security plan. The TO should also notify the owner of the primary control center the substation no longer causes a cascading event. R2 - Timelines to complete third party verification under R2.2 and third party review under R6.2 are both too short. Increase 90 days to 120 days or 180 days. a. Verifying entities may recommend that the Transmission Owner conduct additional planning studies to confirm asset identifications such as interactions between BES Elements in adjacent Transmission Owner footprints. A 90-day time limit may not provide sufficient time to conduct and verify a revised or supplemental BES assessment. b. For security reviews, conducting an accurate and meaningful review with sound recommendations applicable to a specific TPs facts and circumstances may require

additional time for assessment and discussions with the TO. A short review window is more likely to lead to misunderstandings, or disagreements with the TO which in turn could lead to discrepancies or improper application of the assessment requiring justification. This could cause the reviewer to avoid making recommendations that should be considered by the TO and improve the TO's assessment. c. As currently written, it appears if the TO disagrees with the reviewer's comments and writes a technical reason why he believes the original conclusion were correct, the recommendation(s) by the reviewer may be rejected and the TO's decision is final. Although I agree with this position it may be interpreted differently by the auditors. Please clarify which was the intent of the SDT. R3 - No comments
No
R4 - Sub requirement 4.1 should be modified to include specific language focusing the security study to those elements within the substation that can affect the reliability of the BES. The security plan should protect those elements of the substation as identified in the planning study in R1 that could cause the cascade or other unacceptable event identified in R1. Many substations identified in these studies are very large geographically and potentially very expensive to protect elements that may be located 30 to 50 feet above the ground. If these elements are determined to be critical they should be protected. If not, there is no justifiable reason to expend the resources to protect these devices. The security plans should concentrate on the protection of elements that could actually cause a cascading event, otherwise large expenditures may be made while adding no benefit or improvement to the reliability of the BES. R4.1 should read: 4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) including the identified elements within the station, substation or control center, that need to be protected that could initiate the cascading collapse identified by the planning study in R1; Under both R4 and R5 clarification should be provided to the auditors affirming that auditors do not need the work papers, or backup information used in preparing the security plan, it is preferable auditors be allowed to only view the plan on site and not be allowed to take a copy of the plan for their files due to the sensitive nature of the security plan. Having copies of the security plans of critical targets consolidated into the files of the auditing entity increases the security risk to the plan and identified assets do to a security beach or accidental release of the file. While having one security plan of a critical location is a security risk in and of itself, having a compilation of security plans by one entity becomes a national security risk. R5 - states in part that each TO and TOP "shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2." The "and implement" should be deleted. It should be made clear the facilities, additional employees or other measure identified in the plan are not required to be in place at the end of the 120 days. The requirement should be clearly stated that a timeline needs to be developed as part of the plan and the TO and TOP will implement the plan per the timeline identified in the plan. The implementation may require several years to get through budget cycles, procurement, installation and implementation. R6 - The standard should make clear the auditor is not to audit the security plan for its content or appropriateness, but to confirm a security plan has been developed and that particular

security plan has been reviewed by a qualified entity. It should also be clear that a TO could expand its actual security beyond that identified in the approved/reviewed plan without requiring an additional review of such modification. Example: The original, approved plan had card readers on the doors and cameras within the yard. During the 30 months until the next required review, the TO added motion detectors as additional security measures at the substation even though they were not required in the initial security plan. The installation of additional monitoring or security measures beyond those in the approved plan should not initiate the need for a new security plan or third party review.
Yes
Definitions: primary control center - although not capitalized and therefore not a defined term, it is used in this standard in requirements 1, 3, 4, 5, and 6. The same term "primary control center" (again not capitalized) is used with a completely different meaning in standards EOP-008 in requirements 1.3, 1.5, 1.6, 2, 3, 4 and 7.1. Similarly "primary control room" is used in EOP-005 requirement 5 and in EOP-006 requirement 6 and is defined as the control center from which a TOP normally operates as opposed to the backup center. In CIP-014, it is defined/implied to be the control center that actually controls the circuit breakers at two or more substations. • If the term “primary control center” is used there will be confusion over the different meanings within the NERC Reliability Standards. • A completely different term should be used such as “primary local control center” or “primary transmission operations center”. The SDT apparently meant a "facility that has direct Supervisory Control". The term should be defined completely in the standard and should become a defined term within the Glossary of Terms used in NERC Reliability Standards. Proposed defined term: Primary Transmission Operations Center - One or more Transmission Owner or Transmission Operator facilities hosting operations personnel having primary operational real-time control of the BES elements in one or more remotely located substations using SCADA, EMS or other electronic means.” Please clarify whether these security plans are also required at any backup control center. Many of these control centers are generally not manned on a 24 by basis. unaffiliated - should be either defined or a footnote needs to be added to the Standard to explain that unaffiliated - means the selected verifying or reviewing entity cannot be a corporate affiliate, as stated in the guidance document. • Would two entities that do not have a direct ownership stake in each other but both are parties to an ownership in a third organization be considered to be unaffiliated? Example: Two utilities each have an ownership of a joint power plant but no ownership of each other. • What if they both had no ownership of the third party but both had purchase contracts with a third party? An explanation needs to be in the standard and not in the separate guidance document.
Individual
Michael P Moltane
ITC
Yes
ITC agrees with utilizing, as a starting point, the CIP-002-5.1 “medium impact” rating to determine the facilities needing enhanced physical security. As ITC indicated in its comments

to FERC in Docket No. RD14-6, these new physical security Standards must be developed in a coordinated manner to avoid duplicative, overlapping, or contradictory requirements among the various existing Reliability Standards that cover a similar if not an identical set of assets. By ensuring “that entities could apply the same set of criteria to assist with identification of facilities under CIP Version 5 and proposed CIP-014-1,” the SDT has fully met our expectations with respect to the applicability of the standard.
No
ITC believes that limiting physical security requirements in CIP-014-1 to those substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection does not adequately raise the bar for critical infrastructure protection of valuable and strategic substation assets. Indeed, those substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection certainly warrant additional physical protection. However, so does any other substation asset deemed critical through the cybersecurity initiatives already in place through applicable companion Reliability Standards. If a substation is deemed critical through the CIP-002-5 screening process, it at a minimum, should warrant an “evaluation of potential threats and vulnerabilities of a physical attack to the facilities (CIP-014-1 R4). ITC supports using the brightline test criteria of CIP-002-5, as noted in our comments for Question 1, above, but also feels that all substation assets passing the brightline test criteria should move directly to R4 for an assessment of threats and vulnerabilities, eliminating the need for R1 and R2. This has the benefit of using industry-vetted, bright-line criteria that creates valuable consistency between physical and cybersecurity assessment practices. This does not undermine the Commission’s three-part requirement for addressing physical security, but rather allows the responsible entity to meet the Commission’s first requirement (identification of critical assets) by using the same critical asset identification criteria for physical and cybersecurity. ITC believes if a facility is critical enough to warrant cybersecurity protection, then it should also warrant physical security and that the requirements should not be so narrowly defined to ignore the importance of substations beyond those few whose individual loss causes cascading outages. This simplified approach avoids potential contradictory and duplicative requirements between existing CIP standards, and would allow this standard to focus exclusively on physical security aspects and not on asset identification
Yes
Yes
Transmission systems tend to have facilities for which inoperability, while not causing immediate system failure or separation, would nonetheless leave the system in a degraded state. This degraded state will require system operators to reconfigure the system in a way to mitigate the loss of such facilities, but at that point, a new group of facilities could effectively become “critical” as that term is currently defined in CIP-014-1. For example, the loss of a given substation may cause several transformers to be inoperable, and with the long lead time for replacement components, the transmission owner would realistically need to plan for

the substation to be out of service for an extended period of time. During this time in which the substation is out of service, a second tier of assets may exist for which inoperability would now cause separation or failure of the type that would afford them a “critical” designation as currently defined under CIP-014-1. This condition would persist for as long as the original equipment was out of service. If the SDT were to adopt ITC’s proposed modifications to R1 (see above), this would not be an issue, since all CIP-002-5 substations would already be covered by CIP-014-1. However, if the SDT chooses not to adopt ITC’s proposal, the SDT should consider whether entities should assess the transmission system in this new degraded condition to determine if new critical assets are created due to the degraded condition (i.e., a reapplication of the analysis performed in the current R1 to determine if the loss of a particular substation causes widespread cascading.) The Standard could also trigger additional transmission system studies to determine if the transmission system remains reliable during the extended period in which the critical assets remain out of service.
Group
PPL NERC Registered Affiliates
Brent Ingebrigtson
Yes
These comments are submitted on behalf of the following PPL NERC Registered Affiliates: Louisville Gas and Electric Company and Kentucky Utilities Company; PPL Electric Utilities Corporation, PPL EnergyPlus, LLC; PPL Generation, LLC; PPL Susquehanna, LLC; and PPL Montana, LLC. The PPL NERC Registered Affiliates are registered in six regions (MRO, NPCC, RFC, SERC, SPP, and WECC) for one or more of the following NERC functions: BA, DP, GO, GOP, IA, LSE, PA, PSE, RP, TO, TOP, TP, and TSP. The PPL NERC Registered Affiliates support the draft standard. As members of EEI, we also support the comments being submitted by EEI. In addition, we have provided specific comments that we believe would add clarity to the standards and simplify the requirements. We urge the SDT to consider our comments and incorporate them as appropriate when developing the final standard that will be balloted. Comments: Section 4.1.1.2 includes in the applicability Transmission Owners that own Transmission Facilities that are operating between 200kV and 499 kV at a single station or substation, where the station or substation is connected at 200kV or higher voltages to three or more other Transmission stations or substations and has an “aggregated weighted value” exceeding 3000 according to the table set forth in section 4.1.1.2. Because section 4.1.1.1 covers transmission facilities operated at 500 kV and above and section 4.1.1.2 only references Facilities operating between 200 kV and 499 kV, the fourth row in the table in section 4.1.1.2 referencing voltages of “500kV and above” is unnecessary and should be removed.
Yes
Requirement 1: 1. Requiring completion of an initial risk assessment for Transmission stations and substations planned to be in service within 24 months can lead to audit difficulties. Planned in service dates often change for a variety of internal or external reasons. It is requested that the SDT consider changing this language to a more easily identifiable trigger

such as requiring the risk assessment to be performed before a new Transmission station or substation is energized. 2. Does the R1 risk analysis require consideration of the impact of loss of lines with voltages below 200 kV in an identified Transmission station or substation? 3. It is unclear when the R.1 risk assessment needs to be completed. This should be clarified. 4. The wording in the Rationale for Requirement 1 box identifies the primary control center, but it also notes that control center electronic actions can cause direct physical actions at the Transmission station and substation. This would typically implicate the backup control center as well because the backup control center will have similar functional capabilities. There appears to be a disconnect between the use of the term primary control center and the parenthetical that follows which appears to include any control center that performs the listed functions.
Yes
Requirement 5: In the VSL table, does implemented mean complete execution of the plan including any necessary construction, or does it mean having initiated the plan but not necessarily completed all planned construction? There are only 10 days between VSLs. Requirement 6: 1. Similar to Requirement 2.3, the sub-requirements under Requirement 6.1 should be bullets, not individual sub-requirements. 2. Does R6 require subsequent third-party reviews when the security plan is revised? If so, what are the criteria?
Yes
We recommend that the SDT include a timeline within the standard which includes all required steps.
Individual
Eric Olson
Transmission Agency of Northern California
Agree
American Public Power Association
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
Agree
American Public Power Association
Individual
Tony Eddleman
Nebraska Public Power District
No
Due to the imposed time constraints and expedited development of this standard, sufficient time isn't available to develop more realistic criteria for determining applicable substations creating unnecessary work and expense for transmission planners and reviewers.
No

The third party verification is unnecessary and should be deleted from the standard. There is no other unaffiliated third party that has knowledge and expertise comparable with the incumbent Transmission Planner who develops the detailed models, performs the reliability assessments, and develops the required long term plans for the Transmission Owner on an annual basis. If the verification remains in the standard, 90 calendar days is not a sufficient amount of time to complete verification. A Transmission Planner may ask a Planning Authority (PA) to review its risk assessments, but the same PA will likely be asked to review multiple utilities. Recommend at least 180 days to complete the verification.
Yes
Since we are using CIP-002-5 for identifying Transmission stations and substations, the confidential information for these facilities is already protected under CIP-011-1 Information Protection. CIP-014-1, requirements 2.4 and 6.4 are redundant with already approved requirements and are not needed. Adding requirements for protecting sensitive or confidential information in this standard will create confusion and double jeopardy. CIP-006-5 covers physical security and any information pertaining to the substations identified through the CIP-002-5 criteria. CIP-011-1 already protects this information. Due to the expedited development of this standard, sufficient time isn't available to provide clear requirements in the standard to evaluate compliance. The RSAW does contain language that will help, but the RSAW isn't the enforceable document and can be changed without industry approval. We've learned from implementing the other CIP standards that auditors can take a completely different position than what was meant by the drafting team with little recourse for utilities.
Group
GridWise Alliance
Ladeene Freimuth
Yes
Yes
Yes
Yes
GWA includes electric utilities, information and communications technology service and equipment providers, Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs), academic institutions, and energy consulting firms. GWA appreciates the acknowledgment in the Order of the significant efforts that industry already is undertaking to enhance the resilience of the electric grid and thereby protect the grid from a range of threats, including physical, cyber, natural, and other hazards. Industry has been working in close partnership with various levels of government to enhance grid protection, reliability, resilience, and security. This collaboration is ongoing and should be fostered for the

future. As you are aware, the electric grid is dynamic in nature. Electric grid owners and operators are making investments to enhance the reliability and resiliency of the grid, and are actively managing the operation of the grid to prevent outages and to restore power expeditiously, when outages do occur. As this process moves forward, GWA wants to underscore the importance that the result not be overly burdensome or inhibit innovation. It is important that the risk assessment process indeed be limited to truly "critical" infrastructure that is deemed essential to the functioning of the bulk electric system. This will help ensure that protection measures are reasonable and cost-effective, as well as cost-sensitive, to help minimize costs to industry and also to consumers, who ultimately must bear the costs of these investments. Industry is working hard to monitor and stay ahead of the myriad threats that could arise – physical, natural, cyber, and otherwise – recognizing that the types of threats and the motivations of potential actors continue to change over time. NERC should partner with FERC to ensure that an all-hazards approach to addressing risk is undertaken going forward. We appreciate the Order's acknowledgement of the vital need to protect confidential and sensitive information. Yet, we are concerned about the nature of information-sharing under this Order, and what protections and assurances, in fact, would be implemented to prevent the inappropriate sharing of confidential information. While also recognizing the need to protect the confidentiality of such sensitive information, we also note that it is important to ensure that information sharing is facilitated between the government and the private sector, as well as within the private sector. Vendors who supply critical systems and equipment are incorporated into this process, since continued coordination and cooperation among all the stakeholders is essential.
Individual
RoLynda Shumpert
South Carolina Electric and Gas
Yes
No
A) The FERC order directs that the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. It does not require verification of the specific or particular facilities identified. Therefore, SCE&G believes this section should be clarified and specifically state that the assessment itself (i.e. the methodology used by the owner or operator) be verified and not the facilities. B) SCE&G would like the drafting team to comment on the liabilities a NERC registered entity may assume as the third party when they are used to verify the risk assessment. Specifically, if in a future audit the owner or operator's assessment is found noncompliant, then would the independent NERC registered third party entity suffer any noncompliance as well? It is important for NERC registered entities to understand their compliance risks as third parties before they agree to perform independent verification of other entities assessments.
Yes

Yes
The requirement for unaffiliated third party verification throughout this standard is not consistent with other NERC Reliability Standard verification requirements. SCE&G is concerned that this standard sets precedence for future standard third party verification which would be very costly, confusing and burdensome.
Group
SERC CIPC
Cynthia Hill-Watson
Yes
Recommend that the drafting team include the Transmission Planner who would be performing the risk assessment in the applicability as discussed in R1.
No
Recommend that the Transmission Planner perform the risk assessment in R1 instead of the Transmission Owner. Need further clarification and examples for the term “unaffiliated”. Would “peer” reviews studies that do not have a single registered entity with controlling interest suffice as an “unaffiliated” third party reviewer? What role does the SDT envision the ERO (including regional entities) playing in the review process?
No
Recommend adding electric utility experience to 6.1.3 and 6.1.4. Consider removing the requirement for CPP and PSP certifications. Rationale: Numerous other mandatory enforceable standards (e.g. MTSA, CFATS, and CT-PATS) that do not require specific certifications nor are we aware of similar certifications in cyber elsewhere in the CIP standards. Suggest clarification of “electric utility experience” and “physical security experience” to allow the ERO and registered entities to justifiably select authorized third party reviewers.
Yes
Until the process of the standards has more fully matured there should not be a presecribed methodology for conducting the Security Vulnerability Assesments (SVAs) as long as generally accepted criteria as well as as stated in the standard in 4.1, 4.2, and 4.3 are followed in the development of the evaluation and plan(s). The comments expressed herein represent a consensus of the views of the above named members of the SERC CIPC only and should not be construed as the position of the SERC Reliability Corporation, or its board or its officers.
Individual
William Temple
Northeast Utilities
Yes
Standard Drafting Team should define the term widespread. NU suggests the following definition: Widespread – An event that causes voltage collapse, Cascading and/or instability

that results in uncontrolled separation across significant portions of the Interconnection. The registered entity shall use regional criteria to evaluate.
Yes
Requirement 1 should match that language in the FERC order and not limit the assessment to Transmission System analysis and allow for an opportunity to apply technical expertise and judgment prior to the Transmission System analysis. We agree to Requirement 2 and Requirement 3.
Yes
Suggest standard allow entities to have a Master Physical Security Plan and that the standard provide for flexibility to accomplish mitigation activities associated with the results of vulnerability assessments and capture those under a separate mitigation plan (similar to the action plans associated to vulnerability assessments being conducted on Cyber Assets).
No
Group
Foundation for Resilient Societies
William R. Harris
No
1. Reliability Coordinators (RCs) would be exempted under the draft standard. Not all Reliability Coordinators are Transmission Operators or Owners. Peak Reliability, Midcontinent ISO, and Southwest Power Pool would be exempted because they are not in the NERC Compliance Registry as Transmission Operators or Owners. (MISO is not a Reliability Coordinator under its MRO registration.) The following standards apply to Reliability Coordinators but not Transmission Operators and Owners: Standard EOP-006-2 — "System Restoration Coordination"; Standard EOP-002-3.1 — "Capacity and Energy Emergencies" (Applies to Balancing Authorities, Reliability Coordinators, and Load-Serving Entities); Standard IRO-009-1 — "Reliability Coordinator Actions to Operate Within IROLs"; Standard IRO-015-1 — "Notifications and Information Exchange Between Reliability Coordinators." The Joint U.S.-Canada report on the 2003 Blackout concluded that insufficient wide-area control, such as that provided by Reliability Coordinators, was a contributing factor to the blackout. Yet the Standard Drafting Team has disregarded these findings in exempting Reliability Coordinators. It is a fallacy to believe that only entities with direct control of substations need protection from physical attack. If critical substations and their Reliability Coordinators are attacked in a coordinated manner, what entity will lead system restoration? It is essential that Reliability Coordinators are designated as responsible entities, both to protect their own facilities and to enable their authority to review the adequacy of physical security capabilities for operating utilities in their coordinating areas. Key findings of the joint U.S.- Canada Outage Task Force on the August 2003 blackout demonstrated the need for the Reliability Coordinators to actively supervise operating entities both to meet essential operating needs and to assure adequate regional visibility. See U.S.-Canada Power System Outage Task Force

Report (April 2004). <http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf> 2. Balancing Authorities would be exempted under the standard. According to the NERC Compliance Registry, there are 19 Balancing Authorities that are not also Transmission Operators or Owners. The following standards apply to Balancing Authorities but not to Transmission Operators or Owners: Standard BAL-001-2 — "Real Power Balancing Control Performance"; Standard BAL-002-1 — "Disturbance Control Performance"; Standard BAL-003-1 — "Frequency Response and Frequency Bias Setting"; Standard BAL-004-0 — "Time Error Correction"; Standard EOP-002-3.1 — "Capacity and Energy Emergencies"; Standard IRO-006-5 — "Reliability Coordination — Transmission Loading Relief". If critical substations and their Balancing Authorities are attacked in a coordinated manner, what entity will balance demand and generation and manage the emergency, especially if the attack causes a regional load imbalance? 3. Generator Operators would be exempted under the proposed standard. Generator Operators have vulnerable and hard-to-replace Generator Step Up (GSU) Transformers, just as Transmission Operators have these transformers. Generation facilities could present contingencies in excess of spinning reserves, especially in congested areas with import of large megawatts of power over long transmission lines. Hence, Generator Operators should be included in mandatory physical security protection standards. 4. The standard does not require modeled contingency planning for scenarios of physical attack. Contingency planning for physical attack should include megawatt capacity of all generators at single generation facility, not just failure of some individual units at the facility. 5. Without explicit modeling for physical attack, some substations may fall through the cracks under "Aggregate Weighted Value" methodology in the standard. Physical attack of multiple transformers is different than the random failures planned for under the standard N-1 criterion. We have already seen attack on multiple transformers and their circuits at the Metcalf substation. The standard's criterion for violation of IROL limits would not be valid if the IROL limits assume random failures rather than coordinated physical attack. 6. Some "High Impact" control centers would be exempt under the standard. Examples include the control centers for Peak Reliability, MISO, and SPP. In all, these control centers manage power for 141 million Americans. Control centers for Reliability Coordinators, Balancing Authorities, and Generator Operators are included in the "High Impact" Criteria for CIP-002-5.1 How can the standard drafting team take the CIP-002-5.1 criteria for substations but not control centers of Reliability Coordinators, Balancing Authorities, and Generator Operators? FERC Directive RD14-6-000 specifically requires protection of critical control centers in Footnote 6: "… the Commission expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers." 7. While FERC Directive RD14-6-000 [146 FERC ¶61,166] did not require specific security measures, it could have been reasonably expected that NERC would have developed specific measures to be applied on an as-needed basis. Nonetheless, the draft standard contains no specific requirements or even suggested guidelines for physical security measures. Such measures might include: Opaque Fencing; Concrete Jersey Barriers; Motion Sensors; License Plate Scanners; Intentional Electromagnetic Interference (IEMI) Detectors; Gunfire Locators; Limiting of Close Public Access, Including Recreational Access; Armed Private Guards; Police Details; Deployment of National Guard

Troops; Better Stocking of Spares—e.g., Transformer Bushings and Radiators; Equipment Monitoring and Redundant Telemetry to Control Centers. Instead, the standard relies upon self-devised security measures without prioritization or other guidance. 8. The Metcalf incident unambiguously showed the value of equipment monitoring in mitigating physical attack on power transformers. Gunfire locators, had they been installed at Metcalf, could have alerted system operators to the attack in real-time, allowing prompt dispatch of law enforcement. Intentional Electromagnetic Interference (IEMI) Detectors could likewise provide real-time warning. If threat sensors with reliable and cyber-protected alerts are not part of a physical security system, it will be impossible to mobilize time-urgent countermeasures and impractical to take precautionary measures at other at-risk facilities vulnerable to coordinated attack. 9. Intentional Electromagnetic Interference should be a physical threat included in the standard, because IEMI attack could occur in the physical proximity of facilities and could cause permanent physical damage in additional to temporary upset. IEMI detectors are a cost-effective measure as these devices cost approximately $15,000 per unit. 10. The Metcalf Incident was both a physical attack and a cyber denial-of-service attack. The need for linkage between physical and cyber is explicitly called for in the RD14-6-000 Order of March 7, 2014, para 5, footnote 3. The implementation plan under this Order must require responsible entities to identify and protect cyber assets that link facilities and control centers that are otherwise identified as critical to the reliability of the BES. Communications and Network entities routinely provide hardened and alternate routing for military, other government and the Defense Industrial Base and their services should be an explicit requirement for Physical Security Standards that apply to any units and control centers that are identified by Responsible Entities as critical to the Reliability of the BES. 11. Review and certification of security plans, as proposed in the draft standard, does not necessarily provide a level of independence that would be prudent or credible to the public. Regional Entities or Reliability Coordinators for any facilities under their jurisdiction should be the primary authorities to review and approve security plans. Governmental authorities should have the ability to audit security plans. 12. Improvements to the standard that we suggest would be marginal additions of facilities and their equipment and therefore would be cost-effective. We propose inclusion of primary and backup control centers for Peak Reliability, MISO, and SPP—an increase of 6 control centers as compared to approximately 200 already included Transmission Operator control centers. We propose inclusion of 19 additional Balancing Authorities as compared to 114 Balancing Authorities in total. There are only 50 non-nuclear generation facilities in the United States with nameplate capacity of 2 GW or more—this number is a rough approximation of the number of generation facilities that modeling might show to be capable of causing cascading outage if successfully attacked. 13. RD14-6-000 directs NERC to submit for approval a physical security standard that would apply to the most critical facilities of the Bulk Electric System. The Standard Drafting Team has narrowly interpreted “critical facilities” to mean transmission facilities and directly linked control centers. We disagree with this narrow interpretation. Given the NERC interpretation and the 90 day deadline for standard development, NERC’s draft standard holds tightly to the most minimal facilities and therefore has significant gaps in protection as we describe in our foregoing comments. Some of these gaps, such as the exemption of Reliability Coordinators

and Balancing Authorities, are so fundamental that they should be addressed immediately. For other gaps, we ask that NERC open a Standard Authorization Request (SAR) for a Phase Two physical security standard. This follow-on Phase Two standard should require modeling of BES operations sufficient to ensure identification of facilities that could cause cascading outage, single points of failure, data connectivity needs, and other processes and technologies essential to grid protection—in short, a standard designated CIP-014 Version 2. An approved SAR for a Phase Two standard should be concurrent with NERC Board of Trustees approval of the current standard in development.
No
Same answer as provided to Question 1.
No
The third party review is not adequately specified. The Joint U.S.-Canada Outage Tasf Force Report (April 2004) determined that lack of Reliability Coordinator oversight, and legal authority, contributed to inadequate supervision of transmission operators, and reduced visibility of regional inadequacies. See our comment to Question 1 for our view that Reliability Coordinators and Balancing Authorities must be involved.
Yes
We recognize that FERC has established a 90-day review process, and that NERC has worked to meet the tight deadline. Hence, the Foundation for Resilient Societies asks NERC to develop a SAR for Physical Security Standards - Phase 2. In this process, analytical modeling should be undertaken to identify and prioritize physical security risks that include cyber vulnerabilities, and that relate to the need for reliable warning and communications via redundant channels to control centers and to law enforcement. It should not be acceptable to exclude Regional Coordinators and Balancing Authorities, both groups needing to review and perhaps upgrade their own physical security, and both groups playing key roles in oversight of the operating entities, both TOs and GOs, whose physical security may be essential to prevent long-term outages through coordinated attacks. For additional materials prepared by the Foundation for Resilient Societies, contact the FERC staff designated to assist NERC with standard setting in FERC Docket RD14-6-000.
Individual
Guy Andrews
Georgia System Operations Corporation
No
Georgia System Operations Corporation (GSOC) appreciates all the effort going into the draft of CIP-014-1 Physical Security Reliability Standard. GSOC supports the comments submitted by NRECA.
No
GSOC supports the comments submitted by both Georgia Transmission Corporation (GTC) and NRECA
No

• GSOC supports the comments submitted by both GTC and NRECA. • In addition, GSOC suggests in R4.2 changing “Prior history or attacks on” to Prior history of physical security related events at” to better describe the subrequirement. • GSOC suggests in R6, last sentence, changing the word “development” to “developed” in order to be consistent with the word “performed” in the same sentence.
Yes
GSOC supports the comments submitted by NRECA
Individual
David Godfrey
Texas Municipal Power Agency
Agree
City of Garland and American Public Power Assocation
Group
Bureau of Reclamation
Erika Doot
No
The Bureau of Reclamation (Reclamation) believes that the Transmission Planner, Planning Coordinator, and Reliability Coordinator should be included in the Applicability section of the standard and should be responsible for reviewing the Transmission Owner’s risk assessment (BES impact assessment).
No
Reclamation agrees with this approach. However, to promote consistent identification of critical facilities within an interconnection, Reclamation believes that the third-party review should be conducted by the Transmission Owner (TO)’s Planning Coordinator or Transmission Planner. If the Transmission Owner is also the Transmission Planner and Planning Coordinator, the third-party review should be performed by the Reliability Coordinator. Reclamation also suggests that the drafting team modify the term “risk assessment” to “BES impact assessment.” In the physical security community, the term “risk assessment” generally refers to “The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel.” See ASIS International, General Security Risk Assesment Guideline (2002), http://www.scnus.org/local_includes/downloads/9200.pdf. In its filing to FERC, NERC can explain that it adopted the term “BES impact assessment” so it is clear that the initial evaluation is of risk to the BES if the substation is rendered inoperable or damaged. Reclamation also recommends revising R1.1 to require subsequent risk assessments every 60 months for all Transmission Owners. Reclamation believes that periodic risk assessments are necessary, but has not seen evidence that the costs associated with updating risk assessments every 30 months rather than every 60 months would provide commensurate reliability benefits. Reclamation recommends that the drafting team update R1.1 to state, “Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or Transmission substations that if rendered inoperable or damaged

could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment.”
No
Reclamation agrees with the requirements to develop a threat assessment and physical security plan. Reclamation also agrees with the inclusion of governmental agencies with physical security expertise as threat assessment and physical security plan reviewers. However, Reclamation does not believe that the proposed requirements will allow adequate time for a comprehensive review. Reclamation suggests that at least 180 days would be a more appropriate timeframe for a detailed threat analysis and physical security plan review. Reclamation also requests that the drafting team clarify the scope of third party reviews of these threat assesments and physical security plans, perhaps by adding additional detail to the Guidance and Technical Basis section. Reclamation is not convinced that third-party reviews will increase reliability. Reclamation believes that each entity is in the best position to evaultate threats to its facilities and determine appropriate mitigation plans. Reclamation is concerned that the well-intentioned third-party review mandated by the order could result in classified or national security related information falling into the wrong hands. Reclamation does not believe that non-disclosure agreements will adequately protect this sensitive information.Reclamation believes that audits by regional entities in essence provide a “third-party” review of an entity’s threat assessments and physical security plans.
Yes
Reclamation is concerned that the term “primary control center” will become confused with the NERC Glossary term “Control Center.” As indicated by the use of the term “monitor” in the definition of Control Center, Reclamation does not believe that the concept of “operational control” has been equated with “causing direct physical action” to date. To avoid confusion, Reclamation suggests that the drafting team replace the R1 phrase “primary control center that operationally controls eachTransmission station or Transmission substation” with the phrase “primary control center that physically controls each Transmission station or Transmission substation.”
Individual
David Revill
Georgia Transmission Corporation
No
Georgia Transmission Corporation (GTC) supports the efforts of the drafting team and believes that their efforts to create the CIP-014 Standard are moving in the right direction. GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard.
No
-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard. -GTC is concerned that the language of the standard and rationale around the use of the term “unaffiliated” in R2 and R6 does not

provide sufficient clarity for a registered entity to have confidence in the consistent applicability and auditability of the requirement. GTC suggests additional examples or requirement language to consider whether: -entities that are not under the same corporate parent but which have contractual obligations between each other would be considered “unaffiliated” - organizations or teams made up of representatives of multiple utilities with no one utility having a controlling interest in the findings of the group would be considered “unaffiliated”
No
-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard. - GTC requests revision to the requirement language or addition of guidance around the phrasing of “unique characteristics” in R4 to address whether all equipment within an identified substation has to be assessed in R4 or if an entity has the option to focus their threat and vulnerability assessment on specific facilities in the substation which were identified as causing the adverse effects described in R1. -GTC is concerned that the language of the standard and rationale around the use of the term “unaffiliated” in R2 and R6 does not provide sufficient clarity for a registered entity to have confidence in the consistent applicability and auditability of the requirement. GTC suggests additional examples or requirement language to consider whether: -entities that are not under the same corporate parent but which have contractual obligations between each other would be considered “unaffiliated” - organizations or teams made up of representatives of multiple utilities with no one utility having a controlling interest in the findings of the group would be considered “unaffiliated”
Yes
-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard. -GTC suggests that in M2 the word “communications” be changed to “notifications” to follow the language of the requirement. -GTC suggests that in M2 and M6 the measures should be updated to include evidence of the qualifications and independence of the respective review teams. -GTC suggests that M6 the measures should be updated to include evidence of the implementation of procedures for information protection used during the third-party review.
Individual
Scott Langston
City of Tallahassee
Agree
APPA
Individual
Bernard Johnson
Oglethorpe Power Corporation
Agree
Georgia Transmission Corporation (GTC) National Rural Electric Cooperative Association (NRECA)

Group
National Grid
Michael Jones
Yes
It should be clear that the applicability section of the standard is only intended to provide a valid, technically sound basis to be used as the ‘starting point’ to those transmission facilities or stations that should be included in the risk assessment. We suggest the following modifications: 4.0 Applicability: 4.1 Functional Entities: 4.1.1 Transmission Owner that owns any facilities identified in the following sections (4.1.1.1 through 4.1.1.4) will be required to perform the risk assessment and risk assessment validation as outlined in R1 and R2 of this standard. Should the risk assessment identify critical assets then the Transmission Owner is subject to the remaining requirements (R3 through R6) of the standard. 4.1.2 Transmission Operator
No
While we support using the CIP-002-5.1 criteria as a starting point for applicability of the draft standard, we do have concerns with the inclusion of the phrase “within an Interconnection” in R1. FERC Order RD14-6 directs that "[a] critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System". By introducing the word “within,” the Standard could inadvertently draw widely different interpretations of how to assess risks to the BPS. In practice, this could open up the potential for the inclusion of regional or localized transmission impacts, which we believe is in contrast with the Commission intended scope in the Order. As a result, we suggest that the wording in R1 be modified to the following: “A critical facility is one that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation or cascading failures widespread across significant portions of an Interconnection". Alternatively, we recommend clarifying in the guidance documents that ‘widespread’ and ‘within an Interconnection’ proposed words are intended to apply to impacts to the BPS that reaches deep into the Interconnection, and not affecting a small portion of an Interconnection. For example, if an Interconnection has relatively small Balancing Authorities (BAs), ‘widespread’ would need to be interpreted as impacts that would be crossing several, i.e. more than two, of those BAs in order to be considered ‘widespread’.
Yes
No
Individual
Donna Johnson
Oglethorpe Power Corporation
Agree

Georgia Transmission Corporation (GTC) National Rural Electric Cooperative Association (NRECA)
Individual
Joshua Andersen
Salt River Project
Yes
SRP supports comments submitted by APPA.
No
SRP supports comments submitted by APPA with the following additions: The time frame for completion of the initial risk assessment required in Requirement R1 is not identified in the standard, only in the implementation plan. This may be a point of confusion for entities that fail to fully read and understand the implementation plan. If possible, could the drafting team revise the language of Requirement R1 to make this clear? The periodicity of the risk assessments required by Requirement 1 and the time frame that the risk assessments appear to not align. The risk assessment is required to include Transmission stations and Transmission substations that exist as well as those planned to be in service within 24 months. However, the periodicity for conducting future risk assessments is every 30 calendar months or every 60 calendar months if the prior risk assessment did not identify any Transmission stations or Transmission substations. This potentially leaves a gap of six to 36 months where facilities may not have been assessed. In R2 it is not clear that the primary control center must also be verified, but in subsequent requirements it implies or states that it should be. If the intent in R2 is that the primary control center should also be verified, then it should state so in R2.2 and R2.3 in addition to stating stations and substations. Third Party Verifiers: SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated

with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities. Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers. Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
No
SRP supports comments submitted by APPA with the following additions: Third Party Verifiers: SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different

in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities. Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers. Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
Yes
Section C “Compliance” 1.4 (page 13) which states “...all evidence will be retained at the TO and TOP facilities.” is contradictory with NERC Compliance Monitoring and Enforcement practices which allow data to be exchanged with and sent to Regional Entities such as in pre-Audit data requests and Mitigation Plans. In addition, this would be burdensome for the TO/TOP because the 3rd party verifying/reviewing entities would need to be on-site and potentially incur travel expense.
Individual
Patrick Farrell
Southern California Edison Company
Yes
No
SCE has concerns with both Requirement R1 and Requirement R3. In Requirement R1, SCE recommends that the verbiage be changed from “…that if rendered inoperable or damaged could result in widespread instability...” to “...that if damaged to the point of being rendered inoperable could result in widespread instability..." SCE requests this change to reduce ambiguity in the application of the word "damaged." In addition, language should be added to R1 that specifies: “…system instability such as uncontrolled separation or cascading within 15 minutes of compromise…,” as a 15-minute window would align with criteria in the CIP standards used to determine critical facilities. In the guidance section for R1, SCE would suggest changing the text from “…remedial action schemes (RAS) or special protection

systems (SPS)" to "…special protection systems (SPS)…," because as used in the NERC Glossary of Terms, a RAS is included as a type of SPS. In addition, SCE requests that R1 be revised to include specific examples and criteria for the risks to be measured. For instance, SCE believes the following could be among the examples and criteria specifically included: (a) Thermal overloads beyond facility emergency ratings; (b) Voltage deviation exceeding ± 10%; (c) Cascading outage/Voltage collapse; and (d) Frequency below under-frequency load shed points. With respect to Requirement R3, SCE requests that additional guidance be provided on how a "primary control center" should be identified, as that term in used in both Requirements R1.2 and R3. SCE also asks the team to consider changing the notification requirement in R3 from seven(7) to thirty(30) days in order to allow sufficient time for the transmission owner and transmission operator to perform the required communication.
No
SCE has concerns with Requirements R4, R5, and R6 that will be described below. With respect to Requirement R4, SCE notes that entities are required to "…conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s)…" SCE requests the inclusion of additional guidance or examples of threats and potential vulnerabilities that an entity may want to consider. This will allow entities to perform a threat assessment and develop preventative measures that are commensurate with the intent of the standard. In addition, SCE requests additional guidance on physical security plans that allow for flexibility to deal with emergent threats. With respect to Requirement R5, SCE believes that in the guidance section, the drafting team should consider referencing standards that are used by security professionals or organizations, in order to ensure that the criteria to identify appropriate countermeasures to potential threats and physical attacks are evaluated along similar themes across industry. SCE also requests that the team consider rephrasing R5.1 from "Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond…" to describe the control, to "…deter, detect and delay, and also assess, communicate, and respond…" With respect to Requirement R6, SCE requests that the team consider rewording Requirement R6.1 from "Each Transmission Owner and Transmission Operator…" to "Each Transmission Owner or Transmission Operator, with facilities identified as a result of R2,…"
No
Individual
John Hagen
Pacific Gas and Electric Company
Yes
Yes

R2 Comment: Suggest removal of the requirement for a third party risk assessment verification. Verifications already occur as part of internal compliance programs in CIP-002 and when audited by the Region. What if the assessment is performed by a third party, do you have to get another third party to verify? This creates a significant administrative burden, even if the Standard will only apply to a small number of entities and facilities. R3 (pg. 8) "…the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify…" Comment: Seven calendar days may be too short a time requirement, consider 10-14 days
Yes
R4 (pg. 9) "…shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s)…" Comment: Consider stating "…conduct a physical security risk assessment to identify and evaluate potential threats and vulnerabilities…" The assessment should identify the potential threats and vulnerabilities to evaluate and implement the necessary protective, detective and corrective countermeasures R5 (pg. 10) states to develop and implement a documented security plan (s) within 120 calendar days of completion of R2 (unaffiliated third party verify the risk assessment form R1). Furthermore, R5.1 states to address the potential threats and vulnerabilities from R4. 120 days to implement the countermeasures may not be enough time (logistics, procurement, installation timelines, approvals, etc.). Comment: Could they say "…shall develop and begin implementation of a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days…" because in R5.3 it requires a timeline for implementing the enhancements. 6.1.1. (pg.11) "An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification." Comment: Shouldn't require a specific certification, should say something like "The third party must include in their review the qualifications of the staff performing the review." R6.1.2 (pg. 11) "An entity or organization approved by the ERO." Comment: What criteria is the ERO using to approve entities or organizations? The approval process needs to be spelled out. R6.1.3 (pg. 11) "An entity or organization with demonstrated law enforcement, government, or military physical security expertise" Comment: Does this mean we can use Law Enforcement agencies or firms with retired law enforcement personnel?
Yes
Compliance 1.2 (pg. 13) Comment: can they clarify by being less wordy and just start by saying "The responsible entities shall retain documentation as evidence for three years", followed by the rest in less words?
Group
ISO/RTO Standards Review Committee
Greg Campoli
Yes

Introduction The proposed standard provides adequate flexibility with respect to the risk assessments and security evaluations and plans. This allows the industry to capitalize on their experience in these matters, while also accommodating changes that warrant consideration. Applicability Section The applicability scope is reasonable in terms of identifying the appropriate functional entities to address physical security concerns. Similarly, the proposed standard establishes a reasonable approach for identifying the scope of facilities by 1) initially defining an objective set based on the CIP-002-5.1 criteria, and then 2) refining that set based on analyses that assess the relationship of those facilities to specific, system conditions/impacts metrics – i.e. widespread instability, uncontrolled separation, or Cascading within an Interconnection.
Yes
R1 R1 in conjunctions with the Applicability section is a reasonable approach for identifying the scope of facilities subject to R2 – R6. R2 Imposing a verification requirement is a reasonable way to facilitate an effective outcome in terms of identifying facilities that meet the impact thresholds established in R1. Requiring the use of an unaffiliated third party is reasonable because it mitigates the potential for inadvertent error in study work. Finally, allowing the verification to occur concurrently or subsequently, and leaving that decision to the discretion of the relevant functional entities, is appropriate. The functional entities should have the discretion to determine the most effective means of performing the verification. R2.1 requires that the verifying entity be either 1) a registered RC, PC or TP, or 2) another entity with appropriate planning or analysis experience. This is a reasonable approach that provides appropriate flexibility with respect to third party verification options. It also addresses the different operational and planning structures that comprise the North American electric grid – i.e. organized market regions where different entities can perform the different NERC registered functional roles (ISOs/RTOs) and vertically integrated regions where all the relevant roles under the standard may be performed by a single entity and, therefore, would require the use of an independent third party to perform the unaffiliated verification. R2.2 requires the third party verification to either confirm the TO analysis under R1, or, alternatively, recommend that facilities be added or deleted (the IRC assumes that a verification can confirm some results and also add facilties or remove facilities). Although R2.2 establishes a reasonable standard – i.e. verify TO results or recommend changes - the IRC offers the following comments. The requirement, as written, imposes the obligation on the third party verifying entity. However, the TO is the responsible entity under the standard – i.e. the TO is required to obtain the third party verification. The language should be revised to clarify that the relevant actionable obligation (to obtain the third party verification) lies with the TO. The next issue raised by R2.2 is the timing. The IRC appreciates the importance of the issues being addressed by the proposed standard and the goal of implementing the standard and the relevant processes contained therein in a timely fashion. However, practically speaking, 90 days may be difficult to meet depending on the number of Transmission Owners that require verification from a single Registered Entity. For example, in organized markets there may be numerous TOs all selecting their PC to verify. To the extent implicated in reviews under the standard, IRC members would make best efforts to perform any relevant verifications. This comment is merely intended to highlight the potential resource impacts

under the proposed 90 day timeline. The IRC proposes the following revisions to mitigate the issues in R2.2 described above. 2.2. The third party verification shall either verify the Transmission Owner's risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within a mutually agreed upon timeframe between the Transmission Owner and the third party but no longer than 180 calendar days following the completion of the Requirement R1 risk assessment. R3 R3 obligates the TO to notify a TOP that has operational control of a control center associated with a facility identified pursuant R1 and verified under R2. R3.1 requires similar notification if a facility is removed via those processes. The standard may benefit from including the draft guidance into the R3 rationale section that clarifies that operational control means the ability to take action that affects the physical status of the facility, and that it does not include directive control, which relies upon another entity to take operational action to change the status of the facility. The guidance document addresses this issue, but the SDT could add clarifying language to the rationale section of R3, similar to the language in the guidance document and/or the language in the R1 rationale section, which reads in relevant part: "… identify the primary control center that operationally controls that Transmission station or Transmission substation (i.e., the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity)."
The IRC has no comments on R4-R6.
No
Group
APPA
Paul Haase
Agree
The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the Introduction Section: 7. Critical Facilities Information Records and related information concerning critical facilities, physical infrastructure, including risk assessments

and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. Proposed Requirement Language (new subrequirements): R1 1.3 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under this standard. R3 3.4 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under Requirement R1 of this standard. R4 4.1 The Transmission Owner will keep confidential all records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1 conducted under this standard.
Individual
David Francis
MISO
Yes
MISO supports the proposed applicability section and agrees that other entities do not need to be included. In particular, MISO would not support application of this Standard to Reliability Coordinators or Balancing Authorities, as these entities' control centers are adequately protected with regard to physicial security under CIP-006-3c and its successor standard. Moreover, these control centers are subject to the requirements of EOP-008-1 including the transfer functional control to backup facilities. MISO therefore agrees that the focus of CIP-014-1 should be those facilities that are not otherwise fully protected by CIP-006-3c, such as those that do not not rely entirely on Critical Cyber Assets to maintain reliability.
No
MISO recognizes that the Commission mandated third-party verification of the risk assessment required under R1, however the current language of R2 requires modification to address several concerns MISO has with regard to its potential role as a verifying entity. While MISO has every confidence that it can perform risk assessment verifications in a safe, responsible, and accurate manner, the combination of a high number of requests requiring

verification within a relatively short period of time presents some concerns to MISO regarding its resource allocation and availability. In particular, MISO recommends that the SDT add language limiting the universe of Transmission Owners/Operators that can seek verification from a particular verifying entity (potentially by geographical region or contractual or functional relationship) as well as modify the 90 day requirement to take into account that a single entity may have more requests than it can feasibly complete in such a short time period. An example of language that MISO could support is language that would allow a verifying entity and the requesting Transmission Owners/Operators to agree upon an appropriate completion date beyond the 90 days where the 90 day period will not allow completion of a robust verification due to resource constraints by the berifying entity. Finally, MISO respectfully requests that the SDT consider adding language to Requirement R2 that would allow verifying entities to limit liability related to both enforcement actions within the jurisdiction of FERC, NERC, and the Regional Entities and other actions that could be brought against verifying entities in other jurisdictions and venues unless it is shown that the entity lacked good faith or was grossly negligent.
Yes
No
Individual
Sergio Banuelos
Tri-State Generation and Transmission Association, Inc.
No
The drafting team may want to consider language referencing the CIP-002 Critereon rather than outright copying it in order to prevent changing multiple standards as the CIP-002 standard evolves. CIP-002-5.1 Attachment 1: Overall Application gave guidance on how to treat joint ownership facilities. Tri-State feels that this new standard would also benefit from such guidance.
No
Rather than making it the Responsible Entity’s responsibility to find a third party to verify its assessment, Tri-State believes it would better suit the industry and the standard if R2 required either the Reliability Coordinator or Regional Entity to request TO's assessments on an intervaled basis. This meets the requirements of the March 7 FERC Order. Allowing the requirement to be broad enough to allow third party paid consultants with “transmission planning or analysis experience” creates a conflict of interest and contradicts the draft standard’s requirements for the use of “unaffiliated third part[ies]”. If third party – other than NERC or the RE – verification of the assessment is required by the standard, then this is effectively two audits (and two 3rd party assessments) on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the

standard is currently drafted. Tri-State recommends that rather than 30 months and 60 month risk assessment intervals for R1.1, they should be a more straightforward 36 months and 72 months respectfully in order to be consistent withnormal auditing time periods of three years. This will make the intervals easier to track with internal programs and controls.
No
Tri-State disagrees that the FERC order specifically forces the drafting team to have a requirement for 3rd party verification. The order uses the word “should,” not “shall” or “require.” Tri-State would argue that 3rd party verification would/will occur during scheduled audit times. Again if the drafting team feels a need to require an additional 3rd party verification, it should require the Regional Entity or Reliability Coordinator to request the plans.
Yes
While the FERC Order RD14-6 paragraph 13 does require NERC to file a proposed standard within 90 days, footnote 8 only requires that the proposed standard include timelines for certain elements, without specificity for what those timeframes should be. The bright line CIP version 5 applicability that is used within this standard became effective 02-03-14 and was giving industry 24 months to implement. The CIP-014 draft appears to assume those bright line considerations are already completed for industry and provides just over 6 months to complete an additional assessment to remain compliant. Without specific implementation timeframes provided by FERC, and to stay in closer alignment to the expected completion dates for CIP v5, Tri-State is recommending no less than a one year after this standard becomes effective for the R1 risk assessment to be completed.
Group
California Public Utilities Commission: Safety and Enforcenment Division
Raymond G. Fugere
Agree
California Public Utilities Commission Safety and Enforcenment Division
Group
Bonneville Power Administration
Andrea Jessup
Yes
4. Applicability: BPA believes that the medium list for HV transmission entities will result in numerous facilities having to be protected (all 500 kV) contrary to the drafting team comment that not many facilities will be deemed critical. 4.1. Functional Entities: BPA recommends that this section reference the criteria of CIP-002-5.1 for a “medium impact rating,” instead of re-stating it without citation. Otherwise it is confusing. For example, the source of the tabulated weighting criteria is unclear and it is difficult to know there is a connection to any previous or established standards.
No

R1 Terminology: Although the term “risk assessment” in this section is in alignment with language in the FERC order, BPA recommends that it be revised to consequence or impact assessment. This is a physical security standard, and the term risk assessment should be reserved for the physical security risk section of this standard and align with security industry use of the term. BPA believes the basic intent of R1 is to identify substation facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection can create unacceptable consequences to the BES and not to assess risk of the event happening. Also, BPA suggests that additional sub-requirements be added to provide clarity on what system conditions and performance criteria or methodology need to be considered in order to determine what stations and substations will be deemed critical. Similar language found in existing standards would be helpful. Examples: FAC-010-2.1 (System Operating Limits Methodology for the Planning Horizon), R1-R3; FAC-013-2 (Assessment of Transfer Capability in the Near-Term Planning Horizon), R1; TPL-001-4 (Transmission System Planning Performance Requirements), R1-R6; TPL-004-0a (System Performance Following Extreme BES Events), R1. "R1 1.1. Subsequent risk assessments shall be performed:" BPA recommends revising R1 1.1 to: “Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment.” Justification: This would consolidate the two bulleted actions and make them equally applicable. BPA has been doing substation facility impact and security risk assessments for the past 15 years and our experience is that the criticality of a substation facility does not change once ranked; once it is determined critical it will always be critical particularly when information is used in a physical security risk assessment. A 5 year interval would be a more appropriate interval for this type of assessment as it would always be case of identifying new facilities and not excluding ones previously identified. "R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. [VRF: Medium; Time-Horizon: Long-term Planning]" BPA recommends revising R2 first sentence to: "R2 Each Transmission Owner shall verify the impact assessment performed under requirement R1 by a third party entity other than the owner or operator." Justification: This fully aligns with the requirements of the FERC order by using the requirements of the FERC order. BPA believes the introduction of a requirement of an unaffiliated reviewer is reaching beyond the requirements established by the FERC order, and this requirement will dilute the quality of an impact assessment. It will limit the types of entities that can perform an independent review, and directs use of resources that may not be capable of assessing all physical risks within an electrical facility. BPA proposes that the word unaffiliated be removed from this standard and replaced with language that describes the degree of separation from the facility owning entity to be considered a third party entity other than the owner or operator. Based on the definition provided in this draft “unaffiliated” is especially troublesome for federal government-owned transmission networks and facilities because it could be interpreted as excluding the entire federal government from eligibility as a third party entity to the federal government

transmission owner. Also, BPA believes industry peer reviews should be encouraged and considered as meeting the requirement. Reviews by industry peers are known to be beneficial to the entity receiving the review and for the entity performing the review or audit. Enabling industry peer reviews would not only meet the intent of an independent review but also accelerate continuous learning and translation of the most effective security approaches into widespread use. Please note that the FERC order only recommends this verification as it is stated as “should” and not as “shall.” "R.3 For a primary control center(s) identified by the Transmission Owner according to Requirement R1 and verified according to Requirement R2 that is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. [VRF: Lower; Time- Horizon: Long-term Planning]" BPA recommends revising the 7 day requirement in R3 and R3 3.1 to 30 calendar days. Justification: This information is not that time critical at this stage, and one week will not be enough time to complete all notifications.

No

R4. BPA agrees with the requirements to develop a threat assessment and physical security plan. BPA also agrees with the inclusion of governmental agencies with physical security expertise as threat assessment and physical security plan reviewers as noted in R6 (Section R6.1.3.) However, BPA requests that the drafting team clarify the scope and purpose of third party reviews should they remain as part of the standard. BPA disagrees that third party reviews will increase reliability and notes the draft standard exceeds the scope of the FERC order Paragraph 11. BPA believes that each entity is in the best position to evaluate threats to its facilities and determine appropriate mitigation plans. Nonetheless if third review is deemed necessary, BPA believes that it should be allowed to have another federal agency perform its third party review. In other words, for purposes of this standard, another federal agency would be deemed to be “unaffiliated” with BPA. Keeping this information within the federal government will decrease the risk of inappropriate disclosure of such information. BPA believes that non-disclosure agreements with non-federal parties may be a poor substitute for this because they can only be enforced once a disclosure is made. At that point, it is often too late and the information is available to a wider audience than intended. "R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator’s primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following attributes: [VRF: High; Time-Horizon: Long-term Planning]" BPA recommends revising the 120 day requirement in R5 to 12 calendar months. Justification: This information is important to get right as security designs and enhancements will be built from this plan. 120 days is not be enough time to develop a complete and effective security plan

and incorporate finalized threat assessments. "R6 Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. [VRF: Medium; Time-Horizon: Long-term Planning]" BPA recommends revising R6 first sentence to: "R6 Each Transmission Owner shall verify the risk assessment performed under requirement R4 by a third party entity other than the owner or operator." Justification: BPA believes the proposed revision fully aligns with the requirements of the FERC order by using the requirements of the FERC order. The introduction of a requirement of an unaffiliated reviewer is reaching beyond the requirements established by the FERC order, and this requirement will dilute the quality of a risk assessment. It will limit the types of entities that can perform an independent review, and directs use of resources that may not be capable of assessing all physical risks within an electrical facility. BPA proposes the word unaffiliated be removed from this standard and replaced with language that describes the degree of separation from the facility owning entity to be considered a third party entity other than the owner or operator. Based on the definition provided in this draft "unaffiliated" is especially troublesome for federal government owned transmission networks and facilities because it could be interpreted as excluding the entire federal government from eligibility as a third party entity to the government transmission owner. Also, industry peer reviews should be encouraged and considered as meeting the requirement. Reviews by industry peers are known to be beneficial to the entity receiving the review and for the entity performing the review or audit. Enabling industry peer reviews would not only meet the intent of an independent review but also accelerate continuous learning and translation of the most effective security approaches into wide spread use. Please note that the FERC order only recommends this verification as it is stated as "should" and not as "shall."

Yes

The current draft requiring "unaffiliated" third party review is more restrictive than the requirements language in the FERC order and meeting an unaffiliated requirement will be problematic for federally owned power and transmission systems. Paragraph 8 of the order: "Thus, the Reliability Standards should require the owners or operator to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process." BPA's interpretation of the FERC order is that consultation with peer entities would be acceptable methods for review of evaluation processes. In fact the order by its wording encourages such consultations without restriction as to business or corporate relationships. The draft standard limits and excludes highly qualified security and technical expertise found across the industry and within entities

corporate and governmental structures, hierarchies and partnerships where vast levels of experience, training and ability exist. The “unaffiliated” requirement forces entities to seek expertise where there may or may not be such expertise and where there is no track record of such expertise. The term “unaffiliated” and any reference to that level of separation between entities are completely void from the order and should be removed from the draft standard. Paragraph 11 of the FERC order: “In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity.” BPA believes the draft standard limits and excludes highly qualified security and technical expertise found across the industry and within entities corporate and governmental structures, hierarchies and partnerships where vast levels of experience, training and ability exist. The “unaffiliated” requirement forces entities to seek expertise where there may or may not be such expertise and where there is no track record of such expertise. The term “unaffiliated” and any reference to that level of separation between entities are completely void from the order and should be removed from the draft standard.

Group

California Public Utilities Commission: Safety and Enforcenment Division

Raymond Fugere

No comments

In general, the overall method employed in the draft standard is reasonable. The draft standard has adopted a reasonable level of specificity, without being overly prescriptive. The use of unaffiliated verifying experts is a positive element in the draft standard. In general, the balancing authority or reliability coordinator for the transmission area in question is the best verifying expert. In the event the utilities disagree with the assessments of the unaffiliated verifying entities at any point in the process (for example see section 2.3, second bullet point), not only should the transmission owner or utility be required to document their technical rationale, but the standard should further delineate a process for resolving this disagreement. With respect to Rule R1, Section 1.1, the drafting group should consider whether there should be language added to the standard detailing a process whereby the 30 or 60 month intervals should be accelerated in the event of serious intervening situations. With respect to Rule R2, Section 2.1, the description of “an entity that has transmission planning or analysis experience” is overly vague and should be further clarified, or that the use of this type of expert should be limited to certain small transmission owners. With respect to Rule R2, section 2.4, the language requiring “non-disclosure” agreements is important and a positive element in the draft standard.

In general, the overall method employed in the draft standard is reasonable. The draft standard has adopted a reasonable level of specificity, without being overly prescriptive. The use of unaffiliated verifying experts is a positive element in the draft standard. In general, we believe that the balancing authority or reliability coordinator for the transmission area in question is the best verifying expert. In the event the utilities disagree with the assessments of the unaffiliated verifying entities at any point in the process (for example see section 2.3,

second bullet point), not only should the transmission owner or utility be required to document their technical rationale, but the standard should further delineate a process for resolving this disagreement. Section 5.1 of the draft refers to “resiliency”. Does this term refers to actions such as building redundancy or improving protective schemes, as opposed to direct physical protection activities? The standard should clarify the meaning of the term resiliency. Section 4.1 of the draft refers to “unique characteristics.” Assuming this consideration includes availability of spares and ease of repair, the language is acceptable. With respect to Rule 5, section 5.2, the drafting group should consider language requiring the security plan to include contact and coordinating information for other utilities or important stakeholders, in addition to law enforcement. With respect to Rule R6, section 6.4 the language requiring “non-disclosure” agreements is important and a positive element in the draft standard. Section 4.2 lists the elements to be considered in evaluating the potential threats and vulnerabilities to physical attack, and specifically states "[p]rior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events and ...". We suggest that in additional to geographic proximity, that the section add language concerning "similarity of geographic characteristics". While geographic proximity, is a factor, ease of accessibility, layout and geographic contour, of an attacked facility is also important, if not more so.
Individual
Glen Sutton
ATCO Electric
Yes
No Comment.
Yes
Although the FERC order contains language that a third party verification occur, this type of verification is not used anywhere else in NERC reliability standards for similar activities (e.g. CIP-002 classification). ATCO Electric (AET)respectfully requests that the review be allowed to be performed by qualified in-house Engineering groups who already perform these functions. Mandating a third party verification presents a risk to timelines and the implementation of the other requirements.
Yes
AET agrees with the flexible approach outlined by the draft standard and respectfully offers these following comment for the drafting team’s consideration: R4 – Please consider altering the wording of the final sentence of R4 to “The evaluation shall consider, at a minimum, the following:”. This allows additional flexibility for entities with existing physical security assessment programs to continue to include those extra elements within their plans. R5 – For the timeframe dependency please consider altering the dependent requirement to R4 instead of R2. Within the rationale section the drafting team concedes that R4 must be completed prior to commencing R5 and the drafting team also states that R4 does not state when the evaluation must occur, only that it must occur in time to meet R5. AET respectfully suggests

that a linear progression be established just as in R1, R2, and R3. This would require a timeline be added to R4 for the completion of the physical security risk assessment (AET suggests 120 calendar days from the completion of R2). AET also respectfully suggests that R5 then be made dependent on the completion of R4 (AET suggest 120 calendar days from the completion of R4). R6 – Please consider the removal of the required certifications in R6.1.1. The FERC order specifies that the risk assessment be reviewed by "[…] or another entity with appropriate expertise" and does not specify any particular qualifications. In addition, no other CIP standard calls for specific certifications or qualifications. Neither engineering focused requirements (e.g. CIP-002) or cyber security focused requirements (e.g. CIP-003, 005, 007) specify that those requirements be reviewed or implemented by designated engineers or certified security practitioners (e.g. CISSP). The due diligence required of the entity will determine the level of rigor that that entity is comfortable with defending and should not be included in the standard.
No
Individual
Richard Vine
California ISO
Agree
ISO/RTO Standards Review Committee
Individual
Mauricio Guardado
Los Angeles Department of Water and Power (LADWP)
Yes
LADWP requests the Drafting Team to make the following changes: - For Secion 4, you may want to add Transmission Planner and Planning Coordinator to the applicability. These functions may have responsibility on at least R1 and R2. - Secion 4.1.1.1 – Add "(AC or DC)" as follows: "Transmission Facilities operated at 500 kV (AC or DC) or higher….."
No
LADWP requests the Drafting Team to make the following changes: - For R1, additional time is needed to make sure studies are fully completed and reviewed by TO and its applicable governing authorities. Add ", which is due 30 calendar days after the effective date of the standard" to R1 as follows: "R1. Each Transmission Owner shall perform an initial risk assessment, which is due 30 calendar days after the effective date of the standard and subsequent risk assessments of its Transmission stations and Transmission substations (existing and……" - For R1, change "24 months" to " 30 months" to align the assessment with subsequent risk assessments. - For R2.1, The term "unaffiliated" needs to be defined in the standard to avoid any misinterpretation. - For R2.2, change the "90 calendar days" to "120 calendar days" to allow sufficient time to resolve differences if Planning Coordinator, Transmission Planner or Reliability Coordinator are addressing other deadlines.

No
LADWP requests the Drafting Team to make the following changes: - For R5, replace the word “implement” with “complete” to avoid confusion as to whether the plan needs to be implemented within the timeline provided - For R5.1, the word “Resiliency” needs to be defined in the standard to avoid any misinterpretation. Resiliency means different things to different people - For R5.1, add the language “, mitigate the impacts of,” to the requirement as follows: “5.1. Resiliency or security measures designed to deter, detect, delay, assess, communicate, mitigate the impacts of, and respond…..” - For R5.4, change the requirement language to read as follows: “5.4. Provisions to evaluate evolving physical threats to the Transmission station(s), Transmission substation(s), or primary control center(s), and their corresponding security counter measures. “ This sub-requirement should allow for the TO to revise its already-reviewed security plan within the 30-month cycle without necessarily having to make arrangements for a third party review of the revised plan (although it may do so if TO so desires) and without creating an additional 30-month cycle review that the normal course – this is a matter of efficiency and due diligence to address evolving threats - For 6.1, as previously mentioned, the word “unaffiliated” needs to be defined in the standard to avoid any misinterpretation. - For 6.1.3, change the requirement as follows: “6.1.3. A governmental agency with physical security expertise, which could be a City Department in which the utility resides that requires a review to be performed.” This clarification allows for additional flexibility of independent governmental agencies reviews. - For 6.1.4, change the requirement as follows: “6.1.4. An entity or organization with demonstrated law enforcement, government, or military physical security expertise, such as the local police department in which the utility resides that requires a review to be performed.” This clarification allows for additional flexibility of independent entities or organizations reviews - For R6, add 6.1.5 with the following language: “6.1.5. A peer utility review group with demonstrated law enforcement, government, or military physical security expertise This clarification allows for additional flexibility of other Planning Coordinator, Transmission Planner or Reliability Coordinator review the work of their peers. In the alternative, expand to include Planning Coordinator, Transmission Planner or Reliability Coordinator with law enforcement, government, or military physical security expertise. - For 6.2, change the “90 calendar days” to “120 calendar days” to provide sufficient time to determine reasonable and sound recommendations. - For 6.3, chance the “90 calendar days” to “120 calendar days” to provide sufficient time to address any modifications recommended.
No
Individual
Laurie Williams
PNM Resources
EEI
No

R2.1 puts an unreasonable burden on registered PC and TP. R2.2 which puts the burden of ensuring that the unaffiliated third party review is completed in 90 calendar days on the TO. As a TO PNM can't force another registered entity or third party to complete anything with a specified amount of time and according to the RSAW if the verification is not completed within 90 days then the TO is not in compliance with the requirement. The standard should require registered NERC entities to complete the unaffiliated review and those entities should be included as applicable functional entities and R2.2 should apply to the reviewing entity.
Group
Associated Electric Cooperative, Inc.- JRO00088
David Dockery
Agree
NRECA
Individual
Richard Vine
California ISO
Yes
Yes
We agree with the approach identified in R1 through R3, however we have the following comments regarding the SCOPE of the verification review required by R2.2: • The scope of the 3rd party verification is not well defined. What is the expectation and scope of the verification review? What level of quality is expected/required? Is the Transmission Owner responsible for scoping the verification process to ensure the review meets the required level of review? • Very little guidance is provided on the scope of the review. The scope of the review and verification work would need to be well understood before taking this verification work on. Is a technical analysis required as part of the review and verification process on the part of the 3rd party verifying the Transmission Owner's risk assessment and list of critical facilities, or is it simply to review the risk assessment and list of critical facilities that the Transmission Owner has provided to the 3rd party reviewer, based on their current knowledge of the transmission system from performing prior transmission planning studies? Will NERC be providing additional guidance regarding the scope of work required for verification by a 3rd party?
Yes
No
Group

Cooper Compliance Corp
Mary Jo Cooper
Yes
We support the applicability proposed by CIP-014-1.
No
We do not support the Standard as written today. We agree with the scope and content of the SAR. However, we are concerned with Requirement 6. Requirement 6 requires entities to seek out third parties to review their new physical security protection plans. We don't believe that entities should be obligated to seek assistance from third party individuals. This includes consultants or another unassociated entity. The purpose of the regions, NERC, and FERC are to provide a review of an entities compliance to Standards through the audit and self-certification process. No other Reliability Standards require an entity to use third parties to determine compliance or sufficiency of compliance documentation. We believe that this obligation may place some entities in difficult financial situation and could have a negative impacts in assuring that proper third party entities are being used. Should FERC, NERC, or WECC determine that entities are not following the spirit of the Standard than they may request a modification in a future Standard revision. We will support this Standard if Requirement 6 is removed.
No
We do not support the Standard for the same reason above. We do not support a third party review requirement other than that of the existing Standards. That is a review by FERC, NERC or the appropriate region.
Yes
We would like to address proposed comments by APPA that additional Standards are added to address confidentiality. We do not agree with APPA's position. The functional model requires registered functions to work together to secure reliability. Already, as a result of CIP Standards, vital communications between the Distribution Providers/Load Serving Entities and the Balancing Authorities and/or Transmission Operators have been compromised. Often, The Balancing Authorities and Transmission Operators are in fear of sharing important information with the Distribution Providers and/or Load Serving Entities because they feel they could be subject to a CIP violation. In some cases the Distribution Providers and Transmission Operators even share facilities. Having a requirement that prevents sharing vital information on physical security would simply not work and therefore we do not support APPA's comments.
Individual
Michael Mertz
PNM Resources
Yes
Support the comments submitted by EEI.

No
R2.1 could place an unreasonable burden on entities registered as PC and TP. R2.2 which puts the burden of ensuring that the unaffiliated third party review is completed in 90 calendar days on the TO. As a TO an entity cannot compel another registered entity or third party to complete anything with a specified amount of time and according to the RSAW if the verification is not completed within 90 days then the TO is not in compliance with the requirement. The standard should require registered NERC entities to complete the unaffiliated review and those entities should be included as applicable functional entities and R2.2 should apply to the reviewing entity.
Yes
Support the comments submitted by EEI
Yes
Support the comments submitted by EEI
Individual
Jeffrey Fuller
Dayton Power & Light
Agree
Dayton Power & Light

Comments Received from Herb Schrayshuen

Question 1 – Response: No

Comments: The applicability of the standard is to Transmission Owners and Transmission Operators. Generating plants sites where the facilities production capability exceeds 1000 MW or other suitably larger amount should be included.

Question 2 – Response: No

Comments: In Requirement R1 the use of the term ‘transmission analysis’ and ‘transmission analyses’ in order to identify which substations should have a security plan is vague The TPL standards extreme cases should be used to clearly describe the specific required elements of the analysis. Failure to specify how the analysis is to be done will lead to inconsistencies in the analysis and thereby difficulty for audits of the standard.

In Requirement R2 the use of the word ‘unaffiliated’ introduces ambiguity. There needs to be an understanding (through the standard but if not feasible through RSAW or other tool-e.g. guideline) what “unaffiliated” means.

The term "unaffiliated" is not required because the NERC Reliability Functional model already ensures the independence between the TO/TOP and the verifying entities.

Question 4 – Response: Yes

Comments: The Implementation Plan can be read that it obligates applicable entities to complete the initial risk assessment in Requirement R1, on or before the effective date of the standard. The implementation plan should be adjusted.

The following is a suggestion to facilitate reading of the standard and stay whitn defined terms without introfucing new terms which are undefined: For all requirements: Replace the expression "Transmission stations and Transmission substations" with "Transmission facilities". Otherwise, please explain why such a distinction is necessary.

While the requirement for unaffiliated third party verification of the physical security plan is something required by the FERC in its order, the mandate is misguided and will lead to security breaches while at the same time adding no incremental value to the physical security plan. The utility, which owns the assets, is already highly incentivized to put together a good security plan to avoid loss of its facilities to terrorism without third party verification. The utility may decide to use security consultants to help develop the plan if it involves new, state of the art physical security topics outside the utilities experience base. On balance the third party verification requirement outlined in R6 regarding the physical security plan is unneeded.

Additional comment received from Marcus Pelt, Southern Company

"The wording of Requirement R2.s, as it stands currently, could be interpreted to place requirements on the unaffiliated third party verifier when the responsible entity is actually the Transmission Owner. Southern recommends that R2.2 be reworded as follows to address this concern:

Proposed R2.2
2.2 The responsible Transmission Owner shall ensure the unaffiliated third party verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment. The unaffiliated third party verification may, but is not required to, include recommended additions or deletions of Transmission station(s) or Transmission substation(s)."

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project 2014-04 Physical Security

The Project 2014-04 Physical Security Standard Drafting Team (SDT) thanks all commenters who submitted comments on the CIP-014-1 standard. The standard was posted for a 15-day formal comment period from April 10-24, 2014. Stakeholders were asked to provide feedback on the standard and associated documents through a special electronic comment form. There were 136 sets of responses, including comments from approximately 240 different people from approximately 165 companies representing all 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the project page.

Summary Consideration:

The SDT has reviewed all comments and made the following non-substantive changes to the standard to incorporate stakeholder recommendations:

- Part 4.1.1 is modified:

  4.1.1 Transmission Owner that owns ~~any of the following~~ **a Transmission station or Transmission substation that meets any of the following criteria**:

- The applicability exemption contained Section 4 is modified:

  Exemption: Facilities **in a "protected area," as defined in 10 C.F.R. § 73.2,** within the scope of a security plan approved **or accepted** by the Nuclear Regulatory Commission **are not subject to this Standard;** or**, Facilities within the scope of a security plan approved by** the Canadian Nuclear Safety Commission are not subject to this Standard.

- Requirement R1 is modified:

  R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify ~~any~~ **the** Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

- Measure M1 is modified:

  M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission

substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. **Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.**

- Requirement R2 Part 2.2 is modified:

2.2 The unaffiliated ~~verifying entity~~ **third party verification** shall ~~either~~ verify the Transmission Owner's risk assessment performed under Requirement R1**,** ~~or recommend~~ **which may include recommendations** for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

- Requirement R2 Part 2.4 is modified:

2.4 Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged with~~ **made available to** the unaffiliated **third party verifier** ~~verifying entity~~ **and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.**

- Measure M2 is modified:

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. **Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.**

- Requirement R3 is modified:

R3. For a primary control center(s) **of a Transmission station or Transmission substation** identified ~~by a transmission owner~~ according to Requirement R1**, Part 1.2 that a) operationally controls an identified Transmission Station or Transmission substation** ~~and~~ verified according to Requirement R2, **and b)** ~~that~~ is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

- Measure M3 is modified:

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic **notifications or** communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

- Requirement R4 is modified:

R4. Each Transmission Owner that ~~owns or operates~~ **identified** a Transmission station, Transmission substation, or **a** primary control center ~~identified~~ in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

- Requirement R4 Part 4.2 is modified:

4.2 Prior history ~~or~~ **of** attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

- Requirement R4 Part 4.3 is modified:

4.3 Intelligence or threat warnings **received** from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

- Requirement R5 is modified:

R5. Each Transmission Owner that ~~owns or has operational control of~~ **identified** a Transmission station, Transmission substation, or primary control center ~~identified~~ in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). **The physical security plan(s) shall be developed** within 120 calendar days following the completion of Requirement R2 **and executed according to the timeline specified in the physical security plan(s)**. The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

- Requirement R5 Part 5.1 is modified:

5.1 Resiliency or security measures designed **collectively** to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on the results~~ of **identified during** the evaluation conducted in Requirement R4.

- Requirement R5 Part 5.3 is modified:

5.3 A timeline for ~~implementing~~ **executing** the physical security enhancements and modifications specified in the physical security plan.

- Measure M5 is modified:

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating ~~implementation~~ **execution** of the physical security plan **according to the timeline specified in the physical security plan.**

- Requirement R6 is modified:

R6. Each Transmission Owner that ~~owns or operates~~ **identified** a Transmission station, Transmission substation, or primary control center ~~identified~~ in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

- Requirement R6 Part 6.1 is modified:

6.1 Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- ~~6.1.1~~ An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
- ~~6.1.2~~ An entity or organization approved by the ERO.
- ~~6.1.3~~ A governmental agency with physical security expertise.

- ~~6.1.4~~ An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

- Requirement R6 Part6.3 is modified:

  6.3 If the unaffiliated **third party** ~~reviewing entity~~ **reviewer** recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Requirement R6 Part6.4 is modified:

  6.4 Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged with~~ **made available to** the unaffiliated reviewing entity **and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure**.

- Measure M6 is modified:

  M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. **Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.**

A summary response to each comment follows each question. Please note that because common issues were grouped together in the summaries, an individual's comment may have been addressed in the summary for a question that is different from the question in which they submitted the comment; the SDT encourages reviewers to read all summary responses.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

Index to Questions, Comments, and Responses

1. Applicability: The applicability of proposed CIP-014-1 starts with those Transmission Owners that own Transmission facilities that meet the bright line criteria in Reliability Standard CIP-002-5.1 for a "medium impact" rating. The drafting team did not modify these criteria in their use under CIP-014-1, as they have been previously approved by stakeholders, NERC, and FERC. The SDT sought to ensure that entities could apply the same set of criteria to assist with identification of facilities under CIP Version 5 and proposed CIP-014-1. The team determined that slightly modified criteria could possibly result in confusion in application. The drafting team considered several other alternatives to refine the scoping in the applicability section, such as a particular kV threshold in addition to the other criteria; however, after significant discussion, the team found no technical or reliability basis for providing such limitiation. Importantly, by virtue of application of Requirement R1, the scope of the standard only applies to Transmission Owners that have Transmission stations and Transmission substations that meet the "medium impact" criteria from CIP-002-5.1, and their associated primary control centers. Furthermore, the standard drafting team expects many who are "applicable" to the standard will not identify facilities through their Requirement R1 risk assessment and Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. In those cases, the entity only performs Requirements R1 through R2. When that results in a null set, Requirement R1 additionally provides that subsequent risk assessments may occur less frequently. Similarly, while Transmission Operators are also listed in the applicability section, by virtue of application of the requirements, only certain Transmission Operators that are notified under the standard's Requirement R3 have obligations under the standard. Do you agree with the applicability section? If not, please provide specific recommendations, ensuring to articulate how your suggested approach would not limit the applicability in such a manner as to inadvertently miss a facility that should be covered under the standard as specified in the FERC order on physical security. 27

2. Requirements R1 through R3: The first three requirements of CIP-014-1 require Transmission Owners to: (1) perform risk assessments to identify through transmission planning analysis those Transmission stations and Transmission substations that meet the "medium impact" criteria from CIP-002-5.1, and their associated primary control centers, that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; (2) arrange for a third party verification (as directed in the order) of the identifications; and (3) notify certain Transmission Operators of identified primary control centers that operationally control the identified and verified Transmission stations and Transmission substations. The requirements provide the periodicity for satisfying these obligations. Only an

entity that owns or operates one or more of the identified facilities has further obligations in Requirements R4 through R6. If an entity identifies a null set after applying Requirements R1 through R2, the rest of the standard does not apply. Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security. 60

3. Requirements R4 through R6: The final three requirements of CIP-014-1 require (1) the evaluation of potential threats and vulnerabilities of a physical attack to the facilities identified and verified according to the earlier requirements, (2) the development and implementation of a security plan(s) designed in response to the evaluation, and (3) a third party review of the evaluation and security plan(s) (as directed in the order). Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security. 111

4. Do you have input on other areas of the standard or implementation plan not discussed in the questions above? If so, please provide them here, recognizing that you do not have to provide a response to all questions. Please limit your response to 300 words or less. 152

The Industry Segments are:

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

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Ben Engelby	ACES Standards Collaborators	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Shaver	Arizona Electric Power Cooperative/Southwest Transmission Cooperative, Inc.	WECC	1, 4, 5
2.	Shari Heino	Brazos Electric Power Cooperative, Inc.	ERCOT	1, 5
3.	Kevin Lyons	Central Iowa Power Cooperative	MRO	
4.	Amber Skillern	East Kentucky Power Cooperative	SERC	1, 3, 5
5.	Michael Brytowski	Great River Energy	MRO	1, 3, 5, 6
6.	Chip Koloini	Golden Spread Electric Cooperative, Inc.	SPP	5
7.	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	RFC	1

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

8.	Scott Brame	North Carolina Electric Membership Corporation	SERC	1, 3, 4, 5
9.	Mark Ringhausen	Old Dominion Electric Cooperative	SERC	3, 4
10.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
11.	Dave Viar	Southern Maryland Electric Cooperative	RFC	3
12.	Ellen Watkins	Sunflower Electric Power Corporation	SPP	1
13.	Susan Sosbe	Wabash Valley Power Association	SERC	3

2.	Group	Paul Haase	APPA	X				X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Michael Shaw	LCAR	ERCOT	6
2.	Dixie Wells	LCRA	ERCOT	5
3.	Martyn Turner	LCRA	ERCOT	1

3.	Group	David Dockery	Associated Electric Cooperative, Inc.-JRO00088	X		X		X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3
3.	M & A Electric Power Cooperative		SERC	1, 3
4.	Northeast Missouri Electric Power Cooperative		SERC	1, 3
5.	N.W. Electric Power Cooperative, Inc.		SERC	1, 3
6.	Sho-Me Power Electric Cooperative		SERC	1, 3

4.	Group	Bob Case - NERC Compliance Manager , Bob.Case@blackhillscorp.com	Black Hills Corporation Entities	X		X	X	X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	NCR05030	Black Hills Power	WECC	1, 3, 4
2.	NCR05031	Black Hills Wyoming	WECC	5, 6
3.	NCR00089	Black Hills Colorado Electric	WECC	1, 3, 4
4.	NCR11186	Black Hills Colorado IPP	WECC	5, 6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
5.	Group	Andrea Jessup	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jeff Millennor	Physical Security	WECC	1
2.	Richard Becker	Substation Engineering	WECC	1
3.	Jim Burns	Technical Operations	WECC	1
4.	Kyle Kohne	Transmission Planning	WECC	1

6.	Group	Raymond G. Fugere	California Public Utilities Commission: Safety and Enforcenment Division									X	

	Additional Member	Additional Organization	Region	Segment Selection
1.	Benjamin Brinkman	California Public Utilities Commission: Safety and Enforcenment Division	WECC	9

7.	Group	Peter Yost	Con Edison and Orange & Rockland	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Edward Bedder	ORU	NPCC	1, 3

8.	Group	Mary Jo Cooper	Cooper Compliance Corp	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Draeger	Alameda Municipal Power		3
2.	Fred Fletcher	Burbank Water and Power		3
3.	Blain Ladd	California Pacific Electric Co.		3
4.	Mel Grandi	City of Ukiah		3
5.	Angela Kimmey	Pasadena Water and Power		1, 3
6.	Ken Dize	Salmon River Electric Coop		3

9.	Group	Connie Lowe	Dominion	X		X		X	X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Randi Heise	NERC Compliance Policy	MRO	5
2.	Mike Garton	NERC Compliance Policy	NPCC	5, 6

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

3.	Louis Slade	NERC Compliance Policy	RFC	
4.	John Loftis	Electric Transmission Compliance	SERC	1, 3, 5, 6
5.	Candace Marshall	Electric Transmission Compliance	SERC	1, 3, 5, 6
6.	Larry Nash	Electric Transmission Compliance	SERC	1, 3, 5, 6

10.	Group	Michael Lowman	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils		RFC	1
2.	Lee Schuster		FRCC	3
3.	Dale Goodwine		SERC	5
4.	Greg Cecil		RFC	6

11.	Group	Joe Tarantino	ERTF	X				X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Martyn Turner	LCRA	ERCOT	1
2.	Dixie	Wells	ERCOT	5

12.	Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bill Smith	FE	RFC	1
2.	Cindy Stewart	FE	RFC	3
3.	Doug Hohlbaugh	FE	RFC	4
4.	Ken Dresner	FE	RFC	5
5.	Kevin Querry	FE	RFC	6

13.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tim Beyrle	City of New Smyrna Beach	FRCC	4
2.	Jim Howard	Lakeland Electric	FRCC	3
3.	Greg Woessner	Kissimmee Utility Authority	FRCC	3
4.	Lynne Mila	City of Clewiston	FRCC	3
5.	Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Randy Hahn	Ocala Utility Services	FRCC 3										
7.	Stanley Rzad	Keys Energy Services	FRCC 1										
8.	Don Cuevas	Beaches Energy Services	FRCC 1										
9.	Mark Schultz	City of Green Cove Springs	FRCC 3										
14.	Group	Greg Campoli	ISO/RTO Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Ali Miremadi	CAISO	WECC	2
2.	Cheryl Moseley	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Matthew Goldberg	ISONE	NPCC	2
5.	Terry Bilke	MISO	RFC	2
6.	Stephanie Monzon	PJM	RFC	2
7.	Charles Yeung	SPP	SPP	2

15.	Group	Tom McElhinney	JEA	X		X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Ted Hobson		FRCC	1
2.	Garry Baker		FRCC	3
3.	John Babik		FRCC	5

16.	Group	Michael Jones	National Grid	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brian Shanahan	National Grid	NPCC	3

17.	Group	Steve Hill	NCPA Compliance Management Operating Committee				X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tracy Bibb	NCPA	WECC	4
2.	Scott Tomashefsky	NCPA	WECC	NA
3.	Hari Modi	NCPA	WECC	5

18.	Group	Brent Ingebrigtson	PPL NERC Registered Affiliates	X		X		X	X				

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

	Additional Member	Additional Organization	Region	Segment Selection
1.	Charlie Freibert	Louisville Gas and Electric Company and Kentucky Utilities Company	SERC	3
2.	Brenda Truhe	PPL Electric Utilties Corporation	RFC	1
3.	Annette Bannon	PPL Generation, LLC	RFC	5
4.		PPL Susquehana, LLC	RFC	5
5.		PPL Montana, LLC	WECC	5
6.	Elizabeth Davis	PPL EnergyPlus, LLC	MRO	6
7.			NPCC	6
8.			RFC	6
9.			SERC	6
10.			SPP	6
11.			WECC	6

19.	Group	Paul Haase	Seattle City Light	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Pawel Krupa	Seattle City Light	WECC	1
2.	Dana Wheelock	Seattle City Light	WECC	3
3.	Hao Li	Seattle City Light	WECC	4
4.	Mike Haynes	Seattle City Light	WECC	5
5.	Dennis Sismaet	Seattle City Light	WECC	6

20.	Group	Cynthia Hill-Watson	SERC CIPC	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Cynthia Hill-Watson	TVA	SERC	1, 3, 5, 6
2.	Jack Paul	TVA	SERC	1, 3, 5, 6
3.	Tony Hall	LGE-KU	SERC	1, 3, 5, 6
4.	Neil Phinney	GSOC	SERC	3, 4
5.	Mike Stanley	MEAG	SERC	1, 3, 5

21.	Group	Robert Rhodes	SPP Standards Review Group	X	X	X		X	X				

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

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mo Awad	Westar Energy	SPP	1, 3, 5, 6
2.	Sandie Bayless	Westar Energy	SPP	1, 3, 5, 6
3.	Derek Brown	Westar Energy	SPP	1, 3, 5, 6
4.	Phil Clark	Grand River Dam Authority	SPP	1
5.	Louis Guidry	Cleco Power	SPP	1, 3, 5, 6
6.	Shannon Mickens	Southwest Power Pool	SPP	2
7.	James Nail	City of Independence, MO	SPP	3
8.	Jerald Nottnagel	Oklahoma Gas & Electric	SPP	1, 3, 5
9.	Terri Pyle	Oklahoma Gas & Electric	SPP	1, 3, 5
10.	Valerie Sesler	Westar Energy	SPP	1, 3, 5, 6
11.	Megan Wagner	Westar Energy	SPP	1, 3, 5, 6
12.	Ellen Watkins	Sunflower Electric Power Corporation	SPP	1

22.	Group	Ronald L Donahey	Tampa Electric Company	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sara E Young	Tampa Electric Company	FRCC	1
2.	James Rocha	Tampa Electric Company	FRCC	5
3.	Benjamin Smith	Tampa Electric Company	FRCC	6
4.	Ronald L Donahey	Tampa Electric Company	FRCC	3

23.	Group	Brian Millard	Tennessee Valley Authority	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	DeWayne Scott		SERC	1
2.	Ian Grant		SERC	3
3.	David Thompson		SERC	5
4.	Marjorie Parsons		SERC	6

24.	Group	Lloyd A. Linke	Western Area Power Administration	X					X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Western Area Power Administraton	Upper Great Plains Region	MRO	1, 6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
2. Western Area Power Administraton			Rocky Mountain Region WECC 1, 6										
3. Western Area Power Administraton			Desert Southwest Region WECC 1, 6										
4. Western Area Power Administraton			Colorado River Storage Project WECC 6										
5. Western Area Power Administraton			Sierra Nevada Region WECC 1, 6										
25.	Individual	David Jendras	Ameren	X		X		X	X				
26.	Individual	Thomas Foltz	American Electric Power	X		X		X	X				
27.	Individual	Allen Mosher	American Public Power Association (APPA)	X		X	X	X	X				
28.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
29.	Individual	Joe Tarantino	APPA	X		X	X	X	X				
30.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				
31.	Individual	Glen Sutton	ATCO Electric	X									
32.	Individual	David Rudolph	Basin Electric Power Cooperative (BEPC)	X		X		X					
33.	Individual	Erika Doot	Bureau of Reclamation	X				X					
34.	Individual	Richard Vine	California ISO		X								
35.	Individual	Richard Vine	California ISO		X								
36.	Individual	Raymond Fugere	California Public Utilities Commission: Safety and Enforcenment Division									X	
37.	Individual	Frank Pace	Central Hudson Gas & Electric Corporation	X									
38.	Individual	Kevin Lyons	Central Iowa Power Cooperative	X		X							
39.	Individual	Chad Bowman	CHPD	X									
40.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
41.	Individual	Ronnie C. Hoeinghaus	City of Garland	X		X							
42.	Individual	Bill fowler	City of Tallahassee			X							
43.	Individual	Scott Langston	City of Tallahassee	XX									
44.	Individual	John Allen	City Utilities of Springfield, Missouri										
45.	Individual	David Grubbs	Ciy of Garland	X		X		X	X				
46.	Individual	Jack Stamper	Clark Public Utilities	X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
47.	Individual	Shannon Fair	Colorado Springs Utilities	X		X		X	X				
48.	Individual	Robert Trowbridge	Consumers Energy Company			X		X					
49.	Individual	David Kiguel	David Kiguel								X		
50.	Individual	David Dworzak	Edison Electric Institute	X									
51.	Individual	Earl F. Cass	EF Cass Consulting Inc.								X		
52.	Individual	Mike Kidwell	Empire District Electric Company					X					
53.	Individual	Steve Hamburg	Encari	X									
54.	Individual	Dean Ahlsten	Eugene Water & Electric Board				X						
55.	Individual	Chris Scanlon	Exelon	X		X	X	X	X				
56.	Individual	Linda Jacobson-Quinn	FEUS			X							
57.	Individual	Russ Schneider	Flathead Electric Cooperative, Inc.			X	X						
58.	Individual	Dennis Minton	Florida Keys Electric Cooperative	X									
59.	Individual	Curtis Klashinsky	FortisBC	X									
60.	Individual	William R. Harris	Foundation for Resilient Societies								X		
61.	Individual	Guy Andrews	Georgia System Operations Corporation			X	X						
62.	Individual	David Revill	Georgia Transmission Corporation	X									
63.	Individual	Ladeene Freimuth	GridWise Alliance	X	X	X	X	X					
64.	Individual	Ayesha Sabouba	Hydro One	X		X							
65.	Individual	Chantal Mazza	Hydro QuÃ©bec TransÃ‰nergie	X									
66.	Individual	Mike Marshall	Idaho Power Co.	X									
67.	Individual	Bob Thomas and Kevin Wagner	Illinois Municipal Electric Agency				X						
68.	Individual	Mark Wilson	Independent Electricity System Operator		X								
69.	Individual	John Falsey	Invenergy LLC					X					
70.	Individual	Michael P Moltane	ITC	X									
71.	Individual	Brett Holland	Kansas City Power & Light	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
72.	Individual	Larry Watt	Lakeland Electric	X									
73.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
74.	Individual	Mauricio Guardado	Los Angeles Department of Water and Power (LADWP)	X		X		X	X				
75.	Individual	Dixie Wells	Lower Colorado River Authority					X					
76.	Individual	Donald E Nelson	MA Dept. of Public Utilities									X	
77.	Individual	Shirley Mayadewi	Manitoba Hydro	X		X		X	X				
78.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric Company					X					
79.	Individual	Gary Kruempel	MidAmerican Energy Holding Company	X		X		X	X				
80.	Individual	Randi Nyholm	Minnesota Power	X									
81.	Individual	Dan Inman	Minnkota Power Cooperative	X									
82.	Individual	David Francis	MISO		X								
83.	Individual	Nick Braden	Modesto Irrigation District			X	X		X				
84.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)				X						
85.	Individual	Tony Eddleman	Nebraska Public Power District	X		X		X					
86.	Individual	Alan MacNaughton	New Brunswick Power Corporation	X									
87.	Individual	Wayne Sipperly	New York Power Authority	X		X		X	X				
88.	Individual	Bruce Metruck	New York Power Authority	X									
89.	Individual	Joe O'Brien	NIPSCO	X		X		X	X				
90.	Individual	Terry Volkmann	None	X									
91.	Individual	Guy Zito	Northeast Power Coordinating Council										X
92.	Individual	William Temple	Northeast Utilities	X									
93.	Individual	John Canavan	NorthWestern Energy	X									
94.	Individual	Alan Johnson	NRG Energy, Inc.			X	X	X	X				
95.	Individual	Venona Greaff	Occidental Chemical Corporation							X			

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
96.	Individual	Bernard Johnson	Oglethorpe Power Corporation					X	X				
97.	Individual	Donna Johnson	Oglethorpe Power Corporation						X				
98.	Individual	Mahmood Safi	Omaha Public Power District	X		X		X	X				
99.	Individual	David Ramkalawan	OPG					X					
100.	Individual	John Hagen	Pacific Gas and Electric Company	X		X		X					
101.	Individual	Jared Shakespeare	Peak Reliability	X									
102.	Individual	David Thorne	Pepco Holdings Inc.	X		X							
103.	Individual	Laurie Williams	PNM Resources	X		X							
104.	Individual	Michael Mertz	PNM Resources			X							
105.	Individual	Debra Horvath	Portland General Electric	X		X		X	X				
106.	Individual	Steven Wickel	Public Utility District No. 1 of Chelan County	X		X		X	X			X	
107.	Individual	John Yale	Public Utility District No. 1 of Chelan County	X		X		X	X			X	
108.	Individual	Hugh Owen	Public Utility District No. 1 of Chelan County						X				
109.	Individual	Michiko Sell	Public Utility District No. 2 of Grant County, WA	X		X		X	X			X	
110.	Individual	Kenn Backholm	Public Utility District No.1 of Snohomish County	X		X	X	X	X			X	
111.	Individual	Russell Noble	Public Utitliy District No. 1 of Cowlitz County, WA			X	X	X					
112.	Individual	Greg Froehling	Rayburn Country Electric Cooperative			X							
113.	Individual	Anthony Jablonski	ReliabilityFirst										X
114.	Individual	Joshua Andersen	Salt River Project	X		X		X	X				
115.	Individual	Jennifer Wright	San Diego Gas & Electric	X		X		X					
116.	Individual	Debra Warner	self								X		
117.	Individual	Michael Haff	Seminole Electric Cooperative, Inc.	X		X	X	X	X				
118.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				
119.	Individual	Patrick Farrell	Southern California Edison Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
120.	Individual	Marcus Pelt	Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	X		X		X	X				
121.	Individual	Lynnae Wilson	Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.	X		X		X	X				
122.	Individual	Bob Reynolsa	Southwest Power Pool Regional Entity										X
123.	Individual	David Godfrey	Texas Municipal Power Agency					X					
124.	Individual	Derrick Davis	Texas RE										X
125.	Individual	Ralph Meyer	The Empire District Electric Company	X									
126.	Individual	Kalem Long	The Empire District Electric Company			X							
127.	Individual	Eric Olson	Transmission Agency of Northern California	X									
128.	Individual	Sergio Banuelos	Tri-State Generation and Transmission Association, Inc.	X		X		X					
129.	Individual	Melissa Kurtz	US Army Corps of Engineers					X					
130.	Individual	Brian Evans-Mongeon	Utility Services				X						
131.	Individual	kim moulton	Vermont Transco LLC	X									
132.	Individual	William H. Chambliss, member Operating Committee	Virginia State Corporation Commission										
133.	Individual	Candace Morakinyo	We Energies			X	X	X	X				
134.	Individual	Megan Wagner	Westar Energy	X		X							
135.	Individual	Steve Rueckert	Western Electricity Coordinating Council										X
136.	Individual	Amy Casuscelli	Xcel Energy	X		X		X	X				

If you support the comments submitted by another entity and would like to indicate you agree with their comments, please select "agree" below and enter the entity's name in the comment section (please provide the name of the organization, trade association, group, or committee, rather than the name of the individual submitter).

Organization	Agree	Supporting Comments of "Entity Name"
Central Iowa Power Cooperative	Agree	ACES
MA Dept. of Public Utilities	Agree	Agree with the comments made by NPCC.
Massachusetts Municipal Wholesale Electric Company	Agree	American Public Power Association
Transmission Agency of Northern California	Agree	American Public Power Association
Eugene Water & Electric Board	Agree	American Public Power Association (APPA)
City of Austin dba Austin Energy	Agree	American Public Power Association (APPA). In addition, Austin Energy states the following:The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this Standard may be subject to disclosure under state open records laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard designating the produced, gathered, used and maintained records related to compliance with

Organization	Agree	Supporting Comments of "Entity Name"
		this Standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure.
JEA	Agree	APPA
City of Tallahassee	Agree	APPA
City of Tallahassee	Agree	APPA
City Utilities of Springfield, Missouri	Agree	APPA
New York Power Authority	Agree	APPA
New York Power Authority	Agree	APPA
Public Utility District No. 1 of Chelan County	Agree	APPA and LPPC comments
FEUS	Agree	APPAWECC
NorthWestern Energy	Agree	Arizona Public Service, Bureau of Reclamation, Portland General Electric, WECC
California Public Utilities Commission: Safety and Enforcenment Division	Agree	California Public Utilities CommissionSafety and Enforcenment Division
CHPD	Agree	CHPD is supportive of the comments submitted by APPA
Texas Municipal Power Agency	Agree	City of Garland and American Public Power Assocation

Organization	Agree	Supporting Comments of "Entity Name"
We Energies	Agree	Edison Electric Institute (EEI)
Lakeland Electric	Agree	Florida Municipal Power Agency (FMPA)
Illinois Municipal Electric Agency	Agree	Florida Municipal Power AgencyAmerican Public Power Association
Oglethorpe Power Corporation	Agree	Georgia Transmission Corporation (GTC)National Rural Electric Cooperative Association (NRECA)
Oglethorpe Power Corporation	Agree	Georgia Transmission Corporation (GTC)National Rural Electric Cooperative Association (NRECA)
Occidental Chemical Corporation	Agree	Ingleside Cogeneration, LP
California ISO	Agree	ISO/RTO Standards Review Committee
Lower Colorado River Authority	Agree	Lower Colorado River Authority
Public Utility District No. 1 of Chelan County	Agree	LPPC and APPA
Public Utility District No. 1 of Chelan County	Agree	LPPC and APPA
Invenergy LLC	Agree	NPCC
Associated Electric Cooperative, Inc.- JRO00088	Agree	NRECA

Organization	Agree	Supporting Comments of "Entity Name"
Public Utility District No.1 of Snohomish County	Agree	Salt River Project ("SRP")
ERTF	Agree	The following comments are in agreement with LPPC and ERTF as well as comment from our own entity LCRA: o Use of "primary control center" is ambiguous (R1.2 and others); o Unaffiliated third party review needs to be longer than 90-days, suggestion to be 180-days (R2.2); o Issue with non-disclosure agreement vs. Public Power's obligation to disclose information (R2.4); o Expansion of the Security Plan third-party reviewer to include those functions that are identified in Requirement 2.1 (R6.1). o The standard does not address substations/stations that are owned by multiple Transmission Owners. LCRA TSC recommends adding language describing NERC's expectations associated with jointly-owned substations/stations or substation/stations with multiple asset owners.
APPA	Agree	The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the Introduction Section: 7. Critical Facilities Information Records and related information concerning critical facilities, physical infrastructure,

Organization	Agree	Supporting Comments of "Entity Name"
		including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. Proposed Requirement Language (new subrequirements): R1 1.3 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under this standard. R3 3.4 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under Requirement R1 of this standard. R4 4.1 The Transmission Owner will keep confidential all records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1 conducted under this standard.
US Army Corps of Engineers	Agree	Western Area Power Administration

Organization	Agree	Supporting Comments of "Entity Name"
Public Utitliy District No. 1 of Cowlitz County, WA		American Public Power Association
APPA		American Public Power Association (APPA)
Colorado Springs Utilities		CSU agrees with APPA comments with exception to the confidentiality section, please see CSU's comments below.CONFIDENTIALITYPublicly Owned Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the A. Introduction section, after 6. Background:7. Critical Facilities InformationRecords and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted

Organization	Agree	Supporting Comments of "Entity Name"
		under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. ALTERNATIVE PROPOSED REQUIREMENT LANGUAGE ADDITIONS:R1.3 All records and information related to the risk assessments conducted of this standard are exempt from public disclosure.R3.2 All records and information related to the notifications conducted under Requirement R3 and R3.1 of this standard are exempt from public disclosure. R4.4 All records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1 of this standard are exempt from public disclosure.Adding confidential in the standard would create undo compliance burden and auditing challenges.
PNM Resources		EEI
Modesto Irrigation District		Modesto Irrigation District supports the comments submitted by American Public Power Association/Large Public Power Council
Seminole Electric Cooperative, Inc.		National Rural Electric Cooperative Association (NRECA)
Public Utility District No. 2 of Grant County, WA		Public Utility District No. 2 of Grant County, WA

1. **Applicability: The applicability of proposed CIP-014-1 starts with those Transmission Owners that own Transmission facilities that meet the bright line criteria in Reliability Standard CIP-002-5.1 for a "medium impact" rating. The drafting team did not modify these criteria in their use under CIP-014-1, as they have been previously approved by stakeholders, NERC, and FERC. The SDT sought to ensure that entities could apply the same set of criteria to assist with identification of facilities under CIP Version 5 and proposed CIP-014-1. The team determined that slightly modified criteria could possibly result in confusion in application. The drafting team considered several other alternatives to refine the scoping in the applicability section, such as a particular kV threshold in addition to the other criteria; however, after significant discussion, the team found no technical or reliability basis for providing such limitation. Importantly, by virtue of application of Requirement R1, the scope of the standard only applies to Transmission Owners that have Transmission stations and Transmission substations that meet the "medium impact" criteria from CIP-002-5.1, and their associated primary control centers. Furthermore, the standard drafting team expects many who are "applicable" to the standard will not identify facilities through their Requirement R1 risk assessment and Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. In those cases, the entity only performs Requirements R1 through R2. When that results in a null set, Requirement R1 additionally provides that subsequent risk assessments may occur less frequently. Similarly, while Transmission Operators are also listed in the applicability section, by virtue of application of the requirements, only certain Transmission Operators that are notified under the standard's Requirement R3 have obligations under the standard. Do you agree with the applicability section? If not, please provide specific recommendations, ensuring to articulate how your suggested approach would not limit the applicability in such a manner as to inadvertently miss a facility that should be covered under the standard as specified in the FERC order on physical security.**

Summary Consideration: The SDT thanks all commenters. All comments have been reviewed and changes that the SDT considers appropriate were incorporated into a subsequent revision. Part 4.1.1 was changed to clarify that applicable TO's are those that own transmission stations or transmission substations meeting the criteria in 4.1.1.1 through 4.1.1.4. The exemption for nuclear facilities was changed to provide more specific criteria in terms of the security plans under Nuclear Regulatory Commission or Canadian Nuclear Safety Commission jurisdiction. Several additions were made to the guidance section of the standard to address stakeholder concerns. A summary of comments and the SDT's response is provided**:**

- **Several commenters suggested adding verbiage to the applicability regarding the Transmission Operator to refer to Requirement R3.** The SDT considered this wording during its deliberations and determined it was not necessary as Requirement R3 is explicit in its applicability to only certain Transmission Operators. The SDT notes that, in general, Requirements are not included in the applicability Section of the standard.

- **One commenter suggested applying the standard to Reliability Coordinators (RC) and only the Transmission Operators the RCs deem critical.** The majority of stakeholders concur with the applicability as written. This suggested revision would be a major shift in philosophy and thus the SDT will not make the change.
- **Some commenters suggested that the Reliability Coordinator, Planning Coordinator and Transmission Planner should be added to the Applicability Section.** During the initial deliberations, the SDT considered requiring RCs, PCs and TPs to conduct the R2.2 verification but developed an alternative that was included in the original standard, given that it did not believe it was appropriate or necessary to require RCs, PCs or TPs to be required to conduct the R2.2 verification. R2.2 may be performed by a variety of entities or consultants. It is the responsibility of the Transmission Owner or Transmission Operator to ensure that the third party agreements are written with performance requirements to meet the time-line of R2.2.
- **Several stakeholders had comments about confidentiality, especially with respect to federal and state public disclosure laws applicable to registered entities, such as state regulatory agencies and municipal entities.** The SDT has drafted language in Requirement R2, Part 2.4, Requirement R6, Part 6.4 and Section 1.4 of the Compliance section of the standard to address confidentiality. Specifically, Compliance Section 1.4 states:

  Additional Compliance Information

  "Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities."

Requirement R2, Part 2.4 now provides:

> Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated verifying entity and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

Lastly, Requirement R6, Part 6.4 now provides:

> Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated reviewing entity and from any other form of public disclosure and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

Collectively, these provisions are designed to protect sensitive and confidential information from public disclosure consistent with the intent of paragraph 11 of the FERC order on physical security. Because the scope and intent of NERC standards is to set forth the requirements that owners, operators and users must follow to help protect the reliability of the Bulk-Power System,

the SDT concluded that it is beyond the scope of NERC Reliability Standards to specify whether certain information is exempt from U.S. or Canadian federal or state public disclosure laws. However, the SDT included language in Parts 2.4 and Parts 6.4 of the standard to clarify that entities shall have procedures to protect or exempt sensitive or confidential information developed under the standard from public disclosure. The SDT believes that responsible entities have existing mechanisms for safeguarding confidential or sensitive information used to comply with existing NERC Reliability Standards and also recognizes that there are other forums that can address the applicability of this information to public disclosure laws.

- **Several commenters had concerns with the term "collector bus" as used in the applicability.** The SDT notes that this language was copied directly from the CIP-002-5.1 standard. The SDT has also added language to the Guidelines and Technical Basis section to clarify the use of the term collector bus.
- **Several commenters suggested making revisions to the table in 4.1.1.2.** The SDT notes that this was copied directly from CIP-002-5.1. This language was used to mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1.
- **One commenter suggested revising the applicability to indicate that only a Transmission Owner "that owns any facilities identified in the following sections (4.1.1.1 through 4.1.1.4) will be required to perform the risk assessment and risk assessment validation as outlined in R1 and R2 of this standard."** The SDT notes that this is addressed in the Guidelines and Technical Basis section and that the requirements make this clear.
- **Several commenters requested additional guidance regarding "unaffiliated" third party reviewers.** The SDT has provided additional guidance in the Guidelines and Technical Basis section as well as revisions to Requirement R2, Part2.2 and the Rationale for R2.
- **Some commenters have concerns and recommended that the Applicability section reference the criteria of CIP-002-5.1 for a "medium impact rating" instead of re-stating it and questioned certain aspects of the applicability.** The SDT believes that the Standard and Guidelines and Technical Basis section clearly indicates that the risk assessment is to only identify a Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The SDT notes that this was copied directly from CIP-002-5.1. This language was used to mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1.
- **Some commenters disagree with the decision to limit applicability to only the primary control center.** The SDT believes that providing physical security for the primary control center and not back-up control centers is sufficient to protect the control of the critical Transmission stations and Transmission substations. Back-up control centers are not applicable, as they are already considered a form of resiliency and intentionally redundant.

- **Some commenters believed that the SDT did not go far enough in the applicability of facilities, in particular with respect to physical locations where critical cyber systems are housed and high impact control centers.** The SDT disagrees as the standard follows the FERC Order and employs a risk assessment designed to identify a Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Such a scope is different than the scope of other CIP standards to protect cyber assets.
- **Some commenters question why generation assets are exempt from analysis and verification required by Requirements R1 and R2.as they assert that some generation assets, if rendered inoperable, could result in widespread instability, uncontrolled separation, or Cascading.** The SDT considered whether to include Generator Operators and Generator Owners in the proposed Reliability Standard and decided not to include them as applicable entities. First, the FERC Order does not explicitly mention generation assets, and the order is reasonably understood to focus on the most critical Transmission Facilities. Second, the proposed Reliability Standard accounts for the loss of generation resources as explained in the Guidelines and Technical Basis section. A determination of whether a Transmission station or Transmission substation that meets CIP-002-5.1's medium impact criteria could, if rendered inoperable or damaged, result in widespread instability, uncontrolled separation, or Cascading within an Interconnection will consider the impact of the loss of generation at those Transmission stations or Transmission substations. Specifically, the transmission analysis or analyses conducted under Requirement R1 will take into account the impact of the loss of generation. As such it is not necessary to include Generator Operators and Generator Owners to ensure that the impact of loss of generation is considered.
- **One commenter disagreed with the SDT that many entities that are applicable to the standard will not identify facilities through their Requirement R1 risk assessment and Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.** The SDT members were selected based on their expertise. To more explicitly or in greater detail explain their statements related to the number of Transmission stations or Transmission substations that will be identified in R1 would likely disclose information that is confidential and contrary to national security. In the order, FERC states this opinion in paragraph 12 as well.
- **One stakeholder commented that the standard is too complicated of a draft standard for a 90 day consensus and that it should be simplified by altering the basic approach of the standard.** While the SDT appreciates suggestions on altering the basic approach, it believes it struck the right balance to be consistent with and responsive to the FERC Order and provide for an applicability that has been approved by stakeholders and regulators.
- **Some commenters had concerns regarding the language in the Exemption regarding nuclear facilities.** The SDT has added clarifying language to the exemption to address these concerns.
- **One commenter questioned why a Transmission Owner must go through requirements R1 and R2 before determining whether or not the remaining requirements apply.** TOs that meet the applicability criteria (Section 4) need to perform the risk assessment (R1) and have it verified (R2) regardless of their size. This will identify the critical stations. This concept is provided

in the first paragraph of the Guidelines and Technical Basis section of the standard: "Only those TOs with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6."

- **Many commenters requested additional guidance regarding Transmission Facility, Transmission station and Transmission substation**. The SDT has added clarifying language to the Guidelines and Technical Basis section of the standard.
- **Several commenters suggested that the SDT use the defined term "Control Center" in the standard.** The SDT deliberated this during the development of the standard but did not believe that it was clearly applicable to this standard because a Control Center includes the RC, BA and GOP. These entities are not applicable under this standard. The SDT has decided to retain the original language.
- **One commenter suggested adding the primary control center to the applicability section of the standard.** The SDT deliberated this in previous meetings but decided it was not appropriate. The SDT will retain the existing applicability as we believe that stakeholder consensus has been achieved.
- **Several commenters had concerns with the requirements language regarding the timing components.** The SDT has added language to the guidance to help clarify these issues. The SDT believes that the timelines are aggressive but achievable. Please see responses to specific timing requirements in other questions below.
- **One commenter suggested adding "AC and DC" to the applicability.** The SDT does not believe that this is necessary as the voltage levels shown imply this.

Organization	Yes or No	Question 1 Comment
Foundation for Resilient Societies	No	1. Reliability Coordinators (RCs) would be exempted under the draft standard. Not all Reliability Coordinators are Transmission Operators or Owners. Peak Reliability, Midcontinent ISO, and Southwest Power Pool would be exempted because they are not in the NERC Compliance Registry as Transmission Operators or Owners. (MISO is not a Reliability Coordinator under its MRO registration.) The following standards apply to Reliability Coordinators but not Transmission Operators and Owners: Standard EOP-006-2 - "System Restoration Coordination"; Standard EOP-002-3.1 - "Capacity and Energy Emergencies" (Applies to Balancing Authorities, Reliability Coordinators, and Load-Serving Entities); Standard IRO-009-1 - "Reliability Coordinator Actions to Operate Within IROLs"; Standard IRO-015-1 - "Notifications and Information Exchange

Organization	Yes or No	Question 1 Comment
		Between Reliability Coordinators." The Joint U.S.-Canada report on the 2003 Blackout concluded that insufficient wide-area control, such as that provided by Reliability Coordinators, was a contributing factor to the blackout. Yet the Standard Drafting Team has disregarded these findings in exempting Reliability Coordinators. It is a fallacy to believe that only entities with direct control of substations need protection from physical attack. If critical substations and their Reliability Coordinators are attacked in a coordinated manner, what entity will lead system restoration? It is essential that Reliability Coordinators are designated as responsible entities, both to protect their own facilities and to enable their authority to review the adequacy of physical security capabilities for operating utilities in their coordinating areas. Key findings of the joint U.S.-Canada Outage Task Force on the August 2003 blackout demonstrated the need for the Reliability Coordinators to actively supervise operating entities both to meet essential operating needs and to assure adequate regional visibility. See U.S.-Canada Power System Outage Task Force Report (April 2004). <http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>2. Balancing Authorities would be exempted under the standard. According to the NERC Compliance Registry, there are 19 Balancing Authorities that are not also Transmission Operators or Owners. The following standards apply to Balancing Authorities but not to Transmission Operators or Owners: Standard BAL-001-2 - "Real Power Balancing Control Performance"; Standard BAL-002-1 - "Disturbance Control Performance"; Standard BAL-003-1 - "Frequency Response and Frequency Bias Setting"; Standard BAL-004-0 - "Time Error Correction"; Standard EOP-002-3.1 - "Capacity and Energy Emergencies"; Standard IRO-006-5 - "Reliability Coordination - Transmission Loading Relief". If critical substations and their Balancing Authorities are attacked in a coordinated manner, what entity will balance demand and generation and manage the emergency, especially if the attack causes a regional load imbalance?3. Generator Operators would be exempted under the proposed standard. Generator Operators have vulnerable and hard-to-replace Generator Step Up

Organization	Yes or No	Question 1 Comment
		(GSU) Transformers, just as Transmission Operators have these transformers. Generation facilities could present contingencies in excess of spinning reserves, especially in congested areas with import of large megawatts of power over long transmission lines. Hence, Generator Operators should be included in mandatory physical security protection standards.4. The standard does not require modeled contingency planning for scenarios of physical attack. Contingency planning for physical attack should include megawatt capacity of all generators at single generation facility, not just failure of some individual units at the facility.5. Without explicit modeling for physical attack, some substations may fall through the cracks under "Aggregate Weighted Value" methodology in the standard. Physical attack of multiple transformers is different than the random failures planned for under the standard N-1 criterion. We have already seen attack on multiple transformers and their circuits at the Metcalf substation. The standard's criterion for violation of IROL limits would not be valid if the IROL limits assume random failures rather than coordinated physical attack.6. Some "High Impact" control centers would be exempt under the standard. Examples include the control centers for Peak Reliability, MISO, and SPP. In all, these control centers manage power for 141 million Americans. Control centers for Reliability Coordinators, Balancing Authorities, and Generator Operators are included in the "High Impact" Criteria for CIP-002-5.1 How can the standard drafting team take the CIP-002-5.1 criteria for substations but not control centers of Reliability Coordinators, Balancing Authorities, and Generator Operators? FERC Directive RD14-6-000 specifically requires protection of critical control centers in Footnote 6: "... the Commission expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers."7. While FERC Directive RD14-6-000 [146 FERC Â¶61,166] did not require specific security measures, it could have been reasonably expected that NERC would have developed specific measures to be applied on an as-needed basis. Nonetheless, the draft standard contains no specific requirements or even suggested guidelines for physical security measures. Such measures

Organization	Yes or No	Question 1 Comment
		might include: Opaque Fencing; Concrete Jersey Barriers; Motion Sensors; License Plate Scanners; Intentional Electromagnetic Interference (IEMI) Detectors; Gunfire Locators; Limiting of Close Public Access, Including Recreational Access; Armed Private Guards; Police Details; Deployment of National Guard Troops; Better Stocking of Spares-e.g., Transformer Bushings and Radiators; Equipment Monitoring and Redundant Telemetry to Control Centers. Instead, the standard relies upon self-devised security measures without prioritization or other guidance.8. The Metcalf incident unambiguously showed the value of equipment monitoring in mitigating physical attack on power transformers. Gunfire locators, had they been installed at Metcalf, could have alerted system operators to the attack in real-time, allowing prompt dispatch of law enforcement. Intentional Electromagnetic Interference (IEMI) Detectors could likewise provide real-time warning. If threat sensors with reliable and cyber-protected alerts are not part of a physical security system, it will be impossible to mobilize time-urgent countermeasures and impractical to take precautionary measures at other at-risk facilities vulnerable to coordinated attack.9. Intentional Electromagnetic Interference should be a physical threat included in the standard, because IEMI attack could occur in the physical proximity of facilities and could cause permanent physical damage in additional to temporary upset. IEMI detectors are a cost-effective measure as these devices cost approximately $15,000 per unit.10. The Metcalf Incident was both a physical attack and a cyber denial-of-service attack. The need for linkage between physical and cyber is explicitly called for in the RD14-6-000 Order of March 7, 2014, para 5, footnote 3. The implementation plan under this Order must require responsible entities to identify and protect cyber assets that link facilities and control centers that are otherwise identified as critical to the reliability of the BES. Communications and Network entities routinely provide hardened and alternate routing for military, other government and the Defense Industrial Base and their services should be an explicit requirement for Physical Security Standards that apply to any units and control centers that are identified

Organization	Yes or No	Question 1 Comment
		by Responsible Entities as critical to the Reliability of the BES.11. Review and certification of security plans, as proposed in the draft standard, does not necessarily provide a level of independence that would be prudent or credible to the public. Regional Entities or Reliability Coordinators for any facilities under their jurisdiction should be the primary authorities to review and approve security plans. Governmental authorities should have the ability to audit security plans.12. Improvements to the standard that we suggest would be marginal additions of facilities and their equipment and therefore would be cost-effective. We propose inclusion of primary and backup control centers for Peak Reliability, MISO, and SPP-an increase of 6 control centers as compared to approximately 200 already included Transmission Operator control centers. We propose inclusion of 19 additional Balancing Authorities as compared to 114 Balancing Authorities in total. There are only 50 non-nuclear generation facilities in the United States with nameplate capacity of 2 GW or more-this number is a rough approximation of the number of generation facilities that modeling might show to be capable of causing cascading outage if successfully attacked.13. RD14-6-000 directs NERC to submit for approval a physical security standard that would apply to the most critical facilities of the Bulk Electric System. The Standard Drafting Team has narrowly interpreted “critical facilities” to mean transmission facilities and directly linked control centers. We disagree with this narrow interpretation. Given the NERC interpretation and the 90 day deadline for standard development, NERC’s draft standard holds tightly to the most minimal facilities and therefore has significant gaps in protection as we describe in our foregoing comments. Some of these gaps, such as the exemption of Reliability Coordinators and Balancing Authorities, are so fundamental that they should be addressed immediately. For other gaps, we ask that NERC open a Standard Authorization Request (SAR) for a Phase Two physical security standard. This follow-on Phase Two standard should require modeling of BES operations sufficient to ensure identification of facilities that could cause cascading outage, single points of failure, data connectivity needs, and other processes and

Organization	Yes or No	Question 1 Comment
		technologies essential to grid protection-in short, a standard designated CIP-014 Version 2. An approved SAR for a Phase Two standard should be concurrent with NERC Board of Trustees approval of the current standard in development.
Florida Keys Electric Cooperative	No	o Stations and substations should be clearly understood within the standard, not just through a guidance document or rationale. It is FKEC's understanding that a "station" equates to a switchyard that does not include transformers; and a "substation" is a facility that does include transformers. This should be addressed at the beginning of the standard document to ensure clear understanding throughout the standard. o Do stations and substations focus only on certain key assets or all assets within the facility? Some assets could be those used for local distribution and/or be below 100kV. Clarity on this is required in order to understand the full scope and appropriateness of the standard.
Ciy of Garland	No	Applicability:The applicability section for Transmission Operators under section 4.1.2 should be explicitly limited to each TOP that operates a primary Control Center and receives a verified notification under Requirement R3. As written each TOP would be required to certify on each compliance contact that it has not been notified that it operates an applicable primary control center. The following edited text would accomplish that objective:4.1.2 Transmission Operator that operates a primary Control Center and receives notice from a Transmission Owner under Requirement R3.Please state clearly the Transmission Operator of a primary control center is not responsible for conducting a risk assessment under R1 or arranging for third party verification of the risk assessment under R2.
Black Hills Corporation Entities	No	Black Hills Corporation (referred to as BHC hereafter) believes that Section 4.1.1 has appropriate applicability specifics, but Section 4.1.2 only says "Transmission Operator", which initially implies a much greater scope. Request that similar to

Organization	Yes or No	Question 1 Comment
		Section 4.1.1 styling, Section 4.1.2 alternatively state “Transmission Operators notified by a Transmission Owner according to Requirement R3.”
Nebraska Public Power District	No	Due to the imposed time constraints and expedited development of this standard, sufficient time isn’t available to develop more realistic criteria for determining applicable substations creating unnecessary work and expense for transmission planners and reviewers.
Georgia System Operations Corporation	No	Georgia System Operations Corporation (GSOC) appreciates all the effort going into the draft of CIP-014-1 Physical Security Reliability Standard.GSOC supports the comments submitted by NRECA.
Georgia Transmission Corporation	No	Georgia Transmission Corporation (GTC) supports the efforts of the drafting team and believes that their efforts to create the CIP-014 Standard are moving in the right direction. GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard.
OPG	No	In the applicability section of the proposed standard, does the exemption refer to the Nuclear Generation Facility or the Transmission facility to which the Nuclear Generation Facility is connected? In Canada the Canadian Nuclear Safety Commission has no jurisdiction over the Transmission Owner/Operator; therefore the intent of the standard has to be made clear on this point.
Modesto Irrigation District	No	MID agrees that maintaining selection criteria consistent with CIP-002-5 is a prudent approach. However, if a facility is worthy of protection against a cyber attack, why is that same facility not worthy of consideration and evaluation for a potential physical attack? Inclusion of 'widespread instability, uncontrolled separation, or Cascading within an Interconnection' as an additional criteria is also prudent. These criteria focus on the immediate impact of the physical attack. What is missing is the longer term impact - if serious physical damage is

Organization	Yes or No	Question 1 Comment
		the result, can the damaged system perform adequately during subsequent peak loading periods?MID understands that these changes would extent the scope of the standards coverage beyond what was included in the FERC order. MID would like to respectfully suggest that the FERC order is a step in the right direction but did not fully consider all of the potential physical attacks that could cause 'widespread instability, uncontrolled separation, or Cascading within an Interconnection' or impair long term reliability of the system. MID feels that in responding to the FERC order, it would be acceptable to 'do the right thing' and step up to the challenge and evaluate all facilities identified in CIP-002-5 as high or medium impact the system against possible physical attacks.
New Brunswick Power Corporation	No	New Brusnwick Power (NB Power) agrees with the "applicability section" but not with portions of the preamble above, in question 1, which expands beyond applicability and states that "Furthermore, the standard drafting team expects many who are "applicable" to the standard will not identify facilities through their Requirement R1 risk assessment and Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection." To our knowledge there is no evidence to support the standards drafting teams statement that they expect that many of the applicable entities will not identify facilities through R1 and R2. FERC's statement that "we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System" is not sufficient evidence. NB Power is concerned that the cost impact of this standard may be underestimated as a result of this view that the number of critical facilities will be small. Please see comments below with respect to R1 and R2.
Rayburn Country Electric Cooperative	No	Overall comment is this is too complicated of a draft standard for a 90 day consensus!Keep it simple. I agree with the functional entitiy that is identified however, I would add GO to address any "critical" switchyards that may exist that are not owned by a TO.I also agree with the scoping of the facilities similar

Organization	Yes or No	Question 1 Comment
		to the CIP V5 criteria with the following exception, apparently a list already exists for the substations that should be considered "high" do they deserve an alternative approach to what is within this standard?Altering the existing basic approach as follows:Since the FERC order allowed for “One or More Reliability Standards”, it would be appropriate to address the “High “ facilities separate from the “Medium Facilities”. This approach would make it an easier task to file the “high standard” within the 90 days then follow with the “medium later”. Thus giving more time, latitude and maneuverability to address issues that arise specific to those facilities.
Con Edison and Orange & Rockland	No	Reliability Coordinator, Planning Coordinator and Transmission Planner should be added to the Applicability Section. That will obligate these entities to meet the 90 day review period stipulated in R2.2, if they are identified as a verifying entity by the Transmission Owner.
Clark Public Utilities	No	Section 4.1.2 of the Applicability section states “Transmission Operator.” This reference in the Applicability section should be more specific based on the the actual conditions under which CIP-014 would be applicable to a Transmission Operator. Clark suggests the referense should be revised to “Transmission Operators that have operational control over the primary control center of a Transmission station or Transmission substation identified in section 4.1.1.”
Southwest Power Pool Regional Entity	No	SPPRE does not agree with the applicability because it excludes certain facilities that could pose a significant risk to the BPS reliability if rendered inoperable or damaged as a result of a physical attack. Other facilities that should be applicable are those where high impact BES Cyber Systems are found. Additionally, any Special Protection System and automatic load shedding system capable of shedding 300 Mw or more should be included. Reference CIP-002-5 Attachment 1 (Impact Rating Criteria 1.1, 1.2, 1.4,2.9, and 2.10). SPPRE also

Organization	Yes or No	Question 1 Comment
		disagrees with the decision to limit applicability to only the primary control center.
National Rural Electric Cooperative Association (NRECA)	No	Stations and substations should be clearly understood within the standard, not just through a guidance document or rationale. It is NRECA's understanding that a "station" equates to a switchyard that does not include transformers; and a "substation" is a facility that does include transformers. This should be addressed at the beginning of the standard document to ensure clear understanding throughout the standard.Do stations and substations focus only on certain key assets or all assets within the facility? Some assets could be those used for local distribution and/or be below 100kV. Clarity on this is required in order to understand the full scope and appropriateness of the standard.
Northeast Power Coordinating Council	No	The applicability of the draft standard should be expanded to incude Planning Coordinators in addition to Transmission Owners and Transmission Operators. While NPCC agrees that TOs and TOPs simple application of the screening criteria to determine which facilities need analysis, they may not be able to conduct a complete analysis. The SDT should consider that Transmission Owners in some cases do not have the ability to conduct an analysis with a "wide area" view of consequences. Smaller TOs or TOPs only have an outside equivalent representation of the BES and could need help conducting their analyses. Consideration should be given to allow them to conduct the studies in conjunction with PCs.
EF Cass Consulting Inc.	No	the applicability section table should be modified by either removing the 500kV line or making it a 3000 value. By giving it a 0 value in the table it send a different message than the text indicating all 500kV facilities are in. Also, in the draft RSAW Compliance Assessment approach for R1, it would appear that a Transmission Owner needs to comply with R1 and R2 in order to determine if the standard applies to them. If an entity is required to have a process for determining applicability then it needs to be a requirement. The applicability

Organization	Yes or No	Question 1 Comment
		section should produce a yes or no answer. I spoke with Nick Webber of WECC and his response back was "Much like the requirement of all entities to apply CIP-002, all entities registered as for the TO function must complete CIP-014-1 R1 and R2. Each TO must complete R1 to determine if R3-R6 apply. The TO then must subsequently have that R1 assessment reviewed as required in R2." An entity should not have to comply with 2 of the requirements in order to determine if the standard applies to them. If all TOs are expected to comply with R1 and R2, then move the criteria into the requirement, if that is not the intent, clarify that once an entity reviews the applicability section and determines the standard does not apply they are finished. The rationale for requirement R1 indicates the criteria is in R1 when it is actually in the Applicability section.
Bureau of Reclamation	No	The Bureau of Reclamation (Reclamation) believes that the Transmission Planner, Planning Coordinator, and Reliability Coordinator should be included in the Applicability section of the standard and should be responsible for reviewing the Transmission Owner's risk assessment (BES impact assessment).
Tri-State Generation and Transmission Association, Inc.	No	The drafting team may want to consider language referencing the CIP-002 Critereon rather than outright copying it in order to prevent changing multiple standards as the CIP-002 standard evolves.CIP-002-5.1 Attachment 1: Overall Application gave guidance on how to treat joint ownership facilities. Tri-State feels that this new standard would also benefit from such guidance.
Omaha Public Power District	No	The Omaha Public Power District (OPPD), suggests replacing the term "primary control center", using the NERC defined term "Control Center", with "primary Control Center".
NCPA Compliance Management Operating Committee	No	The Standard Drafting Team (SDT) estimates that relatively few Transmission Owners (perhaps 30 or less) will have Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability or uncontrolled separation. The Applicability section creates a lot of

Organization	Yes or No	Question 1 Comment
		work for many TOs an TOPS to identity those 30 or less transmission stations out of the 55,000 substations. The SDT might consider a higher level of applicability as was done for EOP-010-1, Geomagnetic Disturbance Operations i.e. apply the standard to Reliability Coordinators (RC) and only the Transmission Operators the RCs deem critical.This would be a more efficeint filtering process. Benefits of such an approach would be (1)Simplification and tighter security of critical information and informaton sharing (2) streamling and simplicaton of requirements for unaffiliated third party review, for example one reviewer could handle the risk assessment, vulnerability and threat assessment and review of security plans (combines requirements R2 & R6 together) (3)Time and resources of the entity could be more efficiently and economically managed as all reviews could be handled by a single Reviewer in a continuous manner rather than starting a stopping for different phases. (4) Saves many entities who would fall out of the process after going through the first three requirements. I expect RCs, ISOs and Regional Entities already know this
Kansas City Power & Light	No	There is a use of the term "critical" being used in several NERC Standards, which can cause unintended confusion. Since the applicability of this draft Standard is derived from the approved CIP-002-5.1, can this proposed Standard be added as a revision to CIP-002-5.1?
Utility Services	No	We have seen in the previous versions of the CIP standards that “Risk Assessments” are not performed consistently, and create more problems than they solve, and even violation determinations. The solution in CIP-014 to this inherent problem seems to just add another level of review, but there is no guarantee of consistency within these assessments. Additionally, it seems the drafting team is suggesting a single assessment (“Concurrent with R1 study” specified in R2), this this might eliminate the review stage all together. A clear applicability section with a “brightline” approach would be more appropriate and consistent with the progression of the CIP standards overall. Otherwise, what prevents an auditor from making a determination that the assessment

Organization	Yes or No	Question 1 Comment
		performed was not sufficient or incomplete, even with a 3rd party validation? Entities need a clear definition to avoid the problems of the past. If the drafting team wants to limit the scope of Facilities this could be detailed in the "Exemptions" portion of the "Applicability" section of the standard. 1. The "Exemption" section needs to be clarified. If this applies to the entire section number it 4.2. If it is only applicable to the last bullet it is under give it the appropriate number (4.1.2.1)Suggested re-write4. Applicability:4.1. Functional Entities:4.1.1 Transmission Owner4.1.2 Transmission Operator4.2. Applicable Facilities: The following Facilities, systems, and equipment, owned or operated by each Responsible Entity in 4.1 above are those to which these requirements are applicable. 4.2.1 Transmission Facility operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.4.2.2 Transmission Facility that operate between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.ADD TABLE HERE4.2.3 Transmission Facility at a single station or substation location that is identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.4.2.4 Transmission Facility at a single station or substation whose unplanned unavailability would result in the loss of at least 3000 MW of generation.4.2.5 Control Center that controls:4.2.5.1 Transmission Facilities identified by

Organization	Yes or No	Question 1 Comment
		identification under 4.2.1 through 4.2.4; or4.2.5.2 Two or more Facilities which contain a Cyber System(s) which have been identified as a High or Medium Impact BES Cyber System.4.2.6 Exemptions: 4.2.6.1 All facilities regulated by the Nuclear Regulatory Commission or Canadian Nuclear Safety Commission.4.2.6.2 Transmission station or substation connected to only one other Transmission station or substation.4.2.6.3 Transmission station or substation that does not operate above 200kV.4.2.6.4 control centers not designated as a "primary control center"
SPP Standards Review Group	No	We have some concern with the undefined term 'collector bus facility'. Without a definition for collector bus facility some may consider the entire switchyard at a generating station as a collector bus facility. We do not believe the drafting team intended this to be the case. Therefore, some additional clarification may be needed for the term.
Public Utitliy District No. 1 of Cowlitz County, WA	No	We strongly disagree with applicability statements being outlined in the requirement. We support APPA's recommendation to further define TOP applicability in section 4.1.2 to avoid nuisance compliance certifications.
Western Electricity Coordinating Council	No	WECC questions why generation assets are exempt from analysis and verification required by Requirements R1 and R2. It is possible that some generation assets, if rendered inoperable, could result in widespread instability, uncontrolled separation, or Cascading.WECC recommends removing the 500 kV line in the Weighted Value table. All 500 kV facilities are to be assessed per Applicability Section 4.1.1.1 and including 500 kV lines in the table in applicability section 4.1.1.2 with a zero value seems more likely to add confusion than to provide clarifying information.Applicability section 4.1.2 makes it look like the standard is applicable to all Transmission Operators. WECC suggests adding some clarifying language to indicate that the standard is only applicable to Transmission

Organization	Yes or No	Question 1 Comment
		Operators notified per Requirement R3. This may serve to make the standard more acceptable to Transmission Operators in general.
Herb Schrayshuen	No	The applicability of the standard is to Transmission Owners and Transmission Operators. Generating plants sites where the facilities production capability exceeds 1000 MW or other suitably larger amount should be included.
Bonneville Power Administration	Yes	4. Applicability: BPA believes that the medium list for HV transmission entities will result in numerous facilities having to be protected (all 500 kV) contrary to the drafting team comment that not many facilities will be deemed critical. 4.1. Functional Entities: BPA recommends that this section reference the criteria of CIP-002-5.1 for a "medium impact rating," instead of re-stating it without citation. Otherwise it is confusing. For example, the source of the tabulated weighting criteria is unclear and it is difficult to know there is a connection to any previous or established standards.
Idaho Power Co.	Yes	4.1.2. Seems vague in its description lending the reader to believe that TOPs are in scope at all times which is inconsistent with guidance later in the standard which states they are only required to perform actions when informed they are in scope by a TO. Further Clarification is needed in this section.
American Public Power Association (APPA)	Yes	APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members.CONTROL CENTER - Use the defined term "Control Center" by capitalizing as "primary Control Center" or explain why lower case "primary control center" is different and needs to be used in the standard. Consider inserting "with operational control" after primary Control Center, to express the intent of the text box Rationale for Requirement R1 that the control center must be capable of taking

Organization	Yes or No	Question 1 Comment
		electronic actions that can cause direct physical actions at the identified station or substation. Please also clarify whether the periodic use of a backup control center as the entity's primary control center would make R4 and R5 applicable to both the primary and backup control centers.UNAFFILIATED - needs to be either defined or a footnote needs to be added to the standard to explain that "unaffiliated means that the selected verifying or reviewing entity cannot be a corporate affiliate," as stated in the guidance section.CONFIDENTIALITYPublicly Owned Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the A. Introduction section, after 6. Background:7. Critical Facilities InformationRecords and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments

Organization	Yes or No	Question 1 Comment
		and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. ALTERNATIVE PROPOSED REQUIREMENT LANGUAGE ADDITIONS:R1.3 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under this standard.R3.2 The Transmission Owner will keep confidential all records and information related to the notifications conducted under Requirement R3 and R3.1 of this standard. R4.4 The Transmission Owner and each applicable Transmission Operator will keep confidential all records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1. APPA suggests technical edits to Requirements R2.4 and R6.4 to insert "or made available to" after "exchanged with." This change would clarify that sensitive or confidential information does not have to be actively "exchanged" between entities to be subject to the protections directed under Requirements R2.4 and R6.4. APPLICABILITY 4.1.2 - The applicability section for Transmission Operators under section 4.1.2 should be explicitly limited to each TOP that operates a primary Control Center and receives a verified notification under Requirement R3. As written each TOP would be required to certify on each compliance contact that it has not been notified that it operates an applicable primary control center. The following edited text would accomplish that objective:4.1.2 Transmission Operator that operates a primary Control Center and receives notice from a Transmission Owner under Requirement R3.Please also confirm that the Transmission Operator of a primary control center is not responsible for conducting a risk assessment under R1 or arranging for third party verification of the risk assessment under R2.

Organization	Yes or No	Question 1 Comment
The Empire District Electric Company	Yes	EDE feels this is the right approach on selecting a threashold for applicability to this standard.
ISO/RTO Standards Review Committee	Yes	IntroductionThe proposed standard provides adequate flexibility with respect to the risk assessments and security evaluations and plans. This allows the industry to capitalize on their experience in these matters, while also accommodating changes that warrant consideration. Applicability SectionThe applicability scope is reasonable in terms of identifying the appropriate functional entities to address physical security concerns. Similarly, the proposed standard establishes a reasonable approach for identifying the scope of facilities by 1) initially defining an objective set based on the CIP-002-5.1 criteria, and then 2) refining that set based on analyses that assess the relationship of those facilities to specific, system conditions/impacts metrics - i.e. widespread instability, uncontrolled separation, or Cascading within an Interconnection.
National Grid	Yes	It should be clear that the applicability section of the standard is only intended to provide a valid, technically sound basis to be used as the 'starting point' to those transmission facilities or stations that should be included in the risk assessment.We suggest the following modifications:4.0 Applicability:4.1 Functional Entities:4.1.1 Transmission Owner that owns any facilities identified in the following sections (4.1.1.1 through 4.1.1.4) will be required to perform the risk assessment and risk assessment validation as outlined in R1 and R2 of this standard. Should the risk assessment identify critical assets then the Transmission Owner is subject to the remaining requirements (R3 through R6) of the standard. 4.1.2 Transmission Operator
ITC	Yes	ITC agrees with utilizing, as a starting point, the CIP-002-5.1 "medium impact" rating to determine the facilities needing enhanced physical security. As ITC indicated in its comments to FERC in Docket No. RD14-6, these new physical security Standards must be developed in a coordinated manner to avoid

Organization	Yes or No	Question 1 Comment
		duplicative, overlapping, or contradictory requirements among the various existing Reliability Standards that cover a similar if not an identical set of assets. By ensuring "that entities could apply the same set of criteria to assist with identification of facilities under CIP Version 5 and proposed CIP-014-1," the SDT has fully met our expectations with respect to the applicability of the standard.
Los Angeles Department of Water and Power (LADWP)	Yes	LADWP requests the Drafting Team to make the following changes:- For Secion 4, you may want to add Transmission Planner and Planning Coordinator to the applicability. These functions may have responsibility on at least R1 and R2.- Secion 4.1.1.1 - Add "(AC or DC)" as follows: "Transmission Facilities operated at 500 kV (AC or DC) or higher....."
Public Utility District No. 2 of Grant County, WA	Yes	Language contained in R1 does not align the performance of risk assessments of Transmission stations and Transmission substations with the actual commissioning or energization of such facilities. To ensure that risk assessments and subsequent risk assessments address existing and planned Transmission stations and Transmission substations to be in service within a risk assessment window the following edits are recommended to R1:R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 30 months) ..1.1. Subsequent risk assessments shall be performed at least once every 30 calendar months. (this would apply to all applicable TOs) GCPD also supports comments made by APPA regarding the insertion of the language addressing Confidentiality and treatment of Critical Facilities Information. GCPD's suggested language is as follows: Risk assessments and evaluations of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to

Organization	Yes or No	Question 1 Comment
		Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure.
MidAmerican Energy Holding Company	Yes	MidAmerican Energy Holdings Company (MEHC) agrees with the applicability section.
MISO	Yes	MISO supports the proposed applicability section and agrees that other entities do not need to be included. In particular, MISO would not support application of this Standard to Reliability Coordinators or Balancing Authorities, as these entities' control centers are adequately protected with regard to physicial security under CIP-006-3c and its successor standard. Moreover, these control centers are subject to the requirements of EOP-008-1 including the transfer functional control to backup facilities. MISO therefore agrees that the focus of CIP-014-1 should be those facilities that are not otherwise fully protected by CIP-006-3c, such as those that do not not rely entirely on Critical Cyber Assets to maintain reliability.
ATCO Electric	Yes	No Comment.
SERC CIPC	Yes	Recommend that the drafting team include the Transmission Planner who would be performing the risk assessment in the applicability as discussed in R1.
ReliabilityFirst	Yes	ReliabilityFirst supplies the following comments for consideration:1. ReliabilityFirst believes there may be a perceived disconnect between the Applicability Section and Requirements 5 and 6. Requirements 5 and 6 introduce new requirements surrounding the Transmission Owners "primary control center" though the "primary control center" is not listed within the Applicability section as an asset the Transmission Owner owns that is included in the standard. Consideration may be given to adding "primary control center" under section 4.1.1. [Note: Since "Control Center" is a NERC defined term, this term should be capitalized throughout the standard.]2. Applicability section 4.1.1.4 -

Organization	Yes or No	Question 1 Comment
		ReliabilityFirst believes the term “as essential” is ambiguous and may cause unintended compliance monitoring implications. ReliabilityFirst recommends the following for consideration: “Transmission Facilities identified [in] Nuclear Plant Interface Requirements [which provide offsite power].” ReliabilityFirst believes the recommended language addresses the intent of the SDT.
San Diego Gas & Electric	Yes	San Diego Gas & Electric (SDG&E) agrees that it is appropriate to start with those Transmission Owners that own Transmission facilities that meet the bright line criteria in Reliability Standard CIP-002-5.1 for a “medium impact” rating. However, SDG&E believes that it would be prudent to simply refer to the CIP-002-5.1 Impact Rating Criteria rather than restating it in CIP-014 Standard. Being more specific that this Standard is applicable to Transmission Owners that have any facilities identified as “medium impact” facilities under CIP-002-5.1 Attachment 1, Inpact Rating Criteria 2.4, 2.5, 2.6 and 2.7, would be clearer and more consistent with the general way that CIP-003-5 through CIP-011-5 are built upon the identification of “critical” facilities made in CIP-002-5.1. Linking the two explicitly, rather than simply restating the same language, would prevent the possibility that differences could creep into the rules over time as each Standard is modified.
Seattle City Light	Yes	Seattle City Light supports the Question 1 comments of APPA, with one exception in the area of Confidentiality. Seattle's comments about Confidentiality, in place of APPA's comments on this topic, follow.CONFIDENTIALITYThe stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical

Organization	Yes or No	Question 1 Comment
		information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the Introduction Section:7. Critical Facilities InformationRecords and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access to the records and information, and any agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. Proposed Requirement Language:R1.3 Records and information related to the risk assessments conducted under this standard that are designated confidential by the Transmission Owner are [intended to be] exempt from public disclosure.R3.2 Records and information related to the risk assessments conducted under

Organization	Yes or No	Question 1 Comment
		Requirement R1 of this standard that are designated confidential by the Transmission Owner are [intended to be] exempt from public disclosure. R4.4 Records and information related to the evaluation of physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and/or Control Center(s) identified in Requirement R1 conducted under this standard that are designated confidential by the Transmission Owner or Transmission Operator are [intended to be] exempt from public disclosure.
Arizona Public Service Company	Yes	See related comments under Requirement 2 below.
Seminole Electric Cooperative, Inc.	Yes	Seminole supports the comments by NRECA. Additionally, Seminole supports the use of CIP-002-5 medium impact criteria for use in CIP-014. CIP-002-5 has at least one issue that will apply to CIP-014 as well. There are multiple ways to interpret the phrase Transmission Facility. One example is clarifying what is in the scope of a Transmission Facility. The definition or other documentation should state that the substation is exclusive of the criticality of any connected substation and clarify that a Transmission Facility as used here does not include Transmission Lines.
Salt River Project	Yes	SRP supports comments submitted by APPA.
Northeast Utilities	Yes	Standard Drafting Team should define the term widespread. NU suggests the following definition:Widespread - An event that causes voltage collapse, Cascading and/or instability that results in uncontrolled separation across significant portions of the Interconnection. The registered entity shall use regional criteria to evaluate.
PNM Resources	Yes	Support the comments submitted by EEI.
Texas RE	Yes	The applicability should include the TP, PC, RC, and the unaffiliated entity as they are noted in this standard.

Organization	Yes or No	Question 1 Comment
PPL NERC Registered Affiliates	Yes	These comments are submitted on behalf of the following PPL NERC Registered Affiliates: Louisville Gas and Electric Company and Kentucky Utilities Company; PPL Electric Utilities Corporation, PPL EnergyPlus, LLC; PPL Generation, LLC; PPL Susquehanna, LLC; and PPL Montana, LLC. The PPL NERC Registered Affiliates are registered in six regions (MRO, NPCC, RFC, SERC, SPP, and WECC) for one or more of the following NERC functions: BA, DP, GO, GOP, IA, LSE, PA, PSE, RP, TO, TOP, TP, and TSP.The PPL NERC Registered Affiliates support the draft standard. As members of EEI, we also support the comments being submitted by EEI. In addition, we have provided specific comments that we believe would add clarity to the standards and simplify the requirements. We urge the SDT to consider our comments and incorporate them as appropriate when developing the final standard that will be balloted. Comments: Section 4.1.1.2 includes in the applicability Transmission Owners that own Transmission Facilities that are operating between 200kV and 499 kV at a single station or substation, where the station or substation is connected at 200kV or higher voltages to three or more other Transmission stations or substations and has an "aggregated weighted value" exceeding 3000 according to the table set forth in section 4.1.1.2. Because section 4.1.1.1 covers transmission facilities operated at 500 kV and above and section 4.1.1.2 only references Facilities operating between 200 kV and 499 kV, the fourth row in the table in section 4.1.1.2 referencing voltages of "500kV and above" is unnecessary and should be removed.
NRG Energy, Inc.	Yes	This standard should not address generation interconnection facilities because the BES is designed to withstand the loss of generation facilities through the use of regional reserves.
Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.	Yes	Vectren supports the use of the CIP-002-5.1 medium impact criteria. This approach focuses on the facilities that could have a true adverse impact to the Bulk Electric System and provides consistency with approved standards.

Organization	Yes or No	Question 1 Comment
Hydro One	Yes	We agree with the Applicablity. R1 has provided flexibility in the assessment method.
Independent Electricity System Operator	Yes	We agree with the inclusion of the Transmission Owners and Transmission Operators as they have the obligations to conduct an evaluation of the potential threats and vulnerabilities to a physical attack on each of their respective transmission stations/control centres.
ACES Standards Collaborators	Yes	We support a clear and defined “bright line” criteria that has been industry vetted and FERC approved as the starting point for the risk assessment in R1.
Cooper Compliance Corp	Yes	We support the applicability proposed by CIP-014-1.
Western Area Power Administration	Yes	Western agrees with what we understand as the applicability, based on the CIP-014 Workshops. However, we have some concern with the undefined term ‘collector bus facility’. Without a definition for collector bus facility we are concerned that some parties may consider the entire switchyard at a generating station as a collector bus facility. Based on the discussion during the CIP-014 Workshops we do not believe the drafting team intended this to be the case. Therefore, some additional clarification may be needed for the term.
Vermont Transco LLC	Yes	While we do agree with the need for the standard and the importance of it we do have comments on the proposed standard. The intention of this standard is to protect those facilities that are most critical to the bulk electric system. The CIP-002-5.1 criteria brings into play many facilities that while deemed critical to an entity are not likely critical to this standards definition and would not cause wide area impact.
Consumers Energy Company	Yes	With Michigan situated as a peninsula, Michigan infrastructure may be at a lesser risk, based on the limited number of interconnect avenues into and out of our system. Meaning the highest level of criticality likely would be identified as

Organization	Yes or No	Question 1 Comment
		those key interconnect points, and not the entirety of our system. From our experience with the blackout of August 2003, BES implications were centered in southeast Michigan and although affected, we were able to successfully minimize/sustain our base load generation requirements. Any substation targeted in Michigan may not have a cascading effect on the BES.
Dominion	Yes	
Duke Energy	Yes	
FirstEnergy	Yes	
Florida Municipal Power Agency	Yes	
Tampa Electric Company	Yes	
Tennessee Valley Authority	Yes	
Ameren	Yes	
American Electric Power	Yes	
American Transmission Company, LLC	Yes	
Basin Electric Power Cooperative (BEPC)	Yes	
California ISO	Yes	

Organization	Yes or No	Question 1 Comment
Central Hudson Gas & Electric Corporation	Yes	
City of Garland	Yes	
Colorado Springs Utilities	Yes	
Edison Electric Institute	Yes	
Empire District Electric Company	Yes	
Exelon	Yes	
Flathead Electric Cooperative, Inc.	Yes	
FortisBC	Yes	
GridWise Alliance	Yes	
Hydro QuÃ©bec TransÃ‰nergie	Yes	
Manitoba Hydro	Yes	
Minnesota Power	Yes	
Minnkota Power Cooperative	Yes	
None	Yes	
Pacific Gas and Electric Company	Yes	

Organization	Yes or No	Question 1 Comment
Peak Reliability	Yes	
Pepco Holdings Inc.	Yes	
Portland General Electric	Yes	
South Carolina Electric and Gas	Yes	
Southern California Edison Company	Yes	
Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	Yes	
The Empire District Electric Company	Yes	
Virginia State Corporation Commission	Yes	
Westar Energy	Yes	
Xcel Energy	Yes	
Encari		Historically, FERC and NERC have taken the position that redundancy is not an acceptable criterion to exempt a Critical Cyber Asset from mandated physical or

Organization	Yes or No	Question 1 Comment
		cyber controls. Redundancy is not supposed to be a factor in the determination of the criticality; instead redundancy is used to improve reliability and availability. This principle should be extended to the protective measures applicable to control centers under CIP-014-1. So long as both the primary control center and backup control centers meet the bright line criteria for a medium impact rating under CIP-002-5.1, the protections under CIP-014-1 should apply equally to both the primary and backup control centers.
APPA		SMUD supports the APPA comments and is specifically concerned that records and information developed and maintained under each of the requirements for this standard are afforded the necessary protection through an introduced section, #7 Critical Facilities Information. We respectfully ask the Standard Drafting Team to ensure that AUTHORIZED ACCESS to information pertains to ANY RECORD AND INFORMATION associated with the Physical Security Standard.

2. **Requirements R1 through R3: The first three requirements of CIP-014-1 require Transmission Owners to: (1) perform risk assessments to identify through transmission planning analysis those Transmission stations and Transmission substations that meet the "medium impact" criteria from CIP-002-5.1, and their associated primary control centers, that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; (2) arrange for a third party verification (as directed in the order) of the identifications; and (3) notify certain Transmission Operators of identified primary control centers that operationally control the identified and verified Transmission stations and Transmission substations. The requirements provide the periodicity for satisfying these obligations. Only an entity that owns or operates one or more of the identified facilities has further obligations in Requirements R4 through R6. If an entity identifies a null set after applying Requirements R1 through R2, the rest of the standard does not apply. Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security**.

Summary Consideration: The SDT thanks all commenters. All comments have been reviewed and changes that the SDT considers appropriate were incorporated into a subsequent revision. Requirement R2, Part 2.2 was reworded to align with the intended applicable entity. Language was added to Requirement R2, Part 2.4 to specify that the TO must develop procedures to protect or exempt sensitive or confidential information developed pursuant to the standard from public disclosure. A change was made to Requirement R3 to accurately state which primary control centers are included in the requirement. Corresponding changes were made to each measure. Several additions and clarifications were made to the Guidelines and Technical Basis section based on stakeholder comments. A summary of comments and the SDT's response is provided:

- **Requirement R1. Commenters suggested removal or changes to the term 'Risk Assessment' in R1.** The SDT maintained language consistent with the FERC Order.
- **Requirement R1. Commenters recommended additions to the Guidelines and Technical Basis section to clarify the term 'primary control center'.** The SDT has added language to the Guidelines and Technical Basis section to clarify a primary control center.
- **Requirement R1. Commenters asked for clarification on the type of analysis required for a risk assessment, recommended specific TPL approaches, proposed N-1 analysis for long lead time replacement equipment, and recommended use of IROL criteria.** The SDT has written the requirements to allow flexibility for the TO to include risks that it believes are realistic. The resulting physical security plan is to be designed to protect the assets, including any long lead-time assets. Specifically, in Requirement 5, Part 5.1, the standard identifies resiliency as an appropriate consideration when drafting a physical security plan. A TO may use IROL criteria but the SDT intends for the standard to provide flexibility.
- **Requirement R1. Commenters suggested alternate periodicity.** The SDT believes the specified periodicity is reasonable and will identify assets in a timely manner. The SDT notes that the periodicity is aggressive but achievable. The SDT considered a balance

of risk to the BPS and burden to the responsible entity when developing the periodicity. If the TO does not identify Transmission station or Transmission substation in its risk assessment, then the periodicity changes to 60 months.

- **Requirement R1. A commenter suggested removing the requirement to include facilities that are planned to be in service within 24 months and replacing it with a requirement to update the risk assessment prior to addition of a new Transmission station or Transmission substation.** The SDT chose the language of R1 so that entities would have a fixed starting point for risk assessment of existing stations as well as those planned to be operational within 24 months from the assessment date. The TO may perform additional assessments prior to adding facilities as the standard does not preclude additional assessments. Verification of additional risk assessments conducted more frequently than the periodicity prescribed in the standard is not required.
- **Requirement R2. Commenters recommended removing third party verification, changes to entities in Requirement R2, Part 2.1, additions of PC, TP, and RC to the applicability, limiting verification to the Regional Entities based on confidentiality concerns, or not permitting the same organization that conducted the risk assessment in Requirement R1 to be a verifier.** The third party verifier and reviewer are specified in the FERC Order. The SDT believes its approach with verifiers and reviewers is consistent with the FERC Order. The SDT believes the most reliability benefit will come from providing flexibility to TOs rather than adding prescription, even for purposes of making compliance easier. The SDT discussed many options with respect to the risk assessment and the confidentiality of information. The team reached consensus with the proposed requirements that provide flexibility in who performs the risk assessment and verifications while protecting the confidentiality of information.
- **Requirement R2. Commenters indicated that the term 'unaffiliated' was not sufficiently clear. Federal government-owned entities stated the SDT's definition of unaffiliated could exclude other agencies.** The Guidelines and Technical Basis section explains the SDT's use of the term unaffiliated. It was amended to more clearly indicate that a government-owned utility could use another government entity to satisfy the verification required by R2. The following was added: "The prohibition on registered entities using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. For instance, a U.S. federal power marketing agency may select as its verifier another U.S. federal agency to conduct its verification so long as the selected entity has transmission planning or analysis experience. Similarly, a Transmission Owner owned by a Canadian province can use a separate agency of that province to perform the verification. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit."
- **Requirement R2. Commenters indicated additional guidance on protecting sensitive or confidential information was needed.** The Guidelines and Technical Basis section has been revised to address the concern. Please see response to this concern in Question 1 above.

- **Requirement R2. A commenter asked the SDT to clarify whether third party verification was required for a minor revision to the Requirement R1 risk assessment.** As stated in the requirements, the risk assessment shall be performed at least once every 30 calendar months (or 60 calendar months if no assets were identified in the previous risk assessment) and verified within 90 calendar days of completion. Entities are not precluded from performing additional actions outside the context of the standard requirements.
- **Requirement R2. Commenter proposed alternate language to Requirement R2, Part 2.2 to be consistent with applicability of the standard.** The SDT agreed and made this clarifying change.
- **Requirement R2. Commenters suggested changes to requirements for documenting recommendations from the third party verifier.** The SDT believes it is appropriate to document the TO's response on all recommendations from the verifier, even if the verifier is recommending the removal of an asset from the list developed in Requirement R1.
- **Requirement R2. Some commenters indicated the timeline was too short.** The SDT believes the timeline is aggressive but achievable and further supports stakeholder consensus.
- **Requirement R3. A commenter proposed adding clarification to the Guidelines and Technical Basis section on what operational control means.** The SDT has added a description to the Guidelines and Technical Basis section.
- **Requirement R3. A commenter stated that 7 days was an unnecessarily short timeline.** The SDT believes that the notification is important for reliability since the necessary subsequent actions for developing a security plan may not be triggered until the notification has occurred.

Organization	Yes or No	Question 2 Comment
ACES Standards Collaborators	No	(1) Conceptually, we agree with this approach but have identified the following issues and concerns. (2) R1 requires additional clarification. The Guidelines and Technical Basis section states that the "bright line" criteria in applicability section is used to identify an initial set of stations and substations that must be further evaluated in R1. It is our understanding that if a TO owns one 500 kV transmission station and no other transmission facilities, then that 500 kV station would meet the applicability section 4.1.1.1 criteria. The TO would be required to perform a risk assessment to identify if that facility was rendered inoperable, it could result in widespread instability, uncontrolled separation, or Cascading in an Interconnection. In other words, if the applicability section is met, the TO must perform a risk assessment, but the remainder of the standard (R4-R6) would not apply unless loss of the Facility would result in widespread instability, uncontrolled separation or Cascading. Please confirm if our understanding of applying the requirements is the correct approach. (3) We see a significant compliance risk created by Requirement R2 and question why the unafilliated third party verification cannot be integrated into the Regional Entity compliance monitoring and enforcement processes to minimize costs and limit access to highly sensitive information. The third party verification creates a compliance problem outside of the TO's control because the TO is dependent on a third-party for regulatory compliance and there is no obligation on any of the third parties (i.e. RC, PC) identified in the standard to verify the risk assessment. Thus, the TO will have to rely on consultants to perform the verification. Since all TOs will be working towards the same efffective date, there will be a backlog and the reviews may not be completed by the timelines established in the standard. Review by consultants also will increase the number of people with access to highly sensitive information. While this concern can be partially mitigated through confidentiality agreements, the more people that have the information, the higher the probability the information will be released, whether intentional or unintentional, to persons that should not have the information. All of these issues could be resolved if NERC and Regional Entities conducted the review. The review could be performed as part of a spot check of the standard 90 days after the initial effective date. If NERC or the Regional Entity disagree with the approach or

Organization	Yes or No	Question 2 Comment
		believe additional facilities should be added, RAI would give them the flexibility to treat the issue as not impactful to compliance as long as the TO resolved the issue within a certain time period. This approach would result in a reduced cost impact on industry and minimize the distribution of highly confidential information reducing the likelihood of information leaks. As an alternative, we suggest that a companion requirement that compels either the RC or PC to perform the verification. This would also reduce the costs impacts and distribution of sensitive information since these entities will already be familiar with the TOs they are verifying and will already have access to highly sensitive information. (4) Regarding R3, this requirement does not warrant a 7-day timeline. This is not a near real-time issue. We suggest 30 days as a reasonable notification period.
Ameren	No	(1) Regarding R3 and R3.1, we believe that the 7 day requirement is too short and 30 days would be more appropriate to notify other utilities. (2) R4 should have wording added to the requirement that the R4 evaluation is to be completed 120 days after the completion of R2. Then, the R5 wording should be changed so that the R5 physical security plans should be completed 120 days after the R4 evaluation is completed.
Utility Services	No	1. What is a Transmission "station"? What is the definition of station and what is it intended to cover that substation does not. Generally in the NERC glossary "station" is associated with Generation, not Transmission. 2. There is a concern between R1 and R5. a. R1 states that substations planned to be in service within 24 months should be identified, which would presumably be for stations under construction. b. R5 will then require a Physical Security plan to be in place within 120 days of identification, regardless of the current status of the station. c. Possibly adjust language to allow sites under construction to have the later of 120 days or the operation date of the station. 3. R1.2 should be reworded: "The TO shall identify the primary Control Center with operational authority of each Facility identified in the R1 risk assessment."4. R2, if the assessments are concurrent, could this be a joint effort, with the result being 1 report? 5. R2.1, "unaffiliated" needs some clarification. Is this unaffiliated with the TO in any way? Could the TO use their Planning Coordinator,

Organization	Yes or No	Question 2 Comment
		Transmission Planner or RC for the assessment, or do they need to seek out an entity from another region?
David Kiguel	No	1. For clarity suggest that the word “verify” be changed to “confirm” in sub-requirement 2.2 so that it reads: “The unaffiliated verifying entity shall either confirm the Transmission Owner’s risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s).2. Sub-requirement 3.1 should cover both, addition and removal of elements from the identified facilities list. Suggest changing to:”In the case of addition(s) to, or removal(s) from the identified Transmission stations or Transmission substations list developed under Requirement R1 and verified/modified according to Requirement R2, the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the change(s).”
Texas RE	No	1. For R1, the Transmission Owner is not the appropriate entity to conduct the type of transmission analysis that the requirement describes. It seems like a more logical process would be for the Transmission Planner to conduct an analysis of all substations meeting the applicability in 4.1.1.1 thru 4.1.1.4, and then, if the removal of a substation results in Cascading, instability, or uncontrolled separation, the TP will then notify the TO & TOP to conduct the security threat evaluation per R4 at only those substations identified by the TP.2. R1 - A “risk assessment” pertains to the physical security of Transmission Facilities while a “risk-based assessment” pertains to identification of Critical Assets and Critical Cyber Assets. The two phrases are too similar in meaning to each other, but possess differing meanings and intents.3. For R2, if the approach described in #1 is accepted, it may also satisfy R2 in those cases where the TP is independent from the TO. The independent verification would also be the responsibility of the TP, utilizing another TP, the PC, the RC, or an unaffiliated entity as described in the current language.4. For R3, if the approach described in #1 is accepted, the initial notification to the TOP would originate from the TP.

Organization	Yes or No	Question 2 Comment
South Carolina Electric and Gas	No	A) The FERC order directs that the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. It does not require verification of the specific or particular facilities identified. Therefore, SCE&G believes this section should be clarified and specifically state that the assessment itself (i.e. the methodology used by the owner or operator) be verified and not the facilities.B) SCE&G would like the drafting team to comment on the liabilities a NERC registered entity may assume as the third party when they are used to verify the risk assessment. Specifically, if in a future audit the owner or operator's assessment is found noncompliant, then would the independent NERC registered third party entity suffer any noncompliance as well? It is important for NERC registered entities to understand their compliance risks as third parties before they agree to perform independent verification of other entities assessments.
Florida Keys Electric Cooperative	No	o Comments: R1.1 - FKEC recommends that the 30 months timeframe be revised to 36 months as an annual focus is more straight forward than a 2.5 year focus and it's easier to track for internal programs and controls. 60 months should also be increased to 72 months to maintain the double timeframe that currently exists in the draft requirement. o R2 - The March 7 FERC order does not require an owner or operator to select an entity to verify its critical facilities assessment. The order uses the word "should," not "shall" or "require." The rationale for R2 is not accurate in this sense and should be revised to match the language in the order. Additional clarity is needed regarding what "verify" means in the standard. Guidance and rationale is helpful, but does not carry to legal weight of the standard language. o R2.1 - This section should explicitly include NERC and the Regional Entity (RE) as a potential verifying entity. NERC and the RE should be obligated to perform this role if the owner or operator requests them to do so under this standard. There should not be a direct or indirect requirement to mandate the registered entity to hire a third party to verify the assessment portion of the standard. If a registered entity wants to hire a third party, that should be a decision the registered entity makes, but is not required for standard compliance. If a third party, other than NERC or the RE, verification of the assessment

Organization	Yes or No	Question 2 Comment
		is required by the standard, then this is effectively two audits on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the standard is currently drafted. o Are there enough non-NERC/RE third parties available for what is likely to be a high demand for services, especially if there's a short time period as currently drafted? This is similar to the shortage of vendors that industry faced in theNERC facility ratings alert responses. o How is "transmission planning or analysis experience" judged by NERC compliance and enforcement? This language could be very difficult to comply with depending on the purview of the auditor.o If a registered entity hires a third party to develop and complete an assessement as required in the standard, can that third party also verify the registered entity's assessment? As drafted, the current standard could be read to require two third party entities to be hired - this would be unreasonable and the standard should be revised to clarify that only one third party would be needed to comply with the standard. o R2.2 - This requirement appears to require the third party entity to comply with language in the requirement. This does not seem to be appropriate or legal. The drafting team should revise the language to redirect the compliance burden to the NERC registered entity. In addition, the 90 day requirement could be difficult to comply with if there is a shortage of third party entities to contract with. Consideration should be given to revising this requirement to prevent a registered entity being found in violation of a requirement due to circumstances not under its control. o R2.4 - The words "exchanged with" should be changed to "made available to" in order to clarify that information may not be exchanged, but rather presented for viewing only, to a third party entity o R3.1 - The 7 day requirement appears to be unnecessarily short and not immediately necessary for BES reliability. FKEC believes 30 days is more appropriate timeframe for this requirement.
Black Hills Corporation Entities	No	Although BHC agrees with the overall approach, it has significant concerns regarding the use of the term "risk assessment" without a clear definition of intent. CIP-002 regulatory expectations in the Western interconnect for RBAM have consistently referred to the classic risk definition as "risk" times "probability". However, the further

Organization	Yes or No	Question 2 Comment
		expectation is that the probability of an event is assumed to be 100%, such that the "risk" them becomes equal to the "impact". CIP-014 does not currently lay out the same expectations, which could allow Transmission Owners and other affected (or unaffiliated) parties to disagree over the role of "proabability" in defining risk.This problem can be resolved in the CIP-014 draft by:1. leaving the risk assessment language as is, but adding the above statements about "probability" of occurrence being 100%, or2. changing all references of 'risk assessment' in the standard, to 'impact assessment', or3. leave the risk assessment language as is, but make it clear that CIP-014 is deviating from the historical CIP-002 RBAM definition of risk, such that the probability of the event can change the perceived risk (and that such an interpretation is congruent with the FERC order. This last option seems to be closest to the intent of Paragraph 8 in the FERC directive, but represents a significant departure from past NERC CIP guidance, and needs to be highlighted as such.As written, the TO has exclusive determination say in identifying applicable Transmission stations, substations and primary control centers. R2 speaks to a third party verification of that assessment, but Black Hills believes that coordination of the BES would be better served by having the TO & TOP reach a consensus on the assessment, prior to having the assessment validated by a third party.Requirement 2.1 directs the Transmission Owner to select an unaffiliated Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment. Firstly, Planning Coordinator does not appear in the NERC functional registry and should not be casually equated with the TP and RC functions; without first equating the Planning Coordinator to the PA function per the NERC glossary. Secondly, none of these NERC functional entity designations appear in the applicability section of the standard. Therefore, it can be assumed that the unaffiliated PC, TP, or RC are not obligated to conduct the assessment themselves, but rather the assessment is conducted by mutual agreement of the TO and unaffiliated PC, TP, or RC acting as third-party assessor. If this is not the correct assumption, then the PC, TP, and RC functions should be noted in the applicability section. If the Transmission Owner is affiliated with the Transmission Planner and Planning Coordinator, then the third-party review should be performed by the entity's Reliability Coordinator.The reference to "primary control center" is adequately

Organization	Yes or No	Question 2 Comment
		explained in the rationale section of R1, but confusion between it and “back-up control centers”, “emergency dispatch center”, and those control centers that can only monitor status seem to justify an up-front definition in the standard. Recommend that a special definitions section be added, or the term be clearly defined at its first instance in Section 3.R2.4 could benefit from some added guidance regarding the protection of sensitive or confidential information. Is the intent to employ the entity’s baseline confidentiality banner, or something more robust such as that required by CIP-003-3 R4 or CIP-011-1. The latter seems more appropriate for this CIP standard.
NCPA Compliance Management Operating Committee	No	Applicability is a key issue here. Comments to question 1 apply here as well. Why subject all Transmission Owners who may meet the "medium impact under CIP-002-5.1 to a third pary review for all medium impact stations and substations when only 30 stations will be affected (please define the difference between a Transmission station and Transmission substation. A third party review is appropriate for the 30 or so stations involved, but seems excessive for all owners to obtain third party review when the expectation is that 30 out of 55,000 are te ones of real concern. NCPA elected to have an independent third party risk asssessment and vulnerability assessment performed at its 5 generation facilities and control center. The assessment cost is approximately $150K and takes about 9 months to complete. NCPA'a assets are also low impact. The risk assessment, vulnerability and threat assessments and development of the security plans are able to performed by the same third party reviewer that flows together without interruption. The way in which the requirements are structured creates alot of consultants or third party reviewers running around, with 99% of them stopping work after R3. How much money will be spend for that and for what purpose? There has to be a better way segregate the 99% from the 1% where the real concern is.
Flathead Electric Cooperative, Inc.	No	Do not support the third party requirements, seems like a full employment effort by security consultants and others. Administratively burdensome and time-consuming at the expense of actual security improvements.

Organization	Yes or No	Question 2 Comment
Florida Municipal Power Agency	No	FMPA commends the efforts of the SDT to lay out an excellent process for risk assessment in accordance with the FERC Order in such a short time frame. We only have few comments. WHAT DOES “CONTROL CENTER” MEANIs there a signifance for not using the capitalized term of Control Center throughout the standard? It seems to FMPA that the defined term “Control Center” ought to be used. If the intent is that “control center” and “Control Center” mean two different things, then, what does “control center” mean? If the intent is to include large TOs that may be part of a large TOP, such as a large utility in an RTO, that do not have Control Centers; then, FMPA recommends using a different term such as “the location of the SCADA system that has remote control of breakers associated with the identified substation/station” or similar might avoid confusion.WHAT DOES “UNAFFILIATED” MEANThe term “unaffiliated” may be a source of ambiguity and conflict without further definition. For instance, dictionary.com defines affiliated as: “being in close formal or informal association; related” So, this would imply that peer members of the Transmission Forum are affiliated, which we do not believe is the intent of the SDT. FMAP believes the SDT’s intent is as Black’s Law Dictionary defines affiliate: “1. A corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or sibling corporation. 2. One who controls, is controlled by, or is under common control with an issuer of a security.”; which would mean that peers within the Transmission Forum are unaffiliated, but subsidiaries of a company are affiliated, or members of a Joint Action Agency are affiliated. It also aligns with FERC’s definitions for Affiliate in their market based rates regulations 18 C.F.R. 35.36(a)(9) and in the Pro Forma OATT. FMPA suggests using a footnote to clarify use of the term unaffiliated, such as “Use of the term unaffiliated is in relation to Black’s Law Disctionary defition for affiliated: ‘1. A corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or sibling corporation. 2. One who controls, is controlled by, or is under common control with an issuer of a security.’”PROPER QUALIFICATIONS FOR RISK ASSESSMENT VERIFICATIONFMPA appreciates the challenges of defining qualification for independent verifiers while offering registered entities a broad choice for selection. We interpret that

Organization	Yes or No	Question 2 Comment
		requirements R2 and R6 grant the applicable entity sole authority to choose the 3rd party verifier as long as they meet the qualifications contained within those requirements. Is FMPA correct in that interpretation?CHANGE MANAGEMENT OF THE RISK ASSESSMENTThe standard is somewhat ambiguous on what happens if the responsible entity chooses to revise it's risk assessment of R1 sooner than the required 30 or 60 calendar months. Does every minor revision to the risk assessment require another 3rd party review? Or would only major system changes (e.g., due to adding a major new investment in the power system like a new 500 kV line) require review? Or regardless of system changes, would the review occur once every 30/60 months? FMPA suggests clarification to R2 to say that minor revisions to the risk assessment due to minor power system changes in between the 30/60 month periods do not need a separate 3rd party verification.
Georgia System Operations Corporation	No	GSOC supports the comments submitted by both Georgia Transmission Corporation (GTC) and NRECA
Georgia Transmission Corporation	No	-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard.-GTC is concerned that the language of the standard and rationale around the use of the term "unaffiliated" in R
Hydro QuÃ©bec TransÃ‰nergie	No	Hydro-Quebec TransEnergie (HQT) agrees with this approach but requests that the SDT remove the term "unaffiliated" from Requirements R2 and R6.1HQT notes that the term "unaffiliated" is not used in FERC Order 146. Paragraph 11 of the Order states "In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator." Moreover, it appears that it is not FERC's intent to introduce this restriction regarding the choice of a third party. HQT therefore believes that the use of the term "unaffiliated" goes above and beyond what was stipulated in the FERC Order.Furthermore, the term "unaffiliated" is not required because the NERC Reliability Functional model already ensures the independence between the TO/TOP and the verifying entities (RC, PC and TP) that the SDT is seeking in the draft standard. The Reliability Model uses the term

Organization	Yes or No	Question 2 Comment
		"functional entity" to apply to a class of entities without making reference to specific organizations that register as functional entities.For some Canadian jurisdictions, the use of the term "unaffiliated" renders the standard more stringent due to the fact that certain Canadian entities such as Hydro-QuÃ©bec TransÃ‰nergie are simultaneously registered as TO, TOP, PC and RC. For integrated modeled entities, the restriction of available options that would otherwise be available (such as selecting a PC, TP or RC for the risk assessment verification under R2), makes it difficult to identify an entity with the required expertise capable of performing the reviews stipulated in the standard. HQT believes that the risk assessment of a TO should only be verified by the RC or the PC that has supervision (real-time or planning) over the said TO's assets because only the RC or the PC can ensure a comprehensive approach to critical facility identification that considers the reliability of an entire area.For these reasons, HQT believes that the expression "third party" alone is sufficient and consistent with the expressed concerns in the FERC Order.
Rayburn Country Electric Cooperative	No	I agree with the risk assessment in concept, the standard has far too many requirements and sub requirements to accomplish the task. Since initial analysis apparently this has already been done for the "High Risk" stations, a more efficient approach would be for the RC to perform the analysis based on the criteria mentioned to validate findings and find any second contingency facilities that may not have been identified. Since the RC is the "Reliability Coordinator", this is your third party identifying facilities without bias... Determinations will be based on an engineering basis utilizing standard uniform criteria across North America.The same analysis occurs for all entities within all regions, no variations this would yield consistency! Then the RC notify the entities that they have facilities that have been identified. (much like other NERC standards)Thus the information on which facilities have been identified would disseminated and controlled in a much more secure and better controlled environment while still maintaining the quality and consistency of the study needed.

Organization	Yes or No	Question 2 Comment
New Brunswick Power Corporation	No	In general, a TO may not have the capability to conduct a risk assessment to determine if an identified facility that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Such an assessment requires a wide area view of the Interconnection. It is proposed that the risk assessment be conducted by a PC, or RC for the area in which the facility is located. Doing so would satisfy the third party verification requirement as the TO would not be conducting the analysis. It is the opinion of NB Power that the technical details concerning the transmission analysis, in the proposed standard, are overly vague. This could lead to an inconsistent application of the analysis between entities as well as create obstacles with consensus concerning the proposed 3rd party verification. NB Power suggests a clear analysis methodology be drafted to establish a common basis for study criteria with the ability for each entity to apply additional specific requirements for their respective area.For corporate bodies, such as a vertically integrated utilities, that are registered as the RC, TOP, PC, TP and TO for a particular area, it is the opinion of NB Power that the requirement for unaffiliated 3rd party verification is overly stringent and of little value. The verifying party is limited to entities that have transmission planning or analyses experience, or, are registered as a PC, TP, or, RC from an adjacent area. NB Power is of the view that there are no unaffiliated entities with sufficient knowledge of the local transmission system to provide a meaningful verification within a 90 day period.As a government owned utility, NB Power is required to follow procurement processes which will make it difficult to meet the 90 day period for the third party verification. NB Power is also concerned that it could be non-compliant with the requirement if the third party fails to meet its obligation. While NB Power can mitigate the financial risk of that event it would still result in a recorded non-compliance.It is the opinion of NB Power that the proposed standard does not sufficiently address a disagreement resolution process between the TO and the unaffiliated verifying 3rd party in requirement R2.3. NB Power believes that documenting the technical basis for not following the recommendations of the unaffiliated verifying 3rd party without guidance on what constitutes valid technical reasons presents a compliance and enforcement gap where both the entity

Organization	Yes or No	Question 2 Comment
		and an auditor may not be able to come to consensus. NB Power suggests the SDT develop guidance concerning compliance and enforcement of this requirement indicating acceptable technical reasoning for not following the 3rd parties recommendations.
Kansas City Power & Light	No	In R1, we have concerns about the ambiguity associated with the term "assessments". Can you provide examples of the types of assessments that would be acceptable to meet R1 and that would be CIP audit worthy in the future. We have the same concern in R2 with the term "third-party". Will there be a list of pre-approved third party contractors or will the RE's review and approve a third-party at the request of the registered entity prior to their use in the verification process as described in R2?
Central Hudson Gas & Electric Corporation	No	In regards to R2.2 as currently drafted, the unaffiliated verifying entity should have to ensure verification within 90 days and not the TO, since it is that entity performing the verification.In regards to R2.3 as currently drafted, there appears to be a lack of an appeals process in cases of disagreement between the unaffiliated verifying entity and the TO concerning the recommendations formulated by the unaffiliated verifying entity.
ITC	No	ITC believes that limiting physical security requirements in CIP-014-1 to those substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection does not adequately raise the bar for critical infrastructure protection of valuable and strategic substation assets. Indeed, those substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection certainly warrant additional physical protection. However, so does any other substation asset deemed critical through the cybersecurity initiatives already in place through applicable companion Reliability Standards. If a substation is deemed critical through the CIP-002-5 screening process, it at a minimum, should warrant an “evaluation of potential threats and vulnerabilities of a physical attack to the facilities (CIP-014-1 R4). ITC supports using the brightline test criteria of CIP-002-5, as noted in

Organization	Yes or No	Question 2 Comment
		our comments for Question 1, above, but also feels that all substation assets passing the brightline test criteria should move directly to R4 for an assessment of threats and vulnerabilities, eliminating the need for R1 and R2. This has the benefit of using industry-vetted, bright-line criteria that creates valuable consistency between physical and cybersecurity assessment practices. This does not undermine the Commission's three-part requirement for addressing physical security, but rather allows the responsible entity to meet the Commission's first requirement (identification of critical assets) by using the same critical asset identification criteria for physical and cybersecurity. ITC believes if a facility is critical enough to warrant cybersecurity protection, then it should also warrant physical security and that the requirements should not be so narrowly defined to ignore the importance of substations beyond those few whose individual loss causes cascading outages. This simplified approach avoids potential contradictory and duplicative requirements between existing CIP standards, and would allow this standard to focus exclusively on physical security aspects and not on asset identification
Los Angeles Department of Water and Power (LADWP)	No	LADWP requests the Drafting Team to make the following changes:- For R1, additional time is needed to make sure studies are fully completed and reviewed by TO and its applicable governing authorities. Add ", which is due 30 calendar days after the effective date of the standard" to R1 as follows:"R1. Each Transmission Owner shall perform an initial risk assessment, which is due 30 calendar days after the effective date of the standard and subsequent risk assessments of its Transmission stations and Transmission substations (existing and....."- For R1, change "24 months" to " 30 months" to align the assessment with subsequent risk assessments.- For R2.1, The term "unaffiliated" needs to be defined in the standard to avoid any misinterpretation. - For R2.2, change the "90 calendar days" to "120 calendar days" to allow sufficient time to resolve differences if Planning Coordinator, Transmission Planner or Reliability Coordinator are addressing other deadlines.
Dominion	No	Measure M1 - R1.2 -- Measure M1 does not address sub-requirement R1.2 which requires the Transmission Owner to identify the primary control center that

Organization	Yes or No	Question 2 Comment
		operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment. Dominion recommends the SDT determine whether M1 should include the control center.R2.3 - Relative to R2.3, Dominion does not agree that the TO should have to document the technical basis for retaining assets that have been suggested for removal by the third party.R3 - Dominion suggests R3 be revised to strike the words 'and verified according to Requirement R2', and changing R2 to R1.2 in the next two instances where R2 is mentioned. This is due to the reason there is nothing included in R2 that requires verifing primary control centers.
MISO	No	MISO recognizes that the Commission mandated third-party verification of the risk assessment required under R1, however the current language of R2 requires modification to address several concerns MISO has with regard to its potential role as a verifying entity. While MISO has every confidence that it can perform risk assessment verifications in a safe, responsible, and accurate manner, the combination of a high number of requests requiring verification within a relatively short period of time presents some concerns to MISO regarding its resource allocation and availability. In particular, MISO recommends that the SDT add language limiting the universe of Transmission Owners/Operators that can seek verification from a particular verifying entity (potentially by geographical region or contractual or functional relationship) as well as modify the 90 day requirement to take into account that a single entity may have more requests than it can feasibly complete in such a short time period. An example of language that MISO could support is language that would allow a verifying entity and the requesting Transmission Owners/Operators to agree upon an appropriate completion date beyond the 90 days where the 90 day period will not allow completion of a robust verification due to resource constraints by the berifying entity. Finally, MISO respectfully requests that the SDT consider adding language to Requirement R2 that would allow verifying entities to limit liability related to both enforcement actions within the jurisdiction of FERC, NERC, and the Regional Entities and other actions that could be brought against verifying entities in other jurisdictions and venues unless it is shown that the entity lacked good faith or was grossly negligent.

Organization	Yes or No	Question 2 Comment
Omaha Public Power District	No	OPPD, in general, is in agreement with the approach taken in CIP-014-1 for identifying critical Transmssion stations and substations. We agree that risk assessment be conducted using transmission planning analysis, however, we suggest that this standard identifies what applicable planning analysis is used. We think the TPL standards provide the ability for the Transmission Owners to determine the worst case extreme event for identifying critical transmission stations and substations. OPPD believes that leaving R1 open and vague would encourage various interpretations of the term 'transmission planning analysis' as it applies to a 'risk assessment'. This may place the industry and the ERO in the same position as they were with the ealier versions of CIP-002 and the associated RBAM. Referencing the applicable TPL standards attemptes to remove some of this ambiguity by providing a more concise framework to evaluate those worst case extreme events. Furthermore, since TPL standards associated transmission planning analyses are performed in coordination with the PCs, risk assessment verification by PCs/RCs will not require a re-assessment of a study that has already been performed. We suggest that the SDT consider specifically defining 'transmission planning analysis' to avoid repeat of the uncertainty and vagueness associated with the CIP-002 RBAM. OPPD asks the SDT to consider revising requirement R1 as following: R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify any Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The transmission planning analysis shall be based on the applicable portion(s) of the TPL standards and specifically referenced. [VRF: High; Time-Horizon: Long-term Planning]1.1. Subsequent risk assessments shall be performed: o At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered

Organization	Yes or No	Question 2 Comment
		inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or o At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. 1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.
Ciy of Garland	No	R1 - The auditors should be limited to verifying that a study was completed using the assumptions agreed to by both the TO and the reviewer. The auditor should accept any study and assumptions jointly agreed to by the TO and the reviewer without requiring additional engineering justifications as to why one type of study was used instead of the auditor's preferred methodology. To summarize and echo FERC Commissioner Norris in his clarifying statement, included with the FERC Order that is the basis of the CIP-014 Standard, that if the Planning Studies indicate a transmission solution that would cause the substation to no longer cause the cascading outage that the transmission project could be initiated in lieu of the security plan. The additional transmission solution would potentially add other operational benefits other than just "security" and therefore may be more practical than the security plan in R4 through R6. In the guidance document, statements should be made that a TO may make additional planning studies at any time prior to the 30 months and if the third party reviewer concurs the updated study no longer shows a cascading event, whether due to changing grid conditions or system improvements, the standard would no longer apply including the continued implementation of the security plan. The TO should also notify the owner of the primary control center the substation no longer causes a cascading event.R2 - Timelines to complete third party verification under R2.2 and third party review under R6.2 are both too short. Increase 90 days to 120 days or 180 days. a. Verifying entities may recommend that the Transmission Owner conduct additional planning studies to confirm asset identifications such as interactions between BES

Organization	Yes or No	Question 2 Comment
		Elements in adjacent Transmission Owner footprints. A 90-day time limit may not provide sufficient time to conduct and verify a revised or supplemental BES assessment.b. For security reviews, conducting an accurate and meaningful review with sound recommendations applicable to a specific TPs facts and circumstances may require additional time for assessment and discussions with the TO. A short review window is more likely to lead to misunderstandings, or disagreements with the TO which in turn could lead to discrepancies or improper application of the assessment requiring justification. This could cause the reviewer to avoid making recommendations that should be considered by the TO and improve the TO's assessment.c. As currently written, it appears if the TO disagrees with the reviewer's comments and writes a technical reason why he believes the original conclusion were correct, the recommendation(s) by the reviewer may be rejected and the TO's decision is final. Although I agree with this position it may be interpreted differently by the auditors. Please clarify which was the intent of the SDT.R3 - No comments
Bonneville Power Administration	No	R1 Terminology: Although the term "risk assessment" in this section is in alignment with language in the FERC order, BPA recommends that it be revised to consequence or impact assessment. This is a physical security standard, and the term risk assessment should be reserved for the physical security risk section of this standard and align with security industry use of the term. BPA believes the basic intent of R1 is to identify substation facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection can create unacceptable consequences to the BES and not to assess risk of the event happening.Also, BPA suggests that additional sub-requirements be added to provide clarity on what system conditions and performance criteria or methodology need to be considered in order to determine what stations and substations will be deemed critical. Similar language found in existing standards would be helpful. Examples: FAC-010-2.1 (System Operating Limits Methodology for the Planning Horizon), R1-R3; FAC-013-2 (Assessment of Transfer Capability in the Near-Term Planning Horizon), R1; TPL-001-4 (Transmission System Planning Performance Requirements), R1-R6; TPL-004-0a (System Performance Following Extreme BES Events), R1."R1 1.1. Subsequent risk

Organization	Yes or No	Question 2 Comment
		assessments shall be performed:" BPA recommends revising R1 1.1 to: “Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment.” Justification: This would consolidate the two bulleted actions and make them equally applicable. BPA has been doing substation facility impact and security risk assessments for the past 15 years and our experience is that the criticality of a substation facility does not change once ranked; once it is determined critical it will always be critical particularly when information is used in a physical security risk assessment. A 5 year interval would be a more appropriate interval for this type of assessment as it would always be case of identifying new facilities and not excluding ones previously identified."R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. [VRF: Medium; Time-Horizon: Long-term Planning]"BPA recommends revising R2 first sentence to: "R2 Each Transmission Owner shall verify the impact assessment performed under requirement R1 by a third party entity other than the owner or operator." Justification: This fully aligns with the requirements of the FERC order by using the requirements of the FERC order. BPA believes the introduction of a requirement of an unaffiliated reviewer is reaching beyond the requirements established by the FERC order, and this requirement will dilute the quality of an impact assessment. It will limit the types of entities that can perform an independent review, and directs use of resources that may not be capable of assessing all physical risks within an electrical facility. BPA proposes that the word unaffiliated be removed from this standard and replaced with language that describes the degree of separation from the facility owning entity to be considered a third party entity other than the owner or operator. Based on the definition provided in this draft “unaffiliated” is especially troublesome for federal government-owned transmission networks and facilities because it could be interpreted as excluding the entire federal government from eligibility as a third party entity to the federal government transmission owner.Also, BPA believes industry peer reviews should be

Organization	Yes or No	Question 2 Comment
		encouraged and considered as meeting the requirement. Reviews by industry peers are known to be beneficial to the entity receiving the review and for the entity performing the review or audit. Enabling industry peer reviews would not only meet the intent of an independent review but also accelerate continuous learning and translation of the most effective security approaches into widespread use. Please note that the FERC order only recommends this verification as it is stated as “should” and not as “shall.”"R.3 For a primary control center(s) identified by the Transmission Owner according to Requirement R1 and verified according to Requirement R2 that is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. [VRF: Lower; Time-Horizon: Long-term Planning]" BPA recommends revising the 7 day requirement in R3 and R3 3.1 to 30 calendar days. Justification: This information is not that time critical at this stage, and one week will not be enough time to complete all notifications.
National Rural Electric Cooperative Association (NRECA)	No	R1.1 - NRECA recommends that the 30 months timeframe be revised to 36 months as an annual focus is more straightforward than a 2.5 year focus and it’s easier to track for internal programs and controls. 60 months should also be increased to 72 months to maintain the double timeframe that currently exists in the draft requirement.R2 - The March 7 FERC order does not require an owner or operator to select an entity to verify its critical facilities assessment. The order uses the word “should,” not “shall” or “require.” The rationale for R2 is not accurate in this sense and should be revised to match the language in the order. Additional clarity is needed regarding what “verify” means in the standard. Guidance and rationale is helpful, but does not carry to legal weight of the standard language. R2.1 - This section should explicitly include NERC and the Regional Entity (RE) as a potential verifying entity. NERC and the RE should be obligated to perform this role if the owner or operator requests them to do so under this standard. There should not be a direct or indirect requirement to mandate the registered entity to hire a third party to verify the assessment portion of the standard. If a registered entity wants to hire a third party, that should be a decision the

Organization	Yes or No	Question 2 Comment
		registered entity makes, but is not required for standard compliance. If a third party, other than NERC or the RE, verification of the assessment is required by the standard, then this is effectively two audits on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the standard is currently drafted. Are there enough non-NERC/RE third parties available for what is likely to be a high demand for services, especially if there's a short time period as currently drafted? This is similar to the shortage of vendors that industry faced in the NERC facility ratings alert responses. How is "transmission planning or analysis experience" judged by NERC compliance and enforcement? This language could be very difficult to comply with depending on the purview of the auditor. If a registered entity hires a third party to develop and complete an assessement as required in the standard, can that third party also verify the registered entity's assessment? As drafted, the current standard could be read to require two third party entities to be hired - this would be unreasonable and the standard should be revised to clarify that only one third party would be needed to comply with the standard.R2.2 - This requirement appears to require the third party entity to comply with language in the requirement. This does not seem to be appropriate or legal. The drafting team should revise the language to redirect the compliance burden to the NERC registered entity. In addition, the 90 day requirement could be difficult to comply with if there is a shortage of third party entities to contract with. Consideration should be given to revising this requirement to prevent a registered entity being found in violation of a requirement due to circumstances not under its control. R2.4 - The words "exchanged with" should be changed to "made available to" in order to clarify that information may not be exchanged, but rather presented for viewing only, to a third party entityR3.1 - The 7 day requirement appears to be unnecessarily short and not immediately necessary for BES reliability. NRECA believes 30 days is more appropriate timeframe for this requirement.
PNM Resources	No	R2.1 could place an unreasonable burden on entities registered as PC and TP. R2.2 which puts the burden of ensuring that the unaffiliated third party review is completed

Organization	Yes or No	Question 2 Comment
		in 90 calendar days on the TO. As a TO an entity cannot compel another registered entity or third party to complete anything with a specified amount of time and according to the RSAW if the verification is not completed within 90 days then the TO is not in compliance with the requirement. The standard should require registered NERC entities to complete the unaffiliated review and those entities should be included as applicable functional entities and R2.2 should apply to the reviewing entity.
PNM Resources	No	R2.1 puts an unreasonable burden on registered PC and TP. R2.2 which puts the burden of ensuring that the unaffiliated third party review is completed in 90 calendar days on the TO. As a TO PNM can't force another registered entity or third party to complete anything with a specified amount of time and according to the RSAW if the verification is not completed within 90 days then the TO is not in compliance with the requirement. The standard should require registered NERC entities to complete the unaffiliated review and those entities should be included as applicable functional entities and R2.2 should apply to the reviewing entity.
Tri-State Generation and Transmission Association, Inc.	No	Rather than making it the Responsible Entity's responsibility to find a third party to verify its assessment, Tri-State believes it would better suit the industry and the standard if R2 required either the Reliability Coordinator or Regional Entity to request TO's assessments on an intervaled basis. This meets the requirements of the March 7 FERC Order. Allowing the requirement to be broad enough to allow third party paid consultants with "transmission planning or analysis experience" creates a conflict of interest and contradicts the draft standard's requirements for the use of "unaffiliated third part[ies]". If third party - other than NERC or the RE - verification of the assessment is required by the standard, then this is effectively two audits (and two 3rd party assessments) on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the standard is currently drafted.Tri-State recommends that rather than 30 months and 60 month risk assessment intervals for R1.1, they should be a more straightforward 36 months and 72

Organization	Yes or No	Question 2 Comment
		months respectfully in order to be consistent withnormal auditing time periods of three years. This will make the intervals easier to track with internal programs and controls.
Bureau of Reclamation	No	Reclamation agrees with this approach. However, to promote consistent identification of critical facilities within an interconnection, Reclamation believes that the third-party review should be conducted by the Transmission Owner (TO)'s Planning Coordinator or Transmission Planner. If the Transmission Owner is also the Transmission Planner and Planning Coordinator, the third-party review should be performed by the Reliability Coordinator. Reclamation also suggests that the drafting team modify the term "risk assessment" to "BES impact assessment." In the physical security community, the term "risk assessment" generally refers to "The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel." See ASIS International, General Security Risk Assesment Guideline (2002), http://www.scnus.org/local_includes/downloads/9200.pdf. In its filing to FERC, NERC can explain that it adopted the term "BES impact assessment" so it is clear that the initial evaluation is of risk to the BES if the substation is rendered inoperable or damaged. Reclamation also recommends revising R1.1 to require subsequent risk assessments every 60 months for all Transmission Owners. Reclamation believes that periodic risk assessments are necessary, but has not seen evidence that the costs associated with updating risk assessments every 30 months rather than every 60 months would provide commensurate reliability benefits. Reclamation recommends that the drafting team update R1.1 to state, "Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment."
SERC CIPC	No	Recommend that the Transmission Planner perform the risk assessment in R1 instead of the Transmission Owner. Need further clarification and examples for the term "unaffiliated". Would "peer" reviews studies that do not have a single registered entity with controlling interest suffice as an "unaffiliated" third party reviewer? What role

Organization	Yes or No	Question 2 Comment
		does the SDT envision the ERO (including regional entities) playing in the review process?
Foundation for Resilient Societies	No	Same answer as provided to Question 1.
Southern California Edison Company	No	SCE has concerns with both Requirement R1 and Requirement R3. In Requirement R1, SCE recommends that the verbiage be changed from “...that if rendered inoperable or damaged could result in widespread instability...” to “...that if damaged to the point of being rendered inoperable could result in widespread instability..." SCE requests this change to reduce ambiguity in the application of the word "damaged." In addition, language should be added to R1 that specifies: “...system instability such as uncontrolled separation or cascading within 15 minutes of compromise...,” as a 15-minute window would align with criteria in the CIP standards used to determine critical facilities. In the guidance section for R1, SCE would suggest changing the text from “...remedial action schemes (RAS) or special protection systems (SPS)” to “...special protection systems (SPS)...,” because as used in the NERC Glossary of Terms, a RAS is included as a type of SPS. In addition, SCE requests that R1 be revised to include specific examples and criteria for the risks to be measured. For instance, SCE believes the following could be among the examples and criteria specifically included: (a) Thermal overloads beyond facility emergency ratings; (b) Voltage deviation exceeding Â± 10%; (c) Cascading outage/Voltage collapse; and (d) Frequency below under-frequency load shed points.With respect to Requirement R3, SCE requests that additional guidance be provided on how a "primary control center" should be identified, as that term in used in both Requirements R1.2 and R3. SCE also asks the team to consider changing the notification requirement in R3 from seven(7) to thirty(30) days in order to allow sufficient time for the transmission owner and transmission operator to perform the required communication.

Organization	Yes or No	Question 2 Comment
Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.	No	Specifically, Vectren recommends that R2 be removed from the draft standard, for the reasons set out in this Comment. And that an approach similar to that used for evaluation of designations under CIP 002 Version 3 be adopted for review of the required risk assessment. Vectren urges FERC and NERC to designate registered Planning Coordinators, Transmission Planners, or Reliability Coordinators as the approved verifiers for entity risk assessments AND to establish clear criteria for verifiers, so that NERC auditors can apply a uniform set of criteria to their after the fact assessment of verifier qualifications. As written, these provisions lack the specificity necessary to provide clear direction to entities, increasing the risk of later non-compliance. Such a risk is ironic and unacceptable in requirements that purport to provide a review of risk assessments. Under these draft requirements entities have no assurance that any third party verifier they might select will be considered "qualified" by FERC, NERC or NERC auditors who might review the results later - leaving entities at grave risk of compliance violations if FERC, NERC or any other regulatory body later disagrees with the entity's selection of a third party verifier. Vectren strongly urges NERC and FERC to establish criteria for those who might seek to be designated third party verifiers, rather than leave assessment of qualifications to an after the fact review during a NERC audit or spot check. A lack of certainty leads here by necessity to a lack of confidence in the result, which Vectren surmises was not the intent of FERC or the drafters.
Southwest Power Pool Regional Entity	No	SPPRE believes that greater clarity is required with respect to the risk assessment to be performed. At a minimum an extreme contingency study needs to be performed that takes out the entire facility, all voltages present. The study should also not consider any operating guides or other mitigation when evaluating the impact of the outage. In Section 2.3 technical basis should be changed to engineering basis. Additionally, the unaffliated verifying entity should not be the party performing the original study, under the principle that an auditor cannot audit ones own work; to do so would not be consistent with the expectation of verification by an unaffiliated entity.

Organization	Yes or No	Question 2 Comment
Salt River Project	No	SRP supports comments submitted by APPA with the following additions:The time frame for completion of the initial risk assessment required in Requirement R1 is not identified in the standard, only in the implementation plan. This may be a point of confusion for entities that fail to fully read and understand the implementation plan. If possible, could the drafting team revise the language of Requirement R1 to make this clear?The periodicity of the risk assessments required by Requirement 1 and the time frame that the risk assessments appear to not align. The risk assessment is required to include Transmission stations and Transmission substations that exist as well as those planned to be in service within 24 months. However, the periodicity for conducting future risk assessments is every 30 calendar months or every 60 calendar months if the prior risk assessment did not identify any Transmission stations or Transmission substations. This potentially leaves a gap of six to 36 months where facilities may not have been assessed.In R2 it is not clear that the primary control center must also be verified, but in subsequent requirements it implies or states that it should be. If the intent in R2 is that the primary control center should also be verified, then it should state so in R2.2 and R2.3 in addition to stating stations and substations.Third Party Verifiers:SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered

Organization	Yes or No	Question 2 Comment
		Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities.Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers.Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.

Organization	Yes or No	Question 2 Comment
FortisBC	No	The audit provides an independent review of an entity's application of the standard and therefore, an additional third party review should not be required as described in R2.It is agreed that if a null set is identifed, the rest of the standard does not apply.
Western Electricity Coordinating Council	No	The periodicity for risk assessments and the forward looking time frame for including planned substations do not match. Entities are only required to consider stations planned in the next 24 months, while the risk assessment is applied on a 30 month cycle, or a 60 month cycle if the entity previously identified a null list of applicable stations. This potentially leaves a 6 to 36 month gap. We would encourage the SDT to match the periodicity of the application to the planned implementation window or include language requiring any new asset be evaluated under R1.WECC notes that the time frame for completion of the initial risk assessment required in Requirement R1 is not identified in the standard, only in the implementation plan. This may be a point of confusion for entities that fail to fully read and understand the implementation plan. WECC suggests that at a minimum NERC and the Regions engage in extensive outreach to ensure that the Transmission Owners are aware of this and that if possible the drafting team revise the language of Requirement R1 to make this clear.Requirement R2, part 2.2 appears to be assigning responsibilities to the unaffiliated verifying entity (registered Planning Coordinator, Transmission Planner, or Reliability Coordinator) yet these entities are not included in the applicability section. If these entities are to be held accountable in the standard for actions, why are they not included in the applicability section?
Northeast Power Coordinating Council	No	The Rationale Box for Requirement R2 stipulates that "'unaffiliated' means that the selected verifying entity cannot be a corporate affiliate (i.e., the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission o(O)wner)." This conflicts with Requirement R2 Part 2.1 which lists "A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or An entity that has transmission planning or analysis experience" as those qualifications for an unaffiliated verifying entity. Clarification is needed that an Independent System

Organization	Yes or No	Question 2 Comment
		Operator that has operating authority over an entity is eligible to be the unaffiliated verifying entity.
None	No	The SDT has not factored in the resiliency concerns stated in the FERC order. Many of the facilities selected by the initial screening process will have long lead time equipment that if damaged will be out of service for several months. The assessment process needs to consider the operational risks during the time that the TO is waiting for replacement equipment. R1 should be amended to include the following sub-requirement.If the facility being studied has long lead time items, i.e. 4 months or greater, the study must include an N-1 analysis for the widespread instability, uncontrolled separation, or Cascading within an Interconnection test.In addition, the premise for this standard is a physical attack resulting in faulted equipment. There is no mention of the assessment being conducted for the Facilities under fault conditions and in many cases under delayed clearing.R1 should be amended to include the following sub-requirement.The analysis of the subject Facility must include dynamic simulation of faulted conditions with delay cleared for the most severe contingency within the Facility.The phrase "instability, uncontrolled separation, or Cascading" is core to the definition of Interconnected Reliability Operating Limit (IROL). Every RC and PC has an IROL methodology under the FAC standards. R1 should be amended to include the following sub-requirement.The test for instability, uncontrolled separation, or Cascading must be consistent with the IROL methodology established by PCs and RCs under FAC-010 and FAC-011.
SPP Standards Review Group	No	The Standard intentionally does not provide specific methodologies regarding the type of analyses needed to be conducted for the assessments in R1. This leaves the door open to very different interpretations across the industry. We suggest the drafting team consider specifying analyses such as those contained in the TPL standards. This would eliminate confusion within the industry and provide clear direction for those conducting the analyses. We suggest adding the following sentence at the end of R1. “These analyses will include consideration of the entire loss of the Transmission stations and Transmission substations specified in Applicability Section 4.1.1 taken

Organization	Yes or No	Question 2 Comment
		individually, one at a time." While not specifically referencing the TPL standards (currently enforceable TPL-004-0a, R1 and TPL-001-4, R3 to be enforced in 2016) which cover the loss of switching stations and substations, this language provides guidance regarding the type of analyses to be conducted in the assessments. We strongly suggest that the SDT expand on this addition to R1 in the guidance document to provide needed clarification to the industry.
Westar Energy	No	The Standard intentionally does not provide specific methodologies regarding the type of analyses needed to be conducted for the assessments in R1. This leaves the door open to very different interpretations across the industry. We suggest the drafting team consider specifying analyses such as those contained in the TPL standards. This would eliminate confusion within the industry and provide clear direction for those conducting the analyses. We suggest adding the following sentence at the end of R1. "These analyses will include consideration of the entire loss of the Transmission stations and Transmission substations specified in Applicability Section 4.1.1 taken individually, one at a time." While not specifically referencing the TPL standards (currently enforceable TPL-004-0a, R1 and TPL-001-4, R3 to be enforced in 2016) which cover the loss of switching stations and substations, this language provides guidance regarding the type of analyses to be conducted in the assessments.
Nebraska Public Power District	No	The third party verification is unnecessary and should be deleted from the standard. There is no other unaffiliated third party that has knowledge and expertise comparable with the incumbent Transmission Planner who develops the detailed models, performs the reliability assessments, and develops the required long term plans for the Transmission Owner on an annual basis. If the verification remains in the standard, 90 calendar days is not a sufficient amount of time to complete verification. A Transmission Planner may ask a Planning Authority (PA) to review its risk assessments, but the same PA will likely be asked to review multiple utilities. Recommend at least 180 days to complete the verification.

Organization	Yes or No	Question 2 Comment
Encari	No	There should be a strong, rebuttable presumption that an applicable Transmission Facility requires physical protection owing to its classification under the bright-line "medium impact" rating criteria under CIP-002-5.1 (which is repeated in the Applicability section of CIP-014-1 for Transmission Facilities). The utility of a risk assessment could be recognized, however, as justification for rebutting the presumed need for a set of mandated physical security measures.
Consumers Energy Company	No	We agree to the approach, however, our concern is around protection of information shared between the entity and the third party. There should be a requirement within the standard that requires the third parties to protect the information and not leave it up to the entities.
Cooper Compliance Corp	No	We do not support the Standard as written today. We agree with the scope and content of the SAR. However, we are concerned with Requirement 6. Requirement 6 requires entities to seek out third parties to review their new physical security protection plans. We don't believe that entities should be obligated to seek assistance from third party individuals. This includes consultants or another unassociated entity. The purpose of the regions, NERC, and FERC are to provide a review of an entities compliance to Standards through the audit and self-certification process. No other Reliability Standards require an entity to use third parties to determine compliance or sufficiency of compliance documentation. We believe that this obligation may place some entities in difficult financial situation and could have a negative impacts in assuring that proper third party entities are being used. Should FERC, NERC, or WECC determine that entities are not following the spirit of the Standard than they may request a modification in a future Standard revision. We will support this Standard if Requirement 6 is removed.
Independent Electricity System Operator	No	While the proposed R1 to R3 collectively meet the FERC requirements for having an entity to identify the critical facilities and having the assessments of such identification verified, we believe it is more appropriate that the 3rd party verification be performed by NERC registered entities only (which could be the Reliability Coordinator, Planning

Organization	Yes or No	Question 2 Comment
		Coordinator or Transmission Planner). An entity that has transmission planning or analysis experience may only have an outside equivalent representation of the BES and their ability to conduct an analysis with a "wide area" view of consequences may not be possible. As such, we suggest to revise Requirement 2.1 by eliminating the second bullet point : "An entity that has transmission planning or analysis experience".
National Grid	No	While we support using the CIP-002-5.1 criteria as a starting point for applicability of the draft standard, we do have concerns with the inclusion of the phrase "within an Interconnection" in R1. FERC Order RD14-6 directs that "[a] critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System". By introducing the word "within," the Standard could inadvertently draw widely different interpretations of how to assess risks to the BPS. In practice, this could open up the potential for the inclusion of regional or localized transmission impacts, which we believe is in contrast with the Commission intended scope in the Order.As a result, we suggest that the wording in R1 be modified to the following:"A critical facility is one that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation or cascading failures widespread across significant portions of an Interconnection".Alternatively, we recommend clarifying in the guidance documents that 'widespread' and 'within an Interconnection' proposed words are intended to apply to impacts to the BPS that reaches deep into the Interconnection, and not affecting a small portion of an Interconnection. For example, if an Interconnection has relatively small Balancing Authorities (BAs), 'widespread' would need to be interpreted as impacts that would be crossing several, i.e. more than two, of those BAs in order to be considered 'widespread'.
Herb Schrayshuen	No	In Requirement R1 the use of the term 'transmission analysis' and 'transmission analyses' in order to identify which substations should have a security plan is vague The TPL standards extreme cases should be used to clearly describe the specific required elements of the analysis. Failure to specify how the analysis is to be done will lead to inconsistencies in the analysis and thereby difficulty for audits of the standard.

Organization	Yes or No	Question 2 Comment
		In Requirement R2 the use of the word 'unaffiliated' introduces ambiguity. There needs to be an understanding (through the standard but if not feasible through RSAW or other tool-e.g. guideline) what "unaffiliated" means. The term "unaffiliated" is not required because the NERC Reliability Functional model already ensures the independence between the TO/TOP and the verifying entities.
ATCO Electric	Yes	Although the FERC order contains language that a third party verification occur, this type of verification is not used anywhere else in NERC reliability standards for similar activities (e.g. CIP-002 classification). ATCO Electric (AET)respectfully requests that the review be allowed to be performed by qualified in-house Engineering groups who already perform these functions. Mandating a third party verification presents a risk to timelines and the implementation of the other requirements.
American Public Power Association (APPA)	Yes	APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members.TIMELINES to complete third party verification under R2 and third part review under R6 are both too short. Increase 90 days to 120 days or 180 days. Verifying entities may recommend that the Transmission Owner conduct additional planning studies to confirm asset identifications such as interactions between BES Elements in adjacent Transmission Owner footprints. A short 90-day time limit may not be sufficient time to conduct and verify a revised or supplemental BES assessment. For security reviews, conducting a meaningful review with sound recommendations applicable to a specific TO's or TOP's facts and circumstances may also take time along with necessary discussions with the TO. A short review window is more likely to lead to disagreements with the TO which in turn would lead to discrepancies that would need to be justified - which in turn might cause the reviewer

Organization	Yes or No	Question 2 Comment
		to avoid making proposals that should be considered by the TO or pressure on the TO to accept recommendations that could be improved upon.R1 GUIDANCE - TRANSMISSION PLANNING BASE CASES: Please revise the Guidance for R1 to clarify that TOs should start their initial and subsequent risk assessments with a common regional or area transmission planning base case used for transmission planning purposes. The base case should include existing BES stations and substations and those planned to be in service within 24 months within the region or area, to ensure forward-looking risk assessments and security planning.R2 VERIFICATION - Third party verification of third party risk assessments conducted under R1: some medium sized TOs with applicable transmission stations and substations may contract with a third party consultant to conduct necessary BES risk assessments, to ensure accurate and comprehensive consideration of the risk of widespread cascading, instability and uncontrolled separation. Such entities seek clarification that a single expert risk assessment study, in conjunction with a verification by an unaffiliated PC, TP or RC would suffice.
Arizona Public Service Company	Yes	AZPS generally agrees with the approach of the standard as drafted. The following comments relate to suggested modifications for Requirements 1-3.AZPS suggests that the drafting team modify the term “risk assessment” to “BES impact assessment” in Requirements 1-3. The term risk assessment is not a defined term in the NERC Glossary of Terms. It is used in other CIP standards (CIP-002, and CIP-004) each with a different context. Changing the term to “BES impact assessment” ensures that the risks will be categorized and evaluated correctly.Requirement 2.1 directs the Transmission Owner to select a Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment. However, none of these NERC functional entity designations appear in the applicability section of the standard. Thus it is assumed that the entities listed above are not obligated to conduct the assessment once selected but rather the assessment is conducted by mutual agreement. AZPS suggests that the drafting team provide clarifying language in the requirement to indicate that the assessment is conducted by mutual agreement between the Transmission Owner and the third-party assessor.AZPS is concerned that the term “primary control center” will

Organization	Yes or No	Question 2 Comment
		be confused with the NERC Glossary Term “Control Center.” The definition of Control Center is partially defined as “monitor and control the BES...”. The rationale for Requirement 1 introduces the term “operationally control” in its definition of primary control center which is further defined to mean “causing direct physical action”. The concept of monitoring is explicitly excluded from this definition. To avoid confusion, AZPS suggests that the drafting team define the term primary control center or adopt a new term that clearly differentiates itself from the common term “control center”.
FirstEnergy	Yes	FirstEnergy supports the proposed requirements R1 through R3.
Idaho Power Co.	Yes	Further clarification is needed on several points. There is no specificity to provide consistency with how the "risk assessment" should be performed or what methodology or components to the methodology should be used. Additionally, there is no defined meaning of "widespread instability, uncontrolled separation, or Cascading within an Interconnection." Does this refer to regionally identified IROLs or some other objective criteria or only based on the analysis performed? Additionally, there is no mechanism built into R3 to allow for a dispute between a TO and a TOP if they disagree on a particular station or substation as there is in the third party reviews under R2 and R6 where there is a mechanism to disagree with the reviewer.
Public Utitliy District No. 1 of Cowlitz County, WA	Yes	However, the TOP does not receive any relief from R1-R2 null set(s) and will be required to provide attestations to auditors and yearly certification of the absence of any notice from Transmission Owners.
MidAmerican Energy Holding Company	Yes	MEHC agrees with the R1 through R3 approach. However, MEHC suggests the following changes to improve the standards as written:The term “unafilliated third party” is used in R2 and in R6, but in parts 2.1, 2.3 and 2.3. “unaffiliated verifying entity” and in part 6.3 “unaffiliated reviewing entity” is used. Unless the intent was that the terms have different meanins, it is suggested that “unafilliated third party” be used throughout the standard.

Organization	Yes or No	Question 2 Comment
NRG Energy, Inc.	Yes	NRG agrees the approach described in Requirements 1 through 3 address the directives specified in FERC Docket No. RD14-6-000. However, NRG does have concerns with the standard as currently composed and offers the following points it believes will improve the standard if implemented: o Primary control centers are referenced in the "purpose" of the standard, but are not included in the "applicability" section. For clarity, NRG suggests the addition of section 4.1.1.5, stating "Control Centers and backup Control Centers associated with the Transmission stations and Transmission substations identified in requirements 4.1.1.1 through 4.1.1.4." o R1 directs that the Transmission Owner to perform an initial risk assessment with subsequent studies and include an unaffiliated third party to verify the risk assessment performed. NRG is concerned the standard does not indicate how information shared under this Requirement will be protected and held in confidence. NRG believes the information subject to this standard should be treated as Critical Energy Infrastructure Information (CEII). o R1 is vague in providing guidance as to the criteria to be used in developing the risk assessment. NRG appreciates this is intentional to allow flexibility in developing the assessment. However, this results in the potential for a determination of non-compliance during the audit process. NRG suggests reliance on the CIP-002 standard used for defining Critical Assets, which is based on solid metrics. o R2 seems to allow the same third party to perform both the initial risk assessment and the review of the initial risk assessment, potentially negating the need for a separate review. o R2.2 calls for review of the results of the initial risk assessment by an unaffiliated third party. The standard provides no guidance regarding the criteria (assumptions, contingencies, etc.) to be used for this review, which could provide results differing from the initial assessment. More objective measures should be incorporated.
Xcel Energy	Yes	Overall Xcel Energy agrees with the approach, but we offer the following items for consideration of the Standard Drafting Team.R1 requires an assessment of facilities, including those to be in service within the next 24 months, followed by an additional review every 30 or 60 months. If a facility is brought into service, it is unclear when the review should be performed due to the 6 month gap between the in service date and

Organization	Yes or No	Question 2 Comment
		the review. R2 requires a Transmission Owner to have an unaffiliated third party "verify" the risk assessment performed under R1. By contrast, R6 requires each Transmission Owner to have an unaffiliated entity "review" the evaluation performed under R4 and the security plan under R5. Xcel Energy recognizes that use of "verify" and "review" reflects the Commission's wording, but it would be helpful if the standard explained the difference between the two terms, if there is a difference.The 90 days prescribed by R2 to obtain third party verification may be too restrictive due to the availability and/or capacity of applicable resources. The standard requirement which imposes the action/deliverable by a third party, but the accountability to the TO/TOP, is also a cause for concern. It might be better to have the timing of R1 and R2 combined as this would enable flexibility of performing the assessment and completing the third party verification within the overall timeframe desired. We also suggest the Regional Entities or NERC be considered as parties that can provide third party verification and contract out if desired. It would also be helpful to expressly clarify in R2.1 that an "entity with transmission planning or analysis experience" could include a peer TO/TOP or a panel of employees from peer TO/TOPs, for example from the North American Transmission Forum. Allowing peer review would assist in identification and dissemination of best practices, we believe.R2.3 requires documentation of any recommendation to add or remove facilities as recommended by the verifying entity, but does not specify if any actions are required if no recommendations are made. Since the VRFs reference various levels of severity based upon documentation of recommendations, it would seem beneficial to allow a "no recommendations" option. Also, it is unclear if there are specific criteria the third party reviewer should utilize to review/verify and make recommendations if facilities are to be added or removed. While an entity could indicate why recommendations were or were not adopted, it would be useful to have verification criteria defined more clearly. R3 seems to be unclear in whether TOs or TOPs have operational control over facilities. In order to more clearly identify that TOPs have operational control, R3 should indicate that the TO shall notify the TOP of the identified facility.

Organization	Yes or No	Question 2 Comment
Peak Reliability	Yes	Peak believes the RC entity should perform the R2 verification because the RC has the wide-area view in the Western Interconnection. The alternative would be to have individual transmission entities perform varied verifications, which could result in inconsistent methodologies and results.
ISO/RTO Standards Review Committee	Yes	R1R1 in conjunctions with the Applicability section is a reasonable approach for identifying the scope of facilities subject to R2 - R6.R2Imposing a verification requirement is a reasonable way to facilitate an effective outcome in terms of identifying facilities that meet the impact thresholds established in R1. Requiring the use of an unaffiliated third party is reasonable because it mitigates the potential for inadvertent error in study work. Finally, allowing the verification to occur concurrently or subsequently, and leaving that decision to the discretion of the relevant functional entities, is appropriate. The functional entities should have the discretion to determine the most effective means of performing the verification. R2.1 requires that the verifying entity be either 1) a registered RC, PC or TP, or 2) another entity with appropriate planning or analysis experience. This is a reasonable approach that provides appropriate flexibility with respect to third party verification options. It also addresses the different operational and planning structures that comprise the North American electric grid - i.e. organized market regions where different entities can perform the different NERC registered functional roles (ISOs/RTOs) and vertically integrated regions where all the relevant roles under the standard may be performed by a single entity and, therefore, would require the use of an independent third party to perform the unaffiliated verification. R2.2 requires the third party verification to either confirm the TO analysis under R1, or, alternatively, recommend that facilities be added or deleted (the IRC assumes that a verification can confirm some results and also add facilties or remove facilities). Although R2.2 establishes a reasonable standard - i.e. verify TO results or recommend changes - the IRC offers the following comments. The requirement, as written, imposes the obligation on the third party verifying entity. However, the TO is the responsible entity under the standard - i.e. the TO is required to obtain the third party verification. The language should be revised to clarify that the

Organization	Yes or No	Question 2 Comment
		relevant actionable obligation (to obtain the third party verification) lies with the TO. The next issue raised by R2.2 is the timing. The IRC appreciates the importance of the issues being addressed by the proposed standard and the goal of implementing the standard and the relevant processes contained therein in a timely fashion. However, practically speaking, 90 days may be difficult to meet depending on the number of Transmission Owners that require verification from a single Registered Entity. For example, in organized markets there may be numerous TOs all selecting their PC to verify. To the extent implicated in reviews under the standard, IRC members would make best efforts to perform any relevant verifications. This comment is merely intended to highlight the potential resource impacts under the proposed 90 day timeline. The IRC proposes the following revisions to mitigate the issues in R2.2 described above. 2.2. The third party verification shall either verify the Transmission Owner's risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within a mutually agreed upon timeframe between the Transmission Owner and the third party but no longer than 180 calendar days following the completion of the Requirement R1 risk assessment. R3R3 obligates the TO to notify a TOP that has operational control of a control center associated with a facility identified pursuant R1 and verified under R2. R3.1 requires similar notification if a facility is removed via those processes. The standard may benefit from including the draft guidance into the R3 rationale section that clarifies that operational control means the ability to take action that affects the physical status of the facility, and that it does not include directive control, which relies upon another entity to take operational action to change the status of the facility. The guidance document addresses this issue, but the SDT could add clarifying language to the rationale section of R3, similar to the language in the guidance document and/or the language in the R1 rationale section, which reads in relevant part:"... identify the primary control center that operationally controls that Transmission station or Transmission substation (i.e., the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the

Organization	Yes or No	Question 2 Comment
		ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).”
Pacific Gas and Electric Company	Yes	R2 Comment: Suggest removal of the requirement for a third party risk assessment verification. Verifications already occur as part of internal compliance programs in CIP-002 and when audited by the Region. What if the assessment is performed by a third party, do you have to get another third party to verify? This creates a significant administrative burden, even if the Standard will only apply to a small number of entities and facilities.R3 (pg. 8) “...the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify...” Comment: Seven calendar days may be too short a time requirement, consider 10-14 days
Basin Electric Power Cooperative (BEPC)	Yes	R2 - A concern to consider is whether there is an adequate pool of unaffiliated third party verifiers to meet the 90 day timeframe. Possible solutions would include (1) increase the 90 day requirement to six months; or (2) Revise the requirement to allow the NERC Registered Entity to notify the appropriate Regional Entity of the verifier pool constraint and request the Regional Entity act as the verifier or specify an acceptable alternative.
Public Utility District No. 2 of Grant County, WA	Yes	R2 references primary control center(s). Since Control Center is a NERC defined term GCPD suggests that all references to the Control Center be capitalized within the Standard and that “primary” be defined within the standard to not include “back-up” Control Center(s).
Exelon	Yes	R2.1 Drafting Team could consider adding a note to R2 Guidance section similar to that which is included in the recently approved MOD-032 standard.”Planning Authority and Planning Coordinator" (hereafter collectively referred to as “Planning Coordinator”)combines “Planning Authority” with “Planning Coordinator” in the list of applicable functional entities. The NERC Functional Model lists “Planning Coordinator” while the registration criteria lists “Planning Authority” and they are not yet

Organization	Yes or No	Question 2 Comment
		synchronized. Until that occurs, the proposed standard applies to both Planning Authority and Planning Coordinator."
ReliabilityFirst	Yes	ReliabilityFirst supplies the following comments for consideration:1.Requirement R1 - ReliabilityFirst believes there may be a gap in the timing of performing the risk assessment for new Transmission stations and Transmission substations which are planned outside the 24 month window as required in Requirement R1. For example, as written, if a new Transmission stations or Transmission substation is planned for month 25, it would not be included within the initial risk assessment. Thus, there is a potential for this new Transmission stations or Transmission substation to not be assessed for 30 calendar months (for a Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable ...) or 60 calendar months (for a Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability..." With the potential gap in assessing new Transmission stations and Transmission substations being so long, ReliabilityFirst believes reliability may be compromised. For these reasons, ReliabilityFirst recommends the following for consideration: "Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 30 months)..." and including a new bullet under Part 1.1 which states "At least prior to the implementation of all new Transmission stations and Transmission substations (if not assessed within the initial or subsequent risk assessment)"2. Requirement R3 part 3.1 - From a standards writing perspective, if there is only one sub-part, ReliabilityFirst recommends including it within the Parent requirement R3. Typically sub-parts are only included if there are more than one.
Northeast Utilities	Yes	Requirement 1 should match that language in the FERC order and not limit the assessment to Transmission System analysis and allow for an opportunity to apply

Organization	Yes or No	Question 2 Comment
		technical expertise and judgment prior to the Transmission System analysis. We agree to Requirement 2 and Requirement 3.
PPL NERC Registered Affiliates	Yes	Requirement 1: 1. Requiring completion of an initial risk assessment for Transmission stations and substations planned to be in service within 24 months can lead to audit difficulties. Planned in service dates often change for a variety of internal or external reasons. It is requested that the SDT consider changing this language to a more easily identifiable trigger such as requiring the risk assessment to be performed before a new Transmission station or substation is energized. 2. Does the R1 risk analysis require consideration of the impact of loss of lines with voltages below 200 kV in an identified Transmission station or substation? 3. It is unclear when the R.1 risk assessment needs to be completed. This should be clarified.4. The wording in the Rationale for Requirement 1 box identifies the primary control center, but it also notes that control center electronic actions can cause direct physical actions at the Transmission station and substation. This would typically implicate the backup control center as well because the backup control center will have similar functional capabilities. There appears to be a disconnect between the use of the term primary control center and the parenthetical that follows which appears to include any control center that performs the listed functions.
San Diego Gas & Electric	Yes	SDG&E agrees with this approach. A facility's identification as "medium impact" does not necessarily mean that the facility, if rendered inoperable or damaged could result in widespread instability, uncontrolled separation or Cascading within an Interconnection. Application of a risk assessment will ensure that CIP-014-1 is focused on the facilities that are most critical to the system.
Seattle City Light	Yes	Seattle City Light supports the Question 2 comments of APPA as well as the additional comments of Salt River Project (SRP) regarding 3rd party verification.Third Party Verifiers (SRP):SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in

Organization	Yes or No	Question 2 Comment
		regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities.Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers.Confidentially of

Organization	Yes or No	Question 2 Comment
		the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
Seminole Electric Cooperative, Inc.	Yes	Seminole supports the comments by NRECA. Additionally, Seminole agrees with this approach. As this standard is based on the same standards as the impact ratings in CIP-002, it would be cleaner to identify any facility that is determined critical under the Assessment with a separate (non-exclusive) impact rating such high physical impact and use this term for applicability for R3-R6. If an entity has a qualified third party perform the R1 assessment on behalf of or in cooperation with the registered entity, does this also meet the requirement R2? Note that the draft RSAW, not under review here, states that R1 and R2 may occur concurrently. R2.4 is redundant with the information protection requirements in CIP-011-1. It would be appropriate to note that this information is included in the materials subject to enforcement under CIP-011-1 R1.
Vermont Transco LLC	Yes	Specifically the filtering of assets. While starting with CIP-002-5.1 as a starting point, the amount of analysis and assessment to determine if these facilities are critical and applicable to this standard may not be possible in the timeline proposed for this standard if a full transmission planning analysis will be needed. Many planning analysis performed previously by entities were not assessed to the specific defininition included in this requirement and therefore could require considerable work to be performed to analyze. The wording suggests that a full transmission planning assessment should be performed for all CIP-002-5.1 facilities and not to just those an entity feels may cause wide area impact.What if you do not agree with the third parties review of your

Organization	Yes or No	Question 2 Comment
		assessment? what evidence will be required to prove that you do not need to agree with their assessment?If an entity identifies a facility as critical does this require that the control center operating this facility must also have a full physical security plan per the requirements later in the standard?
Hydro One	Yes	Subsequent risk assessments should be performed every 36 months (to align with CIP requirements) instead of every 30 months. The FERC Order allows for the verification to be completed by NERC, the Regional Entity, an RC or another entity. The standard only identifies that the verification can be completed by a registered Planning Coordinator, Transmission Planner, or Reliabity Coordinator, or an entity with transmission planning and analysis experience; it does not mention NERC or the regional entity.
Portland General Electric	Yes	The following comments relate to suggested modifications for Requirements 1-3 -PGE believes the 90-day period to ensure verification of the risk assessment is too short. It will be difficult for every Transmission Owner to establish a contract with an unaffiliated verifying entity during the implementation time period. In addition, the current wording of the standard puts the obligation on the Transmission Owner to make sure that the assessment is done within 90 days, even though by definition they cannot have control over that timeline. Therefore, PGE proposes replacing the R2.2 language, "[t]he Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment," with the language, "[t]he Transmission Owner shall ensure that any agreement executed with the unaffiliated verifying entity stipulate that the verification be completed by a date that is not later than 90 calendar days from the completion of the Requirement R1 risk assessment."In addition, Requirement R3 provides no mechanism for the Transmission Operator who operates a primary control center identified by a different Transmission Owner to disagree with that identification. PGE proposes including similar language to that in R2.3 to allow for the Transmission Operator to

Organization	Yes or No	Question 2 Comment
		document the technical basis for not identifying its primary control center as an asset to be protected.
Virginia State Corporation Commission	Yes	There does not seem to be any timeframe within which the initial assessment is to be completed under R1, nor when the 30 and 60 month periods for subsequent reassessments under R1.1 are to begin and conclude.
California ISO	Yes	We agree with the approach identified in R1 through R3, however we have the following comments regarding the SCOPE of the verification review required by R2.2: o The scope of the 3rd party verification is not well defined. What is the expectation and scope of the verification review? What level of quality is expected/required? Is the Transmission Owner responsible for scoping the verification process to ensure the review meets the required level of review? o Very little guidance is provided on the scope of the review. The scope of the review and verification work would need to be well understood before taking this verification work on. Is a technical analysis required as part of the review and verification process on the part of the 3rd party verifying the Transmission Owner's risk assessment and list of critical facilities, or is it simply to review the risk assessment and list of critical facilities that the Transmission Owner has provided to the 3rd party reviewer, based on their current knowledge of the transmission system from performing prior transmission planning studies? Will NERC be providing additional guidance regarding the scope of work required for verification by a 3rd party?
Western Area Power Administration	Yes	Western agrees with the approach of using Requirements R1 and R2 to identify whether an entity is subject to Requirements R4-R6. However, we suggest that the drafting team modify the term "risk assessment" to "BES impact assessment." In the physical security community, the term "risk assessment" generally refers to "The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel." See ASIS International, General Security Risk Assessment Guideline (2002), http://www.scnus.org/local_includes/downloads/9200.pdf. In its filing to FERC, NERC

Organization	Yes or No	Question 2 Comment
		can explain that it adopted the term “BES impact assessment” so it is clear that the initial evaluation is of risk to the BES if the substation is damaged or rendered inoperable.Western recommends revising R1 1.1 to: “Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment.” This would consolidate the two bulleted actions and make them equally applicable. We believe a 60 month interval would be a more appropriate period for this type of assessment.Western suggest the drafting team clarify requirement 2.1, which directs the Transmission Owner to select a Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment; however, these NERC functional entity designations do not appear in the applicability section of the standard. We also suggest reconsidering the short 90-day period to ensure verification of the risk assessment. This may not allow every Transmission Owner to establish a contract with an unaffiliated verifying entity during the standard’s implementation time period.
Con Edison and Orange & Rockland	Yes	
Duke Energy	Yes	
Tampa Electric Company	Yes	
Tennessee Valley Authority	Yes	
American Electric Power	Yes	
American Transmission Company, LLC	Yes	

Organization	Yes or No	Question 2 Comment
City of Garland	Yes	
Clark Public Utilities	Yes	
Colorado Springs Utilities	Yes	
Edison Electric Institute	Yes	
Empire District Electric Company	Yes	
GridWise Alliance	Yes	
Manitoba Hydro	Yes	
Minnesota Power	Yes	
Minnkota Power Cooperative	Yes	
Modesto Irrigation District	Yes	
OPG	Yes	
Pepco Holdings Inc.	Yes	
Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern	Yes	

Organization	Yes or No	Question 2 Comment
Company Generation and Energy Marketing		
The Empire District Electric Company	Yes	
The Empire District Electric Company	Yes	
California Public Utilities Commission: Safety and Enforcenment Division		In general, the overall method employed in the draft standard is reasonable. The draft standard has adopted a reasonable level of specificity, without being overly prescriptive.The use of unaffiliated verifying experts is a positive element in the draft standard. In general, the balancing authority or reliability coordinator for the transmission area in question is the best verifying expert. In the event the utilities disagree with the assessments of the unaffiliated verifying entities at any point in the process (for example see section 2.3, second bullet point), not only should the transmission owner or utility be required to document their technical rationale, but the standard should further delineate a process for resolving this disagreement. With respect to Rule R1, Section 1.1, the drafting group should consider whether there should be language added to the standard detailing a process whereby the 30 or 60 month intervals should be accelerated in the event of serious intervening situations. With respect to Rule R2, Section 2.1, the description of “an entity that has transmission planning or analysis experience” is overly vague and should be further clarified, or that the use of this type of expert should be limited to certain small transmission owners. With respect to Rule R2, section 2.4, the language requiring “non-disclosure” agreements is important and a positive element in the draft standard.

3. **Requirements R4 through R6: The final three requirements of CIP-014-1 require (1) the evaluation of potential threats and vulnerabilities of a physical attack to the facilities identified and verified according to the earlier requirements, (2) the development and implementation of a security plan(s) designed in response to the evaluation, and (3) a third party review of the evaluation and security plan(s) (as directed in the order). Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security.**

Summary Consideration: The SDT thanks all commenters. All comments have been reviewed and changes that the SDT considers appropriate were incorporated into a subsequent revision. Language to describe the responsible entities for Requirements R4 through R6 was made consistent. Changes were made to clarify factors to be considered by the responsible entity in Parts 4.2 and 4.3. Requirement R5 was reworded to clearly indicate the SDT's intent for security plans to be developed within 120 days of completing Requirement R2 and executed according to the timeline specified in the security plan. Requirement R6, Part 6.1 was changed to clearly indicate that one or more of the criteria must be met. Corresponding changes were made to the measures in the standard. Several additions were made to the Guidelines and Technical Basis section. A summary of comments and the SDT's response is provided:

- **Requirement R4. Various changes were recommended to the parts in Requirement R4 that describe factors to be considered in evaluating threats and vulnerabilities. Some commenters recommended deleting Parts 4.1 to 4.3. Some suggested adding additional language for clarity or to limit factors that must be considered.** Parts 4.1 through 4.3 provide considerations to be used by an entity in determining what threats may be 'realistically contemplated', as directed in the FERC Order. As written, Requirement R4 provides owners with appropriate requirements to develop a tailored evaluation process that takes into account factors such as location, size, function, existing protections, and attractiveness as a target. A clarifying change was made to Part 4.2 to now read "Prior history of attack…"
- **Requirement R4. A commenter recommended modifying Part 4.1 to focus the threat assessments on only those elements within a Transmission station or Transmission substation that affect the reliability of the BES.** The proposed standard satisfies FERC directives to address risks from physical attack on facilities as described in footnote 6 of the Order. A threat assessment must be performed for the entire Transmission station or Transmission substation. As noted in the Guidelines and Technical Basis section for Requirement R5, "While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site."
- **Requirement R5. Commenters asked for clarification on the 120-day time requirement to develop and implement a physical security plan, and the timeline required by Part 5.3 for implementing physical security enhancements or modifications.** Requirement R5 was reworded to clearly indicate the SDT's intentions. Physical security plans required by R5 must be developed within 120 calendar days of the completion of Requirement R2. This plan must include a timeline for executing physical security

enhancements and modifications according to Part 5.3, which may extend to a period determined by the responsible entity. The Guideline and Technical Basis section was also updated to clearly state the SDT's intentions.

- **Requirement R5. Commenters proposed alternate language for Part 5.1, indicated that requirements needed to be more specific, or proposed a specific technical solution.** The SDT accepted those revisions that it believes add clarity and are consistent with NERC Security Guidelines. The proposed standard meets the requirements of FERC's Order in a manner that supports reliability. FERC recognized that a "one-size-fits-all," prescriptive approach to protecting the Bulk Power System from physical security threats would not provide the most benefit. Like all standards, proposed CIP-014-1 is technology neutral. The SDT has provided several references and guiding documents in the guidelines section.
- **Requirement R5. Some commenters proposed removing Part 5.2 (Law enforcement contact and coordination information).** The SDT believes law enforcement contact and coordination information required by Part 5.2 is an essential element of a physical security plan and does not agree that it should be removed. EOP-004-2 includes law enforcement as an example of an organization to be included in an entity's event reporting Operating Plan, which may not meet the reliability objectives of a physical security plan developed to meet the requirements of CIP-014-1.
- **Requirement R5. A commenter recommended that the standard establish specific sequencing for the implementation of the physical security plans required in R5 to follow the review of the physical security plans required in R6.** The SDT believes the standard as written appropriately requires the responsible entities to implement physical security plans in a timely manner and does not support a establishing a timeline that places implementation after review. The SDT also recognizes that entities may develop the physical security plans and have them reviewed concurrently as explained in the Guidelines and Technical Basis section, which would satisfy the commenter's proposed sequencing. .
- **Requirement R6. Some commenters did not support the requirement for third party review or recommended changes to language or organizations listed in Part6.1.** The requirement for third party reviews satisfies the FERC directive and is intended to provide for an added level of physical security expertise beyond the responsible entity in the development of security plans. The SDT agreed with recommendations to change the list in Part 6.1 from numbers (6.1.X) to bullets to reflect their intent that an acceptable third party reviewer did not need to meet each criteria in the list. The SDT agrees that the credentials cited in Part 6.1 are not an exhaustive source of professional certifications. The SDT did not agree that the ERO should be the only authorized reviewer, and did not agree that any other specific additions to the list were necessary. The most appropriate third party reviewer for a given entity may vary based on the entity's specific circumstances and assets; collectively the list in Part 6.1 provides the necessary flexibility for all applicable entities. The suggested addition of a peer review group with physical security expertise is not explicitly necessary as such a reviewer could be utilized with ERO approval. A specific process is not required for the ERO to exercise its authority to approve a reviewing entity under Part 6.1.
- **Requirement R6. Commenters asked for clarification on whether third party reviews are required for plan revisions.** The SDT intends for all periodic review requirements for Requirements R4 and R5 to be addressed by meeting the 30 calendar month

review requirement of Requirement R1 and following the timelines in subsequent requirements. Changes or modifications made within the 30-month period are not specifically required to be reviewed by a third party.

- **Requirement R6. Some commenters indicated that a resolution process was needed or sought clarification for responding to reviewer recommendations.** The requirement for third party reviews as written provides for an added level of physical security expertise beyond the individual entity in the development of the required security plans. The Transmission Owner or Transmission Operator that created the physical security plan is ultimately responsible for physical security of the facility and thus makes the final determination on accepting the recommendations of a reviewer. The SDT believes that in documenting this determination as required in Part 6.3, the responsible entity should clearly explain their considerations and, if appropriate, an alternate approach that achieves the desired result.
- **Requirement R6. Commenters expressed concerns over potential for mishandling confidential or sensitive information.** The SDT agrees that the consequence of mishandling sensitive information is serious and has included methods that a responsible entity could use in complying with the standard in the Guidelines and Technical Basis section.
- **Requirement R6. A commenter proposed an exemption from Requirement R6 for federal entities that have an inspector general.** The SDT does not agree that the proposed exemption would meet the directives in FERC Order, Paragraph 11, which specifies that the review be conducted by an entity other than the owner or operator with appropriate physical security expertise. An Inspector General may be acceptable as a reviewer under Requirement R6 as long as they have the necessary expertise and is an unaffiliated third party. Please see clarifications in the Guidelines and Technical Basis section regarding affiliation.
- **Timelines for Requirements R5 and R6. Some commenters indicated that the standard did not allow sufficient time to complete the requirements.** The SDT believes that the timeline for Requirements R5 and R6 is aggressive but achievable.

Organization	Yes or No	Question 3 Comment
ACES Standards Collaborators	No	(1) We see a significant risk of the compromise of highly sensitive information created by Requirement R6 and question why the unaffiliated third party review cannot be integrated into the ERO compliance monitoring and enforcement processes. There is no compliance obligation on these third parties to complete the review within the required timelines, which could subject the TO to potential compliance violations. Furthermore, there is a limited set of companies with qualified personnel capable of performing this review. Given that all of the Transmission Owners will be working toward the same effective date of the standard, it is highly likely that a backlog of work would occur. Furthermore, review of the evaluations by consultants will increase the

Organization	Yes or No	Question 3 Comment
		the number of people with access to higly senstivie information. While this concern can be partially mitigated through confidentiality agreements, the more people that have the information, the higher the probability the information will be released, whether intentional or unintentional, to persons that should not have the information. To resolve this inssue, NERC and Regional Entities could hire qualified personnel to perform these reviews. NERC and Regional Entities could perform a spot check of the standard 90 days after the initial effective date. If NERC or the Regional Entity disagree with the approach or believe additional facilities should be added, RAI would give them the flexibility to treat the issue as not impactful to compliance as long as the TO resolve the issue within a certain time period. This approach would result in a reduced cost impact on industry and minimize the distribution of highly confidential information reducing the likelihood of information leaks. (2) How can the 'cost to benefit to risk to the BES' be measured consistently across each facility, region and risk? Does a Registered Entity have to authority to not implement a 'recommendation' from a third party based upon a cost to benefit to risk analysis? (3) Given that third parties are required to evaluate critical facility information, further guidance is needed for the required controls to prevent unintended release of highly sensitive and confidential information. What is the risk to the Registered Entity if the information does get leaked? Is this a violation to the Registered Entity, even if the leaked information was not caused by the Registered Entity? We are concerned that if this information were to be leaked, the Registered Entity could be liable for increased risk of attack, additional time and costs to address the leak and could impact the BES due to changes in operations from shutting down those facilities.(4) Part 4.2 has a potential "prove the negative" issue. How do you prove that you considered similar facilities particularly when similar facilities could includes other company's facilities. To resolve this issue we suggest replacing "similar" with "nearby facilities" or "asset owner's other facilities in the area". (5) Part 4.3 could be interpreted as requiring consideration of all threat and intelligence information including information that is not relevant to a given area. To remedy this issue, we recommend using the term "current and local" to describe the types of intelligence and threats that must be considered.(6) We believe that Part 5.2 is redundant to the EOP-004-2 - Event Reporting, especially Attachment 2 Event

Organization	Yes or No	Question 3 Comment
		Reporting Form line 4. Please consider removing and comparing the standard in its entirety to EOP-004-2 to avoid unnecessary duplication.(7) For Part 5.4, please modify the language to clarify that it only applies to facilities identified as a result of application of Requirements R1 and R2.(8) For Part 6.1 please modify "... from the following" to "... from one of the following". This will make it perfectly clear that only one entity must be selected.
Manitoba Hydro	No	(1) Manitoba Hydro has concerns about the need to have a third party to review or verify risk assessments and physical security plans. It is unclear at this point what measures or counter measures are being alluded to here as far as protecting critical assets such as lines and towers. This may potentially be financially burdensome as well as questionably effective.(2) Also missing in the standard is conflict resolution between a TO and this third party reviewer. Clarification should be provided on who weighs in on this and how NERC audits a system that has been verified by a third party. As currently drafted it appears that the third party reviewer/verifier would have no liability under the standard.
Texas RE	No	1. The sequence and timelines for R5 and R6 need to be reviewed. R5 states the TO "shall develop and implement" the security plan within 120 calendar days of completion of R2. R6 states the 3rd party evaluation can occur concurrently with or after completion of R5. It seems like the 3rd party evaluation should be completed before the plan is implemented in R5, otherwise the entity may be planning for or implementing measures that may not be appropriate for the risk level.2. R6 also 3. Also, who evaluates the implementation phase of security plan and whether or not it was implemented correctly or if the plan was effective? There should be an entity assigned for this task. There should be an exercise (like GridEx) to test the plan.4. The third party reviewer could be the same entity in R2 and R6. This could be a question of independence. It also does not indicate the third party actually verifies the implementation of the security plan(s) in R6. This does not permit the Compliance Enforcement Agency to place reliance upon the work of the third party.

Organization	Yes or No	Question 3 Comment
Georgia System Operations Corporation	No	o GSOC supports the comments submitted by both GTC and NRECA. o In addition, GSOC suggests in R4.2 changing "Prior history or attacks on" to Prior history of physical security related events at" to better describe the subrequirement. o GSOC suggests in R6, last sentence, changing the word "development" to "developed" in order to be consistent with the word "performed" in the same sentence.
Florida Keys Electric Cooperative	No	o It's unclear how an auditor will judge compliance with R4 and its subrequirementsas it will be uncertain what an owner or operation is aware of regarding prior history, intelligence information, etc. The language should be revised to clarify the compliance expectations and also taking into consideration that each TO and TOP may have a varied exposure to the items identified in the requirements. o R5.1 - FKEC strongly recommends the removal of "Resiliency or security" as this is not needed for the requirement and resiliency will be next to impossible to audit. o 5.3 - After the word "modifications " add ",if any," as this is a possibile outcome. o R6 - Same as comments on R2 in Question 2 above. and R2.1. o R6.1.1 - NERC standards should not endorse, or appear to endorse, ASIS or its certifications in a requirement. This should be removed. There could be other certifications that an entity may have that provides for the necessary skills under this standard. o R6.1.2 - It is highly unlikely that the ERO is not going to approve consultants for industry use. This should be removed. o R6.1.3 - All government agencies have physical security expertise for their own facilities; that doesn't mean they can be an adequate reviewer under this standard. This should be removed. o R6.1.4 - It is unclear and not auditable whether an entity has demonstrated expertise. This language should be removed.
Flathead Electric Cooperative, Inc.	No	Again, do not support the third party review requirements. Already an auditable standard approach.
Florida Municipal Power Agency	No	Again, FMPA commends the SDT for a job well done. Just a few minor comments.See response to question 1 concerning use of the terms "control center" and "unaffiliated".CHANGE MANAGEMENT OF THE VULNERABILITY ASSESSMENT AND SECURITY PLANSimilar to our comments regarding change management of the risk

Organization	Yes or No	Question 3 Comment
		assessment, it is ambiguous as to how we would implement change management related to the vulnerability assessment and security plans.R4 has no periodicity requirement, but, instead seems to require responsible entities to continuously reevaluate their vulnerability assessments in response to events listed in bullets 4.1, 4.2 and 4.3. If the entity changes their vulnerability assessment to include new threats, does every revision require a new 3rd party review? How do we come to agreement what constitutes a valid "trigger" for a new vulnerability assessment? It seems to imply that each of us would need to have an independent 3rd party on retainer to review our assessment of every intelligence or threat warning from governmental or regulatory agencies, or new attacks that each entity becomes aware of. Is that the intent? If so, what consititues a "warning", e.g., is it an "official" warning through some sort of official channel, such as a NERC Alert? If so, what happens if an entity decided to act on an "unofficial warning", such as a media release, to revise their vulnerability assessment - would that also need a 3rd party review? FMPA suggest clarifying 4.3 with "Official intelligence or threat warnings ...".R5 seems overly ambitious. 120 days, or 4 months, is not a lot of time to perform a vulnerability assessment and develop and implement a security plan, especially in response to a newly identified threat vector/warning, and especially considering that a revised security plan may include capital investments in measures like new enclosures, vehice barriers, or the like. Is the intent that a security plan could be a phased approach, e.g., implement an interim security plan within 120 days while future improvements to that plan take longer? If so, then the language of the requirement ought to reflect that intent. FMPA suggest a modification to R5 such as: "... shall develop and implement the first phase of a documented physical security plan(s) ... within 120 calendar days ..."In addition, R5 does not seem to fit temporally with R2 and R4 well. R2 requires periodic risk assessments every 30/60 months. R4 seems to require changes to vulnerability assessments in response to newly known threat vectors. The timing of R5 refers to R2: "... within 120 calendar days following the completionof R2" with no reference to a revision to the vulnerability assessment. This causes FMPA to belevie that revisions to the security plan as a result of a new threat vector and a revised vulnerability assessment of R4 would not need to be required until 120 days following the next

Organization	Yes or No	Question 3 Comment
		periodic risk assessment of R2. Is that the intent?If that is the intent, if an entity chooses to revise the security plan earlier, would that then need an 3rd party verification at that time, or at the time of the periodic risk assessment?
Black Hills Corporation Entities	No	BHC has the same concern with R4 as expressed in the opening comment of the previous section regarding the definition risk assessment. The tailored evaluation required by FERC directive paragraph 8 introduces a probability of less than 100%, which is in conflict with prior NERC guidance on risk definition. As previously noted, if the unique probability of a threat is to be taken into consideration along with the impact, this change from CIP-002-3 expectation should be clearly highlighted. In addition, the inclusion of probability in the risk assessment will increase disagreements between unaffiliated entities, which will require a mechanism for resolution.BHC questions R4.2: The current language states “Prior history or attack”. BHC believes this opening should state “Prior history of attack” because the current language does not provide an indication of what ‘prior history’ is being referred to.BHC agrees with the AZPS suggestion that a sector specific threat source be utilized to aggregate and disseminate threat information to ensure that relevant and timely data is analyzed consistently across the regions, which would also improve the auditability of the standard as well by removing the subjectivity associated with an unbounded number of threat sources. BHC believes that the 120 day requirement for R5 should be limited to the development of the security plan, and that full implementation should be dependent on the complexity of the plan. Implementation timing of the entity’s plan should be approved by the applicable RC. Provisions could be added for temporarily derating the facility, if the implementation timing were considered by the RC to be excessively long. By mandating a 120 day implementation, entity’s security plans may be down-sized to meet the 120 day implementation window, rather than to meet the potential threats and vulnerabilities at the facility. If “implementing” only means the specific deliverables of R5.1, R5.2, R5.3, and R5.4 (i.e. the timeline required by R5.3 is created, but not executed), then “implementation” needs to be more clearly defined.BHC has a further concern that R5.1 language reads too close to the “Identify, Assess, Correct” language already remanded by FERC in the CIP v5 standards.

Organization	Yes or No	Question 3 Comment
		Alternative language for R5.1 might be "Resiliency or security measures designed to prevent potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4." This simplification is not expected to change entities efforts, but could be more appealing to FERC.BHC agrees with the reasoning of AZPS to simplify R6.1 to read: "Each Transmission Owner and Transmission Operator shall select an unaffiliated third-party reviewer with electric industry physical security expertise." If this language consolidation is not acceptable, then alternatively recommend that Section 6.1.1 be expanded to include other similar certification providers, e.g. the National Sheriffs' Association Institute for Homeland Security offers a Certified homeland protection Professional (CHPP) designation (https://ndpci.us/certification/CHPP_Certifications.php), so as not to appear preferential.
City of Garland	No	Clarification - R6.2: Need to clarify that "completing the security plan(s)" does not include completing the tasks outlined in the time line developed in R5.3 - the time line is required to be complete as part of the plan but not the tasks in the time line.
Tennessee Valley Authority	No	Comment: Proposed language to be added to the end on Requirement 6:This Requirement shall not apply to any Federal corporation or agency that meets any of the criteria in Requirement 6.1 and that has an Inspector General, pursuant to the Inspector General Act Amendments of 1988, appointed by the President of the United States and charged with oversight responsibility for such Federal corporation or agency.Comment: Recommend adding "with electric utility experience" as a reviewer qualification to 6.1.3 and 6.1.4.Rationale: There should be a common standardizing qualification such as PSP, CPP, or electric utility experience that applies across the sub requirements of R6 that entities and the ERO can use as criteria to qualify unaffiliated third party reviewers.
Western Electricity Coordinating Council	No	From a compliance perspective, WECC notes that the criterion identified in R4 is too vague to enable a consistent approach across regions or even entities. Identifying a basic set of attack vectors that must be considered (ie: direct fire ballistic attack,

Organization	Yes or No	Question 3 Comment
		indirect fire attack, explosive device attack, vehicle-borne attack, arson/incendiary attack) fosters a far more consistent approach while allowing the entity the flexibility to tailor their assessment and security plan to the unique characteristics and threat landscape of their asset(s). WECC is concerned that the language of Requirement R5 is confusing or contratictory. Requirement R5 requires the applicable entity to "develop and implement" a documented physical security plan...within 120 calendar days following the completion of Requirement R2. However, part 5.3 requires a timeline for "implementing" the physical security enhancements and modifications specified in the physical security plan. WECC questions whether Requirement R5 requires the physical security plan to be "developed" or "developed and implemented" within 120 calendar days following the completion of Requirement R2. If Requirement R5 requires "development and implementation" within 120 calendar days following the completion of Requirement R2, what is the purpose of the timeline for implementing the physical security enhancements and modifications specified in the physical security plan required by part 5.3?
Georgia Transmission Corporation	No	-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard.- GTC requests revision to the requirement language or addition of guidance around the phrasing of "unique charact
None	No	It is recognized that a one-size-fits all approach is not practical. However the proposed directives as to what should be included in physical security plans are so general that little is likely to change from current practices that are insufficient to protect very critical high risk substations. The only language directive in CIP-01401 is listed on Pg. 10, R5 para 5.1. More definitive guidelines must be outlined if improvements are to really be achieved.The utility industry has used real-time remote monitoring of substation equipment for reliability purposes for decades. Similar technology is available for the very important physical security function. The following sentence needs to be added at the end of paragraph 5.1. "Security measures must include isolation zones of sufficient size covering approaches to substations, in addition to monitoring inside substation fenced areas, to detect both attempted and actual

Organization	Yes or No	Question 3 Comment
		penetration of critical sites and the surrounding buffer areas. The areas must be patrolled with real time monitoring & assessment equipment designed to provide live and playback/recorded video that must be automatically presented to alarm station operators. Detection equipment must include gunshot detectors. Sufficient real-time surveillance must be provided to allow sufficient time to implement a tactical response plan to minimize and interrupt threats."
National Rural Electric Cooperative Association (NRECA)	No	It's unclear how an auditor will judge compliance with R4 and its subrequirements as it will be uncertain what an owner or operation is aware of regarding prior history, intelligence information, etc. The language should be revised to clarify the compliance expectations and also taking into consideration that each TO and TOP may have a varied exposure to the items identified in the requirements.R5.1 - NRECA strongly recommends the removal of "Resiliency or security" as this is not needed for the requirement, and resiliency will be next to impossible to audit.5.3 - After the word "modifications " add ",if any," as this is a possibile outcome.R6 - Same as comments on R2 in Question 2 above. and R2.1. R6.1.1 - NERC standards should not endorse, or appear to endorse, ASIS or its certifications in a requirement. This should be removed. There could be other certifications that an entity may have that provides for the necessary skills under this standard.R6.1.2 - It is highly unlikely that the ERO is going to approve consultants for industry use. This should be removed.R6.1.3 - All government agencies have physical security expertise for their own facilities; that doesn't mean they can be an adequate reviewer under this standard. This should be removed.R6.1.4 - It is unclear and not auditable whether an entity has demonstrated expertise. This language should be removed.
Los Angeles Department of Water and Power (LADWP)	No	LADWP requests the Drafting Team to make the following changes:- For R5, replace the word "implement" with "complete" to avoid confusion as to whether the plan needs to be implemented within the timeline provided- For R5.1, the word "Resiliency" needs to be defined in the standard to avoid any misinterpretation. Resiliency means different things to different people- For R5.1, add the language ", mitigate the impacts of," to the requirement as follows:"5.1. Resiliency or security measures designed to deter,

Organization	Yes or No	Question 3 Comment
		detect, delay, assess, communicate, mitigate the impacts of, and respond.....”- For R5.4, change the requirement language to read as follows:”5.4. Provisions to evaluate evolving physical threats to the Transmission station(s), Transmission substation(s), or primary control center(s), and their corresponding security counter measures. “This sub-requirement should allow for the TO to revise its already-reviewed security plan within the 30-month cycle without necessarily having to make arrangements for a third party review of the revised plan (although it may do so if TO so desires) and without creating an additional 30-month cycle review that the normal course - this is a matter of efficiency and due diligence to address evolving threats- For 6.1, as previously mentioned, the word “unaffiliated” needs to be defined in the standard to avoid any misinterpretation.- For 6.1.3, change the requirement as follows: “6.1.3. A governmental agency with physical security expertise, which could be a City Department in which the utility resides that requires a review to be performed.”This clarification allows for additional flexibility of independent governmental agencies reviews.- For 6.1.4, change the requirement as follows: “6.1.4. An entity or organization with demonstrated law enforcement, government, or military physical security expertise, such as the local police department in which the utility resides that requires a review to be performed.”This clarification allows for additional flexibility of independent entities or organizations reviews- For R6, add 6.1.5 with the following language: “6.1.5. A peer utility review group with demonstrated law enforcement, government, or military physical security expertise This clarification allows for additional flexibility of other Planning Coordinator, Transmission Planner or Reliability Coordinator review the work of their peers.In the alternative, expand to include Planning Coordinator, Transmission Planner or Reliability Coordinator with law enforcement, government, or military physical security expertise.- For 6.2, change the “90 calendar days” to “120 calendar days” to provide sufficient time to determine reasonable and sound recommendations.- For 6.3, chance the “90 calendar days” to “120 calendar days” to provide sufficient time to address any modifications recommended.

Organization	Yes or No	Question 3 Comment
New Brunswick Power Corporation	No	NB Power is concerned with the 120 day timeline to implement a physical security plan that would meet the third party verification requirements. Having limited knowledge of physical security issues NB Power will likely rely on the third party verifier to work with NB Power in developing a security plan. NB Power is not aware of any analysis that was done to ensure that there is enough capacity within the “physical security industry” to support the work load increase resulting from the approval of this standard and as such is concerned that 120 days may be insufficient.NB Power is concerned that it could be non-compliant with R6.2 if the third party fails to meet its obligation. While NB Power can mitigate the financial risk of that event it would still result in a recorded non-compliance.It is the opinion of NB Power that the proposed standard does not sufficiently address a disagreement resolution process between the TO and the unaffiliated reviewing 3rd party in requirement. NB Power believes that documenting the technical basis for not following the recommendations of the unaffiliated reviewing 3rd party without guidance on what constitutes valid technical reasons presents a compliance and enforcement gap where both the entity and an auditor may not be able to come to a consensus. NB Power suggests the SDT develop guidance concerning compliance and enforcement of this requirement indicating acceptable technical reasoning for not following the 3rd party’s recommendations.
Rayburn Country Electric Cooperative	No	Once the in scope facilities have been identified, it would be best for the entites to use the same resources for the evaluation of “Potential Threats” since this language has endless possibilities.i.e. Aerial attack, induced seismic events to name a few to illustrate "Potential". I favor the wording of "reasonable risks"The FBI, DOE or DHS should be involved in the discussion with the entities in lieu of a third party who is only subject to confidentiality agreements and also has interests beyond mitigating the true risks.
Ciy of Garland	No	R4 - Sub requirement 4.1 should be modified to include specific language focusing the security study to those elements within the substation that can affect the reliability of the BES. The security plan should protect those elements of the substation as

Organization	Yes or No	Question 3 Comment
		identified in the planning study in R1 that could cause the cascade or other unacceptable event identified in R1. Many substations identified in these studies are very large geographically and potentially very expensive to protect elements that may be located 30 to 50 feet above the ground. If these elements are determined to be critical they should be protected. If not, there is no justifiable reason to expend the resources to protect these devices. The security plans should concentrate on the protection of elements that could actually cause a cascading event, otherwise large expenditures may be made while adding no benefit or improvement to the reliability of the BES. R4.1 should read:4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) including the identified elements within the station, substation or control center, that need to be protected that could initiate the cascading collapse identified by the planning study in R1;Under both R4 and R5 clarification should be provided to the auditors affirming that auditors do not need the work papers, or backup information used in preparing the security plan, it is preferable auditors be allowed to only view the plan on site and not be allowed to take a copy of the plan for their files due to the sensitive nature of the security plan. Having copies of the security plans of critical targets consolidated into the files of the auditing entity increases the security risk to the plan and identified assets do to a security beach or accidental release of the file. While having one security plan of a critical location is a security risk in and of itself, having a compilation of security plans by one entity becomes a national security risk.R5 - states in part that each TO and TOP "shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2." The "and implement" should be deleted. It should be made clear the facilities, additional employees or other measure identified in the plan are not required to be in place at the end of the 120 days. The requirement should be clearly stated that a timeline needs to be developed as part of the plan and the TO and TOP will implement the plan per the timeline identified in the plan. The implementation may require several years to get through budget cycles, procurement, installation and implementation.R6 - The standard should make clear the auditor is not

Organization	Yes or No	Question 3 Comment
		to audit the security plan for its content or appropriateness, but to confirm a security plan has been developed and that particular security plan has been reviewed by a qualified entity. It should also be clear that a TO could expand its actual security beyond that identified in the approved/reviewed plan without requiring an additional review of such modification. Example:The original, approved plan had card readers on the doors and cameras within the yard. During the 30 months until the next required review, the TO added motion detectors as additional security measures at the substation even though they were not required in the initial security plan. The installation of additional monitoring or security measures beyond those in the approved plan should not initiate the need for a new security plan or third party review.
Bonneville Power Administration	No	R4. BPA agrees with the requirements to develop a threat assessment and physical security plan. BPA also agrees with the inclusion of governmental agencies with physical security expertise as threat assessment and physical security plan reviewers as noted in R6 (Section R6.1.3.) However, BPA requests that the drafting team clarify the scope and purpose of third party reviews should they remain as part of the standard. BPA disagrees that third party reviews will increase reliability and notes the draft standard exceeds the scope of the FERC order Paragraph 11. BPA believes that each entity is in the best position to evaluate threats to its facilities and determine appropriate mitigation plans. Nonetheless if third review is deemed necessary, BPA believes that it should be allowed to have another federal agency perform its third party review. In other words, for purposes of this standard, another federal agency would be deemed to be “unaffiliated” with BPA. Keeping this information within the federal government will decrease the risk of inappropriate disclosure of such information. BPA believes that non-disclosure agreements with non-federal parties may be a poor substitute for this because they can only be enforced once a disclosure is made. At that point, it is often too late and the information is available to a wider audience than intended. "R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each

Organization	Yes or No	Question 3 Comment
		Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following attributes: [VRF: High; Time-Horizon: Long-term Planning]" BPA recommends revising the 120 day requirement in R5 to 12 calendar months. Justification: This information is important to get right as security designs and enhancements will be built from this plan. 120 days is not be enough time to develop a complete and effective security plan and incorporate finalized threat assessments."R6 Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. [VRF: Medium; Time-Horizon: Long-term Planning]" BPA recommends revising R6 first sentence to: "R6 Each Transmission Owner shall verify the risk assessment performed under requirement R4 by a third party entity other than the owner or operator." Justification: BPA believes the proposed revision fully aligns with the requirements of the FERC order by using the requirements of the FERC order. The introduction of a requirement of an unaffiliated reviewer is reaching beyond the requirements established by the FERC order, and this requirement will dilute the quality of a risk assessment. It will limit the types of entities that can perform an independent review, and directs use of resources that may not be capable of assessing all physical risks within an electrical facility. BPA proposes the word unaffiliated be removed from this standard and replaced with language that describes the degree of

Organization	Yes or No	Question 3 Comment
		separation from the facility owning entity to be considered a third party entity other than the owner or operator. Based on the definition provided in this draft "unaffiliated" is especially troublesome for federal government owned transmission networks and facilities because it could be interpreted as excluding the entire federal government from eligibility as a third party entity to the government transmission owner.Also, industry peer reviews should be encouraged and considered as meeting the requirement. Reviews by industry peers are known to be beneficial to the entity receiving the review and for the entity performing the review or audit. Enabling industry peer reviews would not only meet the intent of an independent review but also accelerate continuous learning and translation of the most effective security approaches into wide spread use. Please note that the FERC order only recommends this verification as it is stated as "should" and not as "shall."
Virginia State Corporation Commission	No	R4.2 requires each Transmission Owner of an identified facility to "consider" and "Prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events." Is such consideration to be given to other "similar facilities" of the specific Transmission Owner or of any Transmission Owner anywhere in North America? How will such "consideration" be possible if the scope of such consideration is intended to be the latter? R5 is fine, but R6 suffers from the same ambiguity as R4.
Dominion	No	R5 and R6 are written for the initial risk assessment and don't necessarily apply for subsequent risk assessments. Is the expectation that 3rd party reviews be performed for R4 and R5 every time R1/R2 is run, particularly if there are no changes? Dominion recommends that the SDT modify this in the event the R1 list changes (ie: add stations) to require a subsequent R4/R5 reassessment. If stations drop off, or no change to R1 list for subsequent assessments, then subsequent R4/R5 reassessment is not required.R6 - Through continuous improvement processes and lessons learned, there will be expected changes to the security plan(s). What changes are allowed to the security plan(s) without triggering a 3rd party review?

Organization	Yes or No	Question 3 Comment
Bureau of Reclamation	No	Reclamation agrees with the requirements to develop a threat assessment and physical security plan. Reclamation also agrees with the inclusion of governmental agencies with physical security expertise as threat assessment and physical security plan reviewers. However, Reclamation does not believe that the proposed requirements will allow adequate time for a comprehensive review. Reclamation suggests that at least 180 days would be a more appropriate timeframe for a detailed threat analysis and physical security plan review. Reclamation also requests that the drafting team clarify the scope of third party reviews of these threat assesments and physical security plans, perhaps by adding additional detail to the Guidance and Technical Basis section. Reclamation is not convinced that third-party reviews will increase reliability. Reclamation believes that each entity is in the best position to evaultate threats to its facilities and determine appropriate mitigation plans. Reclamation is concerned that the well-intentioned third-party review mandated by the order could result in classified or national security related information falling into the wrong hands. Reclamation does not believe that non-disclosure agreements will adequately protect this sensitive information.Reclamation believes that audits by regional entities in essence provide a “third-party” review of an entity’s threat assessments and physical security plans.
SERC CIPC	No	Recommend adding electric utility experience to 6.1.3 and 6.1.4. Consider removing the requirement for CPP and PSP certifications. Rationale: Numerous other mandatory enforceable standards (e.g. MTSA, CFATS, and CT-PATS) that do not require specific certifications nor are we aware of similar certifications in cyber elsewhere in the CIP standards. Suggest clarification of “electric utility experience” and “physical security experience” to allow the ERO and registered entities to justifiably select authorized third party reviewers.
Northeast Power Coordinating Council	No	Regarding Part 5.1, the requirement states that the security measures should be designed to deter, detect, delay, assess, communicate and respond to potential physical threats. NPCC suggests removing the obligation to ‘deter’ from this Part and establish a separate Part that addresses deterrence and very basic specifics regarding

Organization	Yes or No	Question 3 Comment
		what constitutes deterrence. The new Part could describe how an entity should implement deterrence and consider some minimum auditable criteria; for example, Consider and Implement measures designed to deter potential physical threats including 1) perimeter control 2) motion detection 3) lighting 4) access control. In this manner the ambiguity surrounding the term 'deter' is eliminated. Part 5.3 should allow flexibility to modify the time line. Suggest that Entities should 1) have a master Physical Security Plan; 2) have the flexibility to accomplish mitigation activities associated with the results of the vulnerability assessment, and 3) capture those mitigation plans under a separate mitigation plan (similar to the action plans for Cyber Assets vulnerability assessments) or include "associated modifications to the time line".
Kansas City Power & Light	No	Same comments about "third-party" from Question 2.
NCPA Compliance Management Operating Committee	No	Same line of reasoning as given in the response to the question 2. If the Applicability Section were changed R1, R3, R4,and R5 could be combined together and R2 and R6 could be combined together. This simplifies the standard and gets to the heart of the Reliability Concern without creating a Consulting industry to perform third party reviews.(If you don't like the suggestion, maybe I found a new business opportunity)
Southern California Edison Company	No	SCE has concerns with Requirements R4, R5, and R6 that will be described below.With respect to Requirement R4, SCE notes that entities are required to "...conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s)..." SCE requests the inclusion of additional guidance or examples of threats and potential vulnerabilities that an entity may want to consider. This will allow entities to perform a threat assessment and develop preventative measures that are commensurate with the intent of the standard. In addition, SCE requests additional guidance on physical security plans that allow for flexibility to deal with emergent threats. With respect to Requirement R5, SCE believes that in the guidance section, the drafting team should consider referencing standards that are used by security

Organization	Yes or No	Question 3 Comment
		professionals or organizations, in order to ensure that the criteria to identify appropriate countermeasures to potential threats and physical attacks are evaluated along similar themes across industry. SCE also requests that the team consider rephrasing R5.1 from “Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond...” to describe the control, to "...deter, detect and delay, and also assess, communicate, and respond..." With respect to Requirement R6, SCE requests that the team consider rewording Requirement R6.1 from “Each Transmission Owner and Transmission Operator...” to “Each Transmission Owner or Transmission Operator, with facilities identified as a result of R2,...”
Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.	No	Specifically, Vectren recommends that R6 be removed from the draft standard, for the reasons set out in this Comment. And that an approach similar to that used for evaluation of designations under CIP 002 Version 3 be adopted for review of the required risk assessment. Vectren urges FERC and NERC to establish clear criteria for verifiers, so that NERC auditors can apply a uniform set of criteria to their after the fact assessment of verifier qualifications. As written, these provisions lack the specificity necessary to provide clear direction to entities, increasing the risk of later non-compliance. Such a risk is ironic and unacceptable in requirements that purport to provide a review of risk assessments. Under these draft requirements entities have no assurance that any third party verifier they might select will be considered “qualified” by FERC, NERC or NERC auditors who might review the results later - leaving entities at grave risk of compliance violations if FERC, NERC or any other regulatory body later disagrees with the entity’s selection of a third party verifier. Vectren strongly urges NERC and FERC to establish criteria for those who might seek to be designated third party verifiers, rather than leave assessment of qualifications to an after the fact review during a NERC audit or spot check. A lack of certainty leads here by necessity to a lack of confidence in the result, which Vectren surmises was not the intent of FERC or the drafters.

Organization	Yes or No	Question 3 Comment
Southwest Power Pool Regional Entity	No	SPPRE disagrees with the inclusion of Requirement 4.2. Prior history is not a predictor of future events and could result in critical facilities not being protected until after a sucessful first damaging attack with adverse BES reliability impact. Requirement 5.3 should be a project plan with measurable milestones for implementing the physical security enhancements and modifications.
Salt River Project	No	SRP supports comments submitted by APPA with the following additions:Third Party Verifiers:SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance

Organization	Yes or No	Question 3 Comment
		responsibilities.Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers.Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
David Kiguel	No	Sub-requirement 6.1.1: While Certified Protection Professional (CPP) or Physical Security Professional (PSP) might be recognized certifications in the U.S.A., that is not necessarily the case across the Canadian Provinces. Recommend to add: “or equivalent in those jurisdictions where such certifications are not recognized.”Sub-requirement 6.4: In addition to the non-disclosure agreements referred to in this sub-requirement, the standard should specify that the reviewing individuals having access to the confidential information must have security clearance and training, similar to the requirement in other CIP standards. Also, the security clearance must be obtained according to the established procedures in the respective jurisdiction.

Organization	Yes or No	Question 3 Comment
Encari	No	The approach taken by the Nuclear Regulatory Commission, which prescribes specific physical protections for nuclear plants and materials in 10 CFR Part 73, is instructive. Applicable Transmission Facilities, which are subject to common potential threats and vulnerabilities, warrant minimum physical security protective measures. Physical security plans should incorporate those prescribed protective measures unless a responsible entity can establish that its validated security plan provides a comparable level of protection required by the Standard.
Hydro QuÃ©bec TransÃ‰nergie	No	The same comments regarding the term "unaffiliated" in Question 2 above apply to R6.HQT believes that the SDT should remain general about the security measures that should be put in place. Requirement R5.1 states "Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4." We believe that rather than the standard dictate what type of measures are to be implemented, it should be rephrased to remain general and use similar language that is used in paragraph 9 of the FERC order. Suggest rewording the requirement to "Resiliency or security measures designed to protect against potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4.".
Foundation for Resilient Societies	No	The third party review is not adequately specified. The Joint U.S.-Canada Outage Tasf Force Report (April 2004) determined that lack of Reliability Coordinator oversight, and legal authority, contributed to inadequate supervision of transmission operators, and reduced visibility of regional inadequacies. See our comment to Question 1 for our view that Reliability Coordinators and Balancing Authorities must be involved.
FortisBC	No	The third party review of the security plan does not guarantee an objective evaluation as they would be funded by the requesting entity. The standard could state that the entity should follow an industry standard technical guideline.The audit provides an independent review of an entity's application of the industry standard technical

Organization	Yes or No	Question 3 Comment
		guideline and therefore, an additional third party review should not be required as described in R6.
Tri-State Generation and Transmission Association, Inc.	No	Tri-State disagrees that the FERC order specifically forces the drafting team to have a requirement for 3rd party verification. The order uses the word “should,” not “shall” or “require.” Tri-State would argue that 3rd party verification would/will occur during scheduled audit times. Again if the drafting team feels a need to require an additional 3rd party verification, it should require the Regional Entity or Reliability Coordinator to request the plans.
Consumers Energy Company	No	We agree to the approach, however, our concern is around protection of information shared between the entity and the third party. There should be a requirement within the standard that requires the third parties to protect the information and not leave it up to the entities.
Public Utitliy District No. 1 of Cowlitz County, WA	No	We are very concerned with the preferential endorsement this Standard affords to ASIS International. We know of at least one other security organization that offers a security certification: the Certified Homeland Protection Professional (CHPP) designation form the National Sheriffs' Association Institute for Homeland Security. If this requirement is left unchanged, FERC's statutory obligation in determining a proposed reliability standard is "not unduly discriminatory or preferential" may trigger the standard to be remanded back to NERC. It is for this concern, and only this concern Cowlitz votes negative. However, Cowlitz plans to vote affirmative in the final Ballot, regardless of any concerns to allow NERC to meet FERC requirements.
Cooper Compliance Corp	No	We do not support the Standard for the same reason above. We do not support a third party review requirement other than that of the existing Standards. That is a review by FERC, NERC or the appropriate region.

Organization	Yes or No	Question 3 Comment
self	No	While the reqirement for unafflilated third party verification of the security plan is required by the FERC order, I believe the mandate will lead to future security compromises.
Western Area Power Administration	Yes	: We recommend striking the qualifier regarding the ASIS “Certified Protection Professional or Physical Security Professional” from the standard R6-6.1.1 as it is inclusive of only one organization and may not provide the best support for each entity . Simply having these certifications does not guarantee the necessary knowledge to perform this unique work. We believe the language does not support the intent of the FERC Order as identified in paragraph 11.We request the Drafting Team clarify the scope of the third party review process identified in R6 and tie the requirement to a specific and established method as consistent in accepted practices, such as the ISO processes. We recommend the third party review process be clarified as a review of the primary entity’s adherence to their established processes in evaluating threats and vulnerably, as well as their security plan(s). We believe the current audits conducted by the regional entities satisfy the third party review process as identified in the FERC Order, paragraph 11.We do not believe R6-6.4 adequately protects the sensitive information contained in the risk, threat, and vulnerability assessments, or the security plan(s). These reports may contain sensitive and/or classified information, or otherwise information that if released would jeopardize the BES, with little to no penalty for an offending party.
Utility Services	Yes	1. R4, what is the time frame for the evaluations? Is this to be conducted during the 30 or 60 month cycle outlined in R2 or more frequently? 2. R6.1, These are all “or” statements and 6.1.1 through 6.1.4 should be bullets, not numbers (this is outlined in the CIP-002-5 page 6, and should maintain consistency with the CIP standards format). 3. R6, Does the ERO have to approve of the third party reviewer? Is there going to be a criteria to determine “demonstrated physical security expertise”?
ATCO Electric	Yes	AET agrees with the flexible approach outlined by the draft standard and respectfully offers these following comment for the drafting team’s consideration:R4 - Please

Organization	Yes or No	Question 3 Comment
		consider altering the wording of the final sentence of R4 to "The evaluation shall consider, at a minimum, the following:". This allows additional flexibility for entities with existing physical security assessment programs to continue to include those extra elements within their plans.R5 - For the timeframe dependency please consider altering the dependent requirement to R4 instead of R2. Within the rationale section the drafting team concedes that R4 must be completed prior to commencing R5 and the drafting team also states that R4 does not state when the evaluation must occur, only that it must occur in time to meet R5. AET respectfully suggests that a linear progression be established just as in R1, R2, and R3. This would require a timeline be added to R4 for the completion of the physical security risk assessment (AET suggests 120 calendar days from the completion of R2). AET also respectfully suggests that R5 then be made dependent on the completion of R4 (AET suggest 120 calendar days from the completion of R4).R6 - Please consider the removal of the required certifications in R6.1.1. The FERC order specifies that the risk assessment be reviewed by "[...] or another entity with appropriate expertise" and does not specify any particular qualifications. In addition, no other CIP standard calls for specific certifications or qualifications. Neither engineering focused requirements (e.g. CIP-002) or cyber security focused requirements (e.g. CIP-003, 005, 007) specify that those requirements be reviewed or implemented by designated engineers or certified security practitioners (e.g. CISSP). The due diligence required of the entity will determine the level of rigor that that entity is comfortable with defending and should not be included in the standard.
American Public Power Association (APPA)	Yes	APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members.R4 CLARITY - Under R4, combining the applicability of this requirement to both TOs and TOPs with applicable control centers within a single sentence is confusing and could be read to imply that a TOP that is affiliated with a TO must arrange for a separate third party review. We recommend

Organization	Yes or No	Question 3 Comment
		revising R4 to read as follows:R4 Each Transmission Owner that owns a Transmission station or Transmission substation identified in Requirement R1 and verified according to Requirement R2, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s) and Transmission substation(s), identified in Requirement R1 and verified according to Requirement R2. Each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to their primary control center identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: [VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning] R4.2 TYPO - Please change: "Prior history or attack..." to "Prior history OF attack..." Make conforming edits to the RSAW. 30-MONTH CYCLE - Identification of new threats and vulnerabilities in R5.4 does not change the 30-month cycle for conducting reliability studies and security evaluations: The standard needs to make clear that the security plan needs to take into account threats and vulnerabilities that are known at the time the plan is developed and the approved plan is capable of addressing new threats and vulnerabilities as they emerge, but that there is no NERC requirement to revise the plan between 30 month cycles and for the NERC CEA to audit such revisions. The TO should apply its existing security plans and procedures to evaluate and mitigate evolving security threats. The TO may also revise the security plan in mid-cycle if it so chooses without arranging for a third party review, but that action does not obviate its obligation to conduct the "subsequent" risk assessment and threat evaluation and security plan on the 30 month cycle. The CEA will audit the processes the TO uses to develop its plans, rather than the content of the plans.REQUIREMENT R5 CLARITY - R5 states in part that each TO and TOP "shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2." Please change "implement" to "complete." The use of implement can easily be read to require the actual

Organization	Yes or No	Question 3 Comment
		implementation of physical security measures within 120 days, rather than the completion of the security plan, starting the 90 day clock for unaffiliated third party review under R6. In contrast, R6 states that: "The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5."
Arizona Public Service Company	Yes	AZPS generally agrees with the approach of the standard as drafted. The following comments relate to suggested modifications or clarifications for Requirements 4-6.AZPS is concerned that Requirement 4.3, which requires the Transmission Owner to evaluate threat warnings from a myriad of sources, will result in inconsistent application by entities. The threat sources need to be consistent, and the threats evaluated must be relevant. AZPS suggests that a sector specific threat source be utilized to aggregate and disseminate threat information to ensure that relevant and timely data is analyzed consistently across the regions. This would also improve the auditability of the standard as well by removing the subjectivity associated with an unbounded number of threat sources. Requirement 6 requires Transmission Owners to secure a third-party review of the security plan developed under Requirements 4 and 5. AZPS strongly supports the development of security measures to protect critical substations. However, AZPS believes that requirements 6.1.1 through 6.1.4 add a level of specificity that does not provide an improved reliability benefit and has the potential to create a bottleneck that would make compliance within the short 90-day timeframe very difficult. AZPS contends that the most important quality of the third party reviewer is electric industry physical security expertise. Further, AZPS does not believe that the CPP or PSP certifications provide additional value from a realiability standpoint since neither certification has a sector specific focus. For these reasons AZPS would suggest that 6.1 be simplified to read: "Each Transmission Owner and Transmission Operator shall select an unaffiliated third-party reviewer with electric industry physical security expertise."
Tampa Electric Company	Yes	Comments to R5Tampa Electric Company appreciates the excellent work of the standard drafting team (SDT). They and their support staffs have evidently worked

Organization	Yes or No	Question 3 Comment
		very hard to produce in a very short time a family of documents that create a workable framework for improving the physical security of Transmission substations and primary Control Centers. We also commend NERC and the SDT for reaching out to the industry through a live a technical conference and by conducting a series Webinars in local and national venues. Moreover, we fully support the intent of the SDT as it has been articulated so well in the technical conference, in NERC and FRCC Webinars and in EEI and NATF conference calls. Unfortunately, there is a critical ambiguity in the text of requirement R5 that is problematic and needs to be addressed by the SDT. Our main concern is that requirement R5 literally reads that all provisions of the security plans for our primary control center and for all our substations and switchyards, including the installation and construction of any physical security upgrades, must be completed "within 120 calendar days following the completion of Requirement R2." Such a requirement may well be impossible to meet depending on the extent of the upgrades, the need for facility outages, and the number of locations that are affected.Members of the SDT have made it very clear in the Webinars and conference calls that they did not intend this result. Instead, the SDT intended to require registered entities, "within 120 calendar days following the completion of Requirement R2," to develop and document plans that include definite timelines for completing any security upgrades that are necessary to protect against the vulnerabilities and threats that are identified under requirement R4. Given that the text of R5 is contrary to the intent of the SDT, Tampa Electric urges the SDT to clarify that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work. This clarification can be accomplished in the guidance document to the standard or by our preference, editing the text of the standard and issue a revised standard for a second ballot. Removing "and implement" from the text of requirement R5 should remove the ambiguity and conform the text to the intent of the SDT. This edit, combined with R5.3 expresses the SDT's intent on this issue: R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to

Organization	Yes or No	Question 3 Comment
		Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following attributes: [VRF: High; Timeâ€ Horizon: Longâ€ term Planning]5.3. A timeline for implementing the physical security enhancements and modifications specified in the physical security plan.
FirstEnergy	Yes	FirstEnergy supports the proposed requirements R4 through R6 but offers two comments: 1) In regard to the inclusion of "primary control centers," we suggest the team add language within the Guidelines and Technical Basis section for requirement R4 and potentially the inclusion of an additional FAQ item to document some of the team's feedback provided during the webinar sessions. During the webinar the team provided a good explanation of how CIP-014 is uniquely different than physical protections provided under CIP-006 and that CIP-014 provides perimeter protection of the primary control center location or site and not just the subset of the control center that may house cyber assets protected under CIP-006. 2) Regarding requirement R5, during the industry webinars it became evident that there is some confusion associated with the word "implement" as used in the statement "shall develop and implement a documented security plan(s)" and that some industry stakeholders questioned if implement intended completion of all identified tasks stated within the plan(s). While FirstEnergy understood the requirement as described by the team during the webinars, to alleviate any confusion and better clarify the intended application, FirstEnergy suggests changing "implement" to "initiate" or "issue" so that it reads "shall develop and initiate a documented security plan(s)". This wording may better align with part 5.3 and the guidance provided in the Guidelines and Technical Basis section that states "Entities have the flexibility to prioritize the implementation of the various resiliency or security measures in their security plan according to risk, resources, or other factors."

Organization	Yes or No	Question 3 Comment
Idaho Power Co.	Yes	Further clarification is needed on several points. 4.2 & 4.3 leave open much room for interpretation under audit to say you did or didn't consider a particular source or threat. There is also some consternation over the use of "potential threat" in this requirement. There are a great many potential threats many that are so remote and nearly impossible to protect against that the risk does not outweigh the cost. It seems like these sub-requirements are a potential audit findings trap by the way they are worded. There are also no criteria specified for what the unaffiliated third party will be looking for in their review of the entity's evaluation. There is a great deal of concern for how these third parties will be able to handle or be willing to handle the influx of these reviews especially considering the short 90 day timeframe listed in 6.2.
Public Utility District No. 2 of Grant County, WA	Yes	GCPD appreciates the flexibility built into the Standard language that allows tailored evaluations of potential threats and vulnerabilities to its own facilities. GCPD supports APPA's suggested edits to the Standard to enhance clarity of requirements under R4, R4.1 & R4.2.In addition, APPA's suggested removal of “and implement” under R5 clarifies that the intent of R5 is to develop the physical security plan, not fully implement the plan within 120 calendar days. This would better align the Standard language contained in R5.3.
Vermont Transco LLC	Yes	how long will and entity have to complete their plans designed due to the evaluation of threats? It appears that the standard is saying that you must develop a plan and a timeline to complete your actions associated with the plan. What if a timeline needs to be adjusted at some point, will an entity have to notify their RRO? Or just track all changes and their need to provide to an auditor during a full audit of the standard?
Portland General Electric	Yes	In Requirement R4 the phrase “owns or operates” is used for the first time. If Transmission Owner Entity A is also a Transmission Operator of a line it does not own, and that line was identified by Transmission Owner Entity B in Requirement R1 and verified according to Requirement R2, Entity A could be responsible for evaluating and protecting that line under this wording. However, there is no mechanism built into the standard to communicate this information or to allow the Transmission Operator to

Organization	Yes or No	Question 3 Comment
		dispute the decision. In addition, Requirement R4.2 should be changed to "[p]rior history of attack."In addition, in Requirement R4.3, the current wording places an unrealistic and unclear burden on every Transmission Owner to monitor intelligence or threat warnings from an open-ended list of sources. We recommend changing the wording from "[i]intelligence or threat warnings from sources" to "[i]intelligence or threat warnings received from sources" to narrow the obligation to information that the Transmission Owner actually received from its monitoring activities.In addition, in Requirement R5, the phrase "owns or has operational control over" is used for the first time. It's not clear why this needs to be different from the "owns or operates" in Requirement R4. Consistent terms should be used to decrease potential confusion.In addition, as above, PGE believes that the 90-day period to review each entity's evaluation and security plan is too short. Again, we propose replacing the R6.2 language, "[t]he Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5," with the language, "[t]he Transmission Owner or Transmission Operator, respectively, shall ensure that any agreement executed with the unaffiliated verifying entity stipulate that the verification be completed by a date that is not later than 90 calendar days from completing the security plan(s) developed in Requirement R5."
MidAmerican Energy Holding Company	Yes	MEHC agrees with the R4 through R6 approach. However, MEHC suggests the following changes to improve the standards as written: The following rewording of R5 is recommended to clarify that the "build out" of security enhancement schedule. R5 Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The plan shall be completed

Organization	Yes or No	Question 3 Comment
		within 120 calendar days following the completion of Requirement R2. Implementation of the plan shall be as documented in the plan.
NRG Energy, Inc.	Yes	NRG agrees the approach described in Requirements 4 through 6 addresses the directives specified in FERC Docket No. RD14-6-000. However, NRG does have concerns with the standard as currently composed and offers the following points it believes will improve the standard if implemented: o R5.1 provides no guidelines or examples of how to combat certain threats, or even what threat thresholds require accounting for. NRG appreciates the flexibility built into the requirement. However, NRG is concerned this flexibility could result in "interpretation" issues during future audits of compliance with the standard. o The ability to meet the time horizon commitment for providing the third party assessment of the vulnerabilities and security plan are contingent upon the availability of certified parties that can adequately perform these assessments. NRG is concerned there may be a lack of qualified resources available to the industry to complete the necessary reviews within the required time frame. o Because the reliability of the bulk power system depends on numerous susbstations all across the nation, it would be more effective to increase the monitoring of the grid to ensure timely, effective re-routing of power when a disruption occurs. o Minimum physical standards should be established within the security plan that include industrial standard chain link fencing with barbed wire topguards; gates secured with chains and locks (not the alloy metal collar around a post); signage that clearly states No Trespassing every 100 ft., or on each perimeter side at small footprints; cameras that are monitored by the appropriate transmission control center, security control center or a contract central monitoring service and capable night viewing to be able to identify intruders.
Minnesota Power	Yes	Overall Minnesota Power agrees with the approach laid out by the Standard Drafting Team in Requirements 4-6, but requests that the SDT consider modifying the wording of R5.1 as follows.Resiliency or security measures designed to deter, detect, delay, assess, communicate, or respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4.An auditor could

Organization	Yes or No	Question 3 Comment
		interpret the use of “and” in “...deter, detect, delay, assess, communicate, and respond...” to mean that each resiliency or security measure be designed to meet all of these, where we believe and hope that the intent of the sub-Requirement is that the resiliency or security measure identified in the physical security plan be designed to “...deter, detect, delay, assess, communicate, or respond...”, while recognizing that it may meet more than one.
Xcel Energy	Yes	Overall Xcel Energy agrees with the approach, but we offer the following items for consideration of the Standard Drafting Team.The rational for R4 and R5.1 indicate that there is no required timeframe to complete the evaluation of the potential threats and vulnerabilities to identified facilities, but it does indicate the linkage of completing this when the physical security plan developed as part of R5 and within 120 days of completion of R2. We suggest that it might be more efficient to combine R4 and R5 or clearly show the linkage to reduce confusion about the timing of these two activities. Maybe the standard should require entities to develop a physical security plan after the risk assessment is completed, not after a verification of facilities as specified in R2. If R2 returns a null set, this seems ambiguous as we may still be required to have a physical security plan, even if blank. Since R4 would only be considered applicable if the R2 risk assessment process identifies facilities, referencing R4 in R5 would seem more intuitive.R5.2 states that the physical security plan must include law enforcement’s contact and coordination information. However, guidance on law enforcement and coordination has already been established with the adoption of EOP-004-2. It is also unclear by what is meant by “coordination”. Since reporting a physical threat to a Facility is a requirement of EOP-004-2 and in order to remove ambiguity around the word coordination, we propose changing R5.2 to read “notification of law enforcement consistent with EOP-004-2”. This would avoid potential confusion whether the R5.2 requirement is different than the EOP-004-2 requirement.R6.1, While there will be some regional variances, if an entity spans multiple regions or even some governmental agency jurisdictions, what protection does an entity have against reviewer discrepancies or differences? For example, the Xcel Energy registered entities anticipate using a common risk assessment methodology, and similar security plans. It

Organization	Yes or No	Question 3 Comment
		would be efficient to have a single evaluator provide the review for all three Xcel Energy registered entities. It would also be important for Regional Entities to apply consistent criteria when auditing the risk assessments and security plans.R6.1.2, if the ERO does not meet any or some parts of the criteria established in R6.1, it is uncertain how the ERO will be able to determine and approve an organization that does. Our security department, like the departments at other utilities of similar size, consists of a mix of multiple CPP and/or PSP holders, prior law enforcement professionals and several career military experts, including nuclear military asset security. It would seem that resources within the industry are the most knowledgeable resources available to evaluate physical security plans, given the criteria, and would have more utility specific knowledge than outside entities. Similar to our comments regarding R2.1, since the industry has the most knowledge on threats and vulnerabilities, and means to prevent them, we again propose adding an option to allow for industry (but non-affiliated) peer review of the physical security evaluation, either directly or through a group organization such as the North American Transmission Forum. Allowing peer review is likely to assist in identifying and disseminating best practices, thereby improving security. R6.3. Similar to our comments regarding R2.3, if no recommendations are made for changes to the evaluation by the unaffiliated reviewing entity, does this conclusion need be documented? Since some of VRFs are built off this requirement, it would seem to follow that all aspects be included to ensure certainty for the industry.
Pacific Gas and Electric Company	Yes	R4 (pg. 9) "...shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s)..." Comment: Consider stating "...conduct a physical security risk assessment to identify and evaluate potential threats and vulnerabilities..." The assessment should identify the potential threats and vulnerabilities to evaluate and implement the necessary protective, detective and corrective countermeasures R5 (pg. 10) states to develop and implement a documented security plan (s) within 120 calendar days of completion of R2 (unaffiliated third party verify the risk assessment form R1). Furthermore, R5.1 states to address the potential threats and vulnerabilities from R4. 120 days to implement

Organization	Yes or No	Question 3 Comment
		the countermeasures may not be enough time (logistics, procurement, installation timelines, approvals, etc.). Comment: Could they say "...shall develop and begin implementation of a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days..." because in R5.3 it requires a timeline for implementing the enhancements. 6.1.1. (pg.11) "An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification." Comment: Shouldn't require a specific certification, should say something like "The third party must include in their review the qualifications of the staff performing the review." R6.1.2 (pg. 11) "An entity or organization approved by the ERO." Comment: What criteria is the ERO using to approve entities or organizations? The approval process needs to be spelled out. R6.1.3 (pg. 11) "An entity or organization with demonstrated law enforcement, government, or military physical security expertise" Comment: Does this mean we can use Law Enforcement agencies or firms with retired law enforcement personnel?
ReliabilityFirst	Yes	ReliabilityFirst supplies the following comments for consideration:1. Requirement R5 - ReliabilityFirst requests clarification on why the term "primary control center" is used throughout the document instead of just "control center", as it seems both a primary and secondary control center would be of equal importance (and have similar vulnerabilities) to reliability.
PPL NERC Registered Affiliates	Yes	Requirement 5:In the VSL table, does implemented mean complete execution of the plan including any necessary construction, or does it mean having initiated the plan but not necessarily completed all planned construction? There are only 10 days between VSLs. Requirement 6:1. Similar to Requirement 2.3, the sub-requirements under Requirement 6.1 should be bullets, not individual sub-requirements. 2. Does R6 require subsequent third-party reviews when the security plan is revised? If so, what are the criteria?

Organization	Yes or No	Question 3 Comment
San Diego Gas & Electric	Yes	SDG&E agrees that an evaluation of potential threats and vulnerabilities of a physical attack to the facilities identified in R1 through R3 of the Standard is appropriate. Security threats and vulnerabilities can, and will vary from location to location and such differences must be accounted for in a robust security plan. It is appropriate and necessary that the Standard not mandate a one-size-fits-all approach, but requires entities to take into account the unique characteristics of each facility. SDG&E understands the Federal Energy Regulatory Commission's concern addressed by its Paragraph 11 directive that the Standard must have the analysis verified by an independent third party. While SDG&E believes it has in-house experts capable of performing such an analysis (as required by R4) and developing a Physical Security plan (as required by R5) adequately, SDG&E appreciates that verification by a third party, essentially a "second opinion," can serve to ensure a robust analysis of the physical security threats and vulnerabilities of facilities identified in Requirements R1 through R3. SDG&E appreciates the broad definition under R6.1 of what qualifies as a "unaffiliated third party reviewer." A list that unnecessarily limits possible reviewers could: 1) result in a bottleneck as too few potential reviewers are available for the industry to use; and 2) result in increased costs and a tight market for reviewers results in higher prices for their services.
Seattle City Light	Yes	Seattle City Light supports the Question 3 comments of APPA.
Seminole Electric Cooperative, Inc.	Yes	Seminole supports the comments by NRECA. Additionally, Seminole agrees with this approach. Requirements R4.1, 4.2, and 4.3 should be moved to the guidelines and technical basis as there is excessive flexibility provided to the auditor for concluding whether the evaluation is adequate and potential that an auditor may choose to determine that identification of events was inadequate. R5.2 requiring law enforcement contact information is redundant with EOP-004-2 R1. If an entity has a qualified third party perform the R5 security planning on behalf of or in cooperation with the registered entity, does this also meet the requirement R5? R6.4 is redundant with the information protection requirements in CIP-011-1. It would be appropriate to

Organization	Yes or No	Question 3 Comment
		note that this information is included in the materials subject to enforcement under CIP-011-1 R
Northeast Utilities	Yes	Suggest standard allow entities to have a Master Physical Security Plan and that the standard provide for flexibility to accomplish mitigation activities associated with the results of vulnerability assessments and capture those under a separate mitigation plan (similar to the action plans associated to vulnerability assessments being conducted on Cyber Assets).
PNM Resources	Yes	Support the comments submitted by EEI
Hydro One	Yes	The Standard allows the TO and TOP sufficient flexibility to complete R4, R5 and R6.
Con Edison and Orange & Rockland	Yes	
Duke Energy	Yes	
National Grid	Yes	
SPP Standards Review Group	Yes	
Ameren	Yes	
American Electric Power	Yes	
American Transmission Company, LLC	Yes	
Basin Electric Power Cooperative (BEPC)	Yes	

Organization	Yes or No	Question 3 Comment
California ISO	Yes	
Central Hudson Gas & Electric Corporation	Yes	
Clark Public Utilities	Yes	
Colorado Springs Utilities	Yes	
Edison Electric Institute	Yes	
Empire District Electric Company	Yes	
Exelon	Yes	
GridWise Alliance	Yes	
Independent Electricity System Operator	Yes	
ITC	Yes	
Minnkota Power Cooperative	Yes	
MISO	Yes	
Modesto Irrigation District	Yes	
Omaha Public Power District	Yes	
OPG	Yes	

Organization	Yes or No	Question 3 Comment
Pepco Holdings Inc.	Yes	
South Carolina Electric and Gas	Yes	
Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	Yes	
The Empire District Electric Company	Yes	
The Empire District Electric Company	Yes	
Westar Energy	Yes	
California Public Utilities Commission: Safety and Enforcenment Division		In general, the overall method employed in the draft standard is reasonable. The draft standard has adopted a reasonable level of specificity, without being overly prescriptive.The use of unaffiliated verifying experts is a positive element in the draft standard. In general, we believe that the balancing authority or reliability coordinator for the transmission area in question is the best verifying expert. In the event the utilities disagree with the assessments of the unaffiliated verifying entities at any point in the process (for example see section 2.3, second bullet point), not only should the transmission owner or utility be required to document their technical rationale, but the standard should further delineate a process for resolving this disagreement. Section

Organization	Yes or No	Question 3 Comment
		5.1 of the draft refers to “resiliency”. Does this term refers to actions such as building redundancy or improving protective schemes, as opposed to direct physical protection activities? The standard should clarify the meaning of the term resiliency.Section 4.1 of the draft refers to “unique characteristics.” Assuming this consideration includes availability of spares and ease of repair, the language is acceptable.With respect to Rule 5, section 5.2, the drafting group should consider language requiring the security plan to include contact and coordinating information for other utilities or important stakeholders, in addition to law enforcement.With respect to Rule R6, section 6.4 the language requiring “non-disclosure” agreements is important and a positive element in the draft standard. Section 4.2 lists the elements to be considered in evaluating the potential threats and vulnerabilities to physical attack, and specifically states "[p]rior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events and ...". We suggest that in additional to geographic proximity, that the section add language concerning "similarity of geographic characteristics". While geographic proximity, is a factor, ease of accessibility, layout and geographic contour, of an attacked facility is also important, if not more so.
ISO/RTO Standards Review Committee		The IRC has no comments on R4-R6.

4. **Do you have input on other areas of the standard or implementation plan not discussed in the questions above? If so, please provide them here, recognizing that you do not have to provide a response to all questions. Please limit your response to 300 words or less.**

Summary Consideration: The SDT appreciates all the additional comments submitted. All comments have been reviewed and changes that the SDT considers appropriate were incorporated into a subsequent revision. Several additions and clarifications were made to the Guidelines and Technical Basis section. A summary of comments and the SDT's response is provided. Note that some of the comments were previously addressed in preceding sections; the SDT's response is not repeated here.

- **Commenters suggested clarification of general terms including control center, primary control center, back-up control center, and widespread.** The SDT provided clarifications in the Guidelines and Technical Basis section.
- **A commenter recommended providing guidance for jointly owned substations.** The SDT has added commentary in the Guidelines and Technical Basis section to addresses joint ownership.
- **A commenter stated that the standard should explicitly allow a single plan to be developed to meet CIP-006 and CIP-014 requirements.** The SDT is aware that there may be a CIP-014-1 and CIP-006-5 physical security plan that differ, given that one is protecting against threats to cyber assets and another is protecting against physical threats. It is also aware the equipment and perimeters of protection will in many cases be significantly different between cyber assets being protected under CIP-006-5 and physical assets under CIP-014-1. Given these different purposes, the SDT believes it is appropriate to keep the physical security plans separate.
- **A commenter recommended providing clarification in the Guidelines and Technical Basis section to avoid placing risk on a verifier who is also a registered entity.** The SDT agrees that verifiers are not subject to violation of CIP-014-1. The plain language of CIP-014-1 in no way implicates that a verifier or reviewer, even if a registered entity, can be found in violation of CIP-014-1 for the work they do as a verifier or reviewer. Also, the language of Part 2.2 was revised to alleviate this concern.
- **A commenter suggested applying Cost Effectiveness Analysis Process (CEAP) to the standard.** The proposed Standard provides TOs and TOPs the ability to consider different methods to physically protect Transmission substations and stations and primary control centers implicated by this Standard. Therefore, the SDT believes that the application of CEAP is not needed.
- **Commenters proposed changing the implementation plan so that compliance with Requirement R1 would not occur simultaneously with the effective date of the standard.** The SDT considered alternate implementations but believes the proposed Implementation Plan provides entities sufficient time to complete Requirement R1 and strikes a balance between risk to the BPS and burden to the responsible entity.
- **A commenter recommended a SAR be developed to examine additional physical security issues and include additional entities in the physical security standards.** The SDT's scope is set forth in its SAR, and will work within that scope. The SDT considered and does not see the need to require the inclusion of RCs and BAs in the proposed Standard. Under the BA, EOP, IRO and TOP

standard families, RCs and BAs already have Real-time communication and oversight requirements, and the SDT does not see a need to duplicate those in CIP-014-1.

- Commenters provided editorial feedback on the VRF and VSL table that was accepted by the SDT where agreed.
- Commenters provided recommended changes to the RSAW which have been provided to the RSAW team.
- Commenters made suggestions regarding general readability of the standard; the SDT accepted recommendations where appropriate.

Organization	Yes or No	Question 4 Comment
FirstEnergy	No	FirstEnergy supports the proposed standard and appreciates the teams consideration of our comments intended to help clarify a few areas of the standard. FirstEnergy appreciates the team's efforts in producing a quality standard within an expeditious schedule and believes the team has provided a product that meets the core expectations described by the FERC Order.
ACES Standards Collaborators	No	Thank you for your time and consideration.
Ameren	No	We recommend adding language in the implementation guidance around the application of the terms 'control center', 'primary control center', and 'transmission station' in the draft standard.Obviously, there are a wide variety of understandings on these terms and additional clarity will help companies' ability to perform under the requirements. Considering that these terms have generic application to bulk power system reliability, the project timeline does not afford time for carefulconsideration of various facts and circumstances that might inform content offormal NERC defined terms.Also, we recommend that the standard drafting team (SDT) consider additions or changes to theimplementation guidance that will clarify several questions on the timing of the various implementation stages of the standard, including particularly that security plans are subject to change over time for a broad

Organization	Yes or No	Question 4 Comment
		range of reasons. In addition, we ask the SDT to consider clarifications in implementation guidance that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work.
Duke Energy	Yes	(1) Duke Energy suggests that language should be incorporated either in the proposed standard or RSAW to allow for the flexibility in modifying the timeline specified in R5.3. We believe there are unforeseen circumstances that could occur which would result in the proposed timeline shifting from the intended completion date.Examples include, but are not limited to:a. Unplanned outage of transmission or generation facilities that results in canceling scheduled work.b. BES reliability concerns should the facility be out of service for a short or extended period of time.c. Third party vendor's availability in implementing recommendations made by an entity or unaffiliated third party verifier.For these reasons, we believe a provision is needed to allow for this type of flexibility in modifying the timeline specified in R5.3.
Manitoba Hydro	Yes	(1) R6.1 - It is not clear whether only one or all of the qualifications in Section 6.1.1 through 6.1.4 must be met. Accordingly, R6.1 should be rephrased to refer to "one of the following".
Utility Services	Yes	1 "primary control center" is confusing. NERC has a defined term "Control Center" which is intentionally not being used. What is the intent of not using the defined term? If the undefined term remains in use more clarity needs to be given on "primary control center".2. what is the definition of "widespread?" Does this mean outside of a Balancing Authority Area, outside of a Region or outside of an interconnection? More clarity is needed in the term. Additionally, TO's may not have the data required to perform this type of assessment. There needs to be process in place for the TOs to obtain the data required to perform the appropriate assessment. 3. The SDT should review projects such as PRC-006 or MOD C, and define groups within the requirements to reduce the length of requirements. For example R4 could be reduced to the following, making the requirement easier to read and adding much

Organization	Yes or No	Question 4 Comment
		needed clarity: “Each Applicable Entity shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Applicable Facilities as identified in R1 and verified in R2. The evaluation shall consider the following:... “RSAW Comment:R1 “Evidence Requested” section doesn’t provide a time frame for the first assessment, no assessment prior to effective date will be considered, but there must be an assessment completed before the effective date to be complaint. This is a catch 22.
MidAmerican Energy Holding Company	Yes	1. The standard anticipates the potential for joint responsibility in involving transmission operator control centers for substations identified by transmission owners. It is suggested that additional guidance be provided regarding joint ownership of substations The following addition to the first paragraph under the Requirement R1 heading which is similar to an aswer to this questions in the webinars is suggested: For substations that are jointly owned the owners may jointly designate one of the joint owners to perform the risk assessment for that substation. 2. It is suggested that a clarification be made to the RSAW with regard to the following question: “ As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?” By referring to risk assessment this seems to imply the stations/substations identified after the completion of the requirement R1 risk assessment rather than just the applicability requirements. It is suggested that the words “as a result of your risk assessment” be deleted from this question. 3. Item 3. in the guidance for Requirement R2 seems to actually be guidance for Requirement R1. However, it does not provide useful guidance for Requirement R1; therefore, it should be removed. The guidance for Requirement R1 that gives the TO discretion to choose its own methods and criteria is preferred.4. The following modification to one of the sentences in the “Performing Risk Assessment” section of the guidance document is suggested: “Using engineering judgment, the Transmission Owner should develop criteria (e.g. imposing a fault near

Organization	Yes or No	Question 4 Comment
		the removed substation) to identify a contingency resulting in potential widespread instability, uncontrolled separation or Cascading within an Interconnection."
American Public Power Association (APPA)	Yes	APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members.See comments on definitions under Question 1.RSAW for R1 poses the following question: "As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?" This question combines a multi-step process into a single question that cannot be answered as yes or no by many TOs. Please break the RSAW for R1 into three discrete questions:1...Do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?2...Have you conducted a risk assessment of each applicable station or substation identified under Applicability section 4.1.1.?3...Did the risk assessment identify one or more Transmission station(s) and/or Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection?RSAW R1 evidence request text from near the top of page 6: (R1) Provide the current and the immediately preceding risk assessments conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant). The draft Implementation Plan states that the risk assessment required by R1 "must be completed on or before the effective date of the standard," yet the RSAW language provided above seems to exclude such an assessment.RSAW R1 "Note to Auditor" on page 7: "Review entity's answer to the above Question and if the auditor can verify the answer is 'no,' Requirements R3-R6 do not apply and no further audit testing of Requirements R3-R6 is necessary." The text appears to reference the following question from page 6: "As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months,

Organization	Yes or No	Question 4 Comment
		meeting the applicability requirements of 4.1.1?" This question is poorly worded, because TOs not meeting the applicability requirements of 4.1.1 are effectively exempt from this standard and do not need to perform a risk assessment.RSAW R3 "Question" on page 11: Please reword to add the following all caps text: "Are THERE any primary control centers identified in Requirement R1, Part 1.2 THAT ARE not under operational control of your NERC registration? RSAW R4 "Compliance Assessment Approach" on page 14: Change "or" to "OF" (R4 Part 4.2) "Prior history OF attack..." See the language used in the Guidelines and Technical Basis on page 31 of the standard.RSAW R5 "Note to Auditor" on page 16 states: "Auditor should cross reference the Transmission stations/substations and primary Control Centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 and the security plan(s) prescribed in Requirement R5 to ensure the plan addresses vulnerabilities that would facilitate physical attacks that have a high probability or likelihood of occurrence." The requirements of the standard do not address "probability" or "likelihood" of occurrence, so these factors should not be in scope of the compliance audit. Rather, auditors should address whether the security plan is complete and the TO or TOP addresses the issues raised by the third-party reviewer.
American Transmission Company, LLC	Yes	ATC supports the draft standard, with the realization that the aggressive time line has raised a broad range of issues or ambiguities resulting from the use of vague language or generic terms. While ATC understands the necessity for this approach, given the compressed timeframe directed by the FERC Order, the project's condensed timeline may not have afforded for the necessary and careful consideration of these terms. Improved guidance around the application of generic terms would increase clarity and help the industry. ATC also supports a follow up effort commensurate with typical standards drafting processes and timeframes to allow for further consideration, improvement, and cleaner language to assure effective implementation of the standard. An example of language like this is in Requirement R1, which includes the vague terminology of "widespread instability, uncontrolled separation, or Cascading." Risk assessment findings can vary

Organization	Yes or No	Question 4 Comment
		significantly depending on the assumptions, criteria, and methodology used for the assessment, and a more thoughtful use of terms could provide for a more uniform risk assessment basis.
Encari	Yes	CIP-014-1 should expressly permit one well-coordinated physical security plan for a Transmission Facility. As proposed, there could be a separate physical security plan under CIP-006-5 for BES Cyber Systems within an applicable Transmission Facility and potentially another physical security plan for the Transmission Facility as whole under CIP-014-1.
Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	Yes	Clarification should be made in the implementation guidance for CIP-014-1 that Verifiers who are also Registered Entities in functions applicable to CIP-014, are not subject to penalty under the requirements of CIP-014 due to verification duties performed at the request of a responsible Transmission Owner and/or Operator.
Tampa Electric Company	Yes	Comments: Comments to DefinitionsTampa Electric also urges the SDT to define certain terms that appear in the standard: 1) “Transmission substation” and “Transmission station,” 2) “collector bus,” and 3)”primary control center. There terms are not defined in the NERC Glossary and may not have definitions that are universally accepted by the industry. “Transmission substation” and “Transmission station”Many industry practitioners use the term “Transmission substation” generally, whether or not any transformers are installed in the facility they are describing. Other practitioners apply the term “Transmission substation” only to facilities that include transformers. The standard implicitly uses the term “Transmission station” in reference to transmission switching arrangements that do not involve transformers. However, the more commonly used term for a transmission switching arrangement that does not include transformers is

Organization	Yes or No	Question 4 Comment
		"Transmission switchyard." NERC addressed this issue in the Guidelines and Technical Basis section of CIP-002-5. The SDT could easily carry that text over to the Guidelines and Technical Basis section of CIP-014-1. However, it would be better to add definitions for "Transmission substation" and "Transmission station" to the Glossary of Terms Used in NERC Reliability Standards. The relevant text in CIP-002-5 is copied below for the convenience of the SDT.CIP-002-5 Guidelines and Technical Basis clarifications of "Transmission stations" and "Transmission substations" The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist."Collector bus""Collector bus" is another term that is not defined in the NERC Glossary and that may not have a definition that is universally accepted by the industry. "Collector bus" appears in 4.1.1.1 and in 4.1.1.2. of CIP-014-1 in text that was carried over from CIP-002-5.4.1.1 Transmission Owner that owns any of the following:4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. [Underlines added]4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a

Organization	Yes or No	Question 4 Comment
		Transmission Facility, but is part of the generation interconnection Facility. [Underlines added]If “Collector bus” is not defined or clarified, some TOs may conclude that some part of every transmission substation or switchyard that receives the output of a generator(s) is excluded from the scope of the standard. However, that is not the case nor the intent of the SDT. Therefore, the drafting team should consider whether it should define or clarify in the guidance document, the term “collector bus” “Primary control center”The NERC Glossary defines “Control Center” in this manner:One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.What might not be clear for the purposes of CIP-014-1 is what exactly distinguishes a “primary control center” from other alternate “Control Centers.” Some registered entities can operate substations from multiple locations. Often, there is one self-designated “main control center” or “primary control center” for which there might be multiple alternate or “backup control centers.” Given that alternate or backup control centers have capabilities that are comparable to so-called main control centers, it might not be clear in some systems whether “primary control center” in CIP-014-1 applies to more than one Control Center.The SDT can solve this problem by adding a definition of “primary control center” to the NERC Glossary or by adding text to CIP-014 that for each critical substation the TO or TOP can designate any Control Center as the “primary control center.”
Pacific Gas and Electric Company	Yes	Compliance 1.2 (pg. 13) Comment: can they clarify by being less wordy and just start by saying “The responsible entities shall retain documentation as evidence for three years”, followed by the rest in less words?
Public Utitliy District No. 1 of Cowlitz County, WA	Yes	Cowlitz commends the SDT's effort in a very difficult situation.

Organization	Yes or No	Question 4 Comment
Ciy of Garland	Yes	Definitions:primary control center - although not capitalized and therefore not a defined term, it is used in this standard in requirements 1, 3, 4, 5, and 6. The same term "primary control center" (again not capitalized) is used with a completely different meaning in standards EOP-008 in requirements 1.3, 1.5, 1.6, 2, 3, 4 and 7.1. Similarly "primary control room" is used in EOP-005 requirement 5 and in EOP-006 requirement 6 and is defined as the control center from which a TOP normally operates as opposed to the backup center. In CIP-014, it is defined/implied to be the control center that actually controls the circuit breakers at two or more substations. o If the term “primary control center” is used there will be confusion over the different meanings within the NERC Reliability Standards. o A completely different term should be used such as “primary local control center” or “primary transmission operations center”. The SDT apparently meant a "facility that has direct Supervisory Control". The term should be defined completely in the standard and should become a defined term within the Glossary of Terms used in NERC Reliability Standards. Proposed defined term:Primary Transmission Operations Center - One or more Transmission Owner or Transmission Operator facilities hosting operations personnel having primary operational real-time control of the BES elements in one or more remotely located substations using SCADA, EMS or other electronic means.”Please clarify whether these security plans are also required at any backup control center. Many of these control centers are generally not manned on a 24 by basis.unaffiliated - should be either defined or a footnote needs to be added to the Standard to explain that unaffiliated - means the selected verifying or reviewing entity cannot be a corporate affiliate, as stated in the guidance document. o Would two entities that do not have a direct ownership stake in each other but both are parties to an ownership in a third organization be considered to be unaffiliated? Example: Two utilities each have an ownership of a joint power plant but no ownership of each other. o What if they both had no ownership of the third party but both had purchase contracts with a third party? An explanation needs to be in the standard and not in the separate guidance document.

Organization	Yes or No	Question 4 Comment
Consumers Energy Company	Yes	Develop a requirement to protect information shared between entities and third party organizations. Requirement number 6 should be revised to state "...third party reviewer that is either..." 6.1.1 or 6.1.2 or 6.1.3 or 6.1.4. R6 seems vague and should be revised
Edison Electric Institute	Yes	EEI supports the draft standard CIP-014-1 as fully responsive to the FERC March 7 order. The project has moved along a very aggressive timeline and naturally raises a broad range of practical and implementation issues. Based on extensive discussions with member companies, EEI recommends that the standard drafting team (SDT) consider additions or changes to the implementation guidance that will clarify for companies several questions on the timing of the various implementation stages of the standard, including especially that security plans are subject to change over time for a broad range of reasons. In addition, EEI asks the SDT to consider clarifications in implementation guidance that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work.Observing the many meetings and webinars that have taken place recently, EEI also recommends that the SDT consider adding language in the implementation guidance around the application of the terms 'control center,' 'primary control center,' and 'transmission station' in the draft standard. Obviously, there are a wide variety of understandings on these terms and additional clarity will help companies' ability to perform under the requirements. Considering that these terms have generic application to bulk power system reliability, the project timeline does not afford time for careful consideration of various facts and circumstances that might inform content of formal NERC defined terms.
SPP Standards Review Group	Yes	Effective Date:The use of the term 'implement' needs clarification . To some implement means installed and in-service. To others it could mean a work in progress. The SDT recognized this confusion in the webinars on April 17 and we encourage them to modify the language to more clearly indicate the intent of the

Organization	Yes or No	Question 4 Comment
		drafting team. VSLs:Capitalize Part 2.3 in the Lower, Moderate and High VSLs for R2.Insert 'and verified according to Requirement 2' following the reference to Requirement R1 in all the VSLs for R5.Delete 'and modify or' in the last High VSL for R6.Guidelines and Technical Basis:Replace 'drafting team' with 'SDT' in the last paragraph under Section 4 Applicability on Page 27. Make the same change in the last paragraph on Page 32 under Requirment R6.Capitalize Remedial Action Schemes (RAS) and Special Protection Systems (SPS) in the paragraph at the top of Page 29. These are defined terms in the Glossary.Insert 'Transmission', capitalize 'Owner' and delete 'or operator' in the 1st paragraph under Requirement R2 on Page 29.Make 'outage' plural in Bullet c. at the top of Page 30.Capitalize 'Transmission Owner' in the 4th bullet in the middle of Page 30.Capitalize 'Owner' in the 1st line of the paragraph immediately preceeding Requirement R3.Insert 'Requirement' in front of R5 in the last line of the paragraph immediately preceeding Requirement R6.Spell out TO and TOP throughout the document. RSAW:The parenthetical statement in the 1st row of the table under Evidence Requested for R1 that states '...any risk assessments conducted prior to the effective date of this standard are not relevant...' is inconsistent with the statement on the Consideration of Issue or Directive in response to paragraph 12 of the FERC order. It states there 'This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard.' We believe the latter is consistent with the view expressed by SDT members on the two webinars conducted on April 17. This is also inconsistent with the posted Implementation Plan in which it states "The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard." Additionally, this is inconsistent with others standards in that action is sometimes taken prior to the effective date of the standard in order to be compliant when the standard becomes effective.Replace 'with' with 'within' in the 3rd row of the table under Compliance Assessment Approach Specific to CIP-014-1, R2. This is the row for R2, Part 2.2.Use lower case control center in the Note to Auditor box at the bottom of the table under Compliance Assessment Approach Specific to CIP-014-1, R4.The phrase 'and compensating mitigating

Organization	Yes or No	Question 4 Comment
		measures' in the 4th row in the table under Evidence Requested for R6 goes beyond the requirement in the standard. The requirement only calls for the reasons for not modifying the security plan according to the reviewer recommendations. It doesn't require the Responsible Entity to specify how it will mitigate the discrepancy.
Westar Energy	Yes	Effective Date:The use of the term 'implement' needs clarification . To some implement means installed and in-service. To others it could mean a work in progress. The SDT recognized this confusion in the webinars on April 17 and we encourage them to modify the language to more clearly indicate the intent of the drafting team. VSLs:Capitalize Part 2.3 in the Lower, Moderate and High VSLs for R2.Insert 'and verified according to Requirement 2' following the reference to Requirement R1 in all the VSLs for R5.Delete 'and modify or' in the last High VSL for R6.Guidelines and Technical Basis:Replace 'drafting team' with 'SDT' in the last paragraph under Section 4 Applicability on Page 27. Make the same change in the last paragraph on Page 32 under Requirment R6.Capitalize Remedial Action Schemes (RAS) and Special Protection Systems (SPS) in the paragraph at the top of Page 29. These are defined terms in the Glossary.Insert 'Transmission', capitalize 'Owner' and delete 'or operator' in the 1st paragraph under Requirement R2 on Page 29.Make 'outage' plural in Bullet c. at the top of Page 30.Capitalize 'Transmission Owner' in the 4th bullet in the middle of Page 30.Capitalize 'Owner' in the 1st line of the paragraph immediately preceeding Requirement R3.Insert 'Requirement' in front of R5 in the last line of the paragraph immediately preceeding Requirement R6.Spell out TO and TOP throughout the document. RSAW:The parenthetical statement in the 1st row of the table under Evidence Requested for R1 that states '...any risk assessments conducted prior to the effective date of this standard are not relevant...' is inconsistent with the statement on the Consideration of Issue or Directive in response to paragraph 12 of the FERC order. It states there 'This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard.' We believe the latter is consistent with the view expressed by SDT members on the two webinars conducted on April 17. This is also inconsistent with the posted Implementation Plan in which it states "The initial risk

Organization	Yes or No	Question 4 Comment
		assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard." Additionally, this is inconsistent with others standards in that action is sometimes taken prior to the effective date of the standard in order to be compliant when the standard becomes effective.Replace 'with' with 'within' in the 3rd row of the table under Compliance Assessment Approach Specific to CIP-014-1, R2. This is the row for R2, Part 2.2.Use lower case control center in the Note to Auditor box at the bottom of the table under Compliance Assessment Approach Specific to CIP-014-1, R4.The phrase 'and compensating mitigating measures' in the 4th row in the table under Evidence Requested for R6 goes beyond the requirement in the standard. The requirement only calls for the reasons for not modifying the security plan according to the reviewer recommendations. It doesn't require the Responsible Entity to specify how it will mitigate the discrepancy.
Florida Municipal Power Agency	Yes	FMPA has concerns for the RSAW and the lack of direction to auditors from the RSAW concerning the scope of their review. The auditor should not have a subjective decision regarding the sufficiency of the risk assessment, vulnerability assessment or security plan of the TO/TOP. The unaffiliated 3rd party is the source of qualified expert subjective opinion on the sufficiency of the risk assessment, vulnerability assessment and security plan. As such, the RSAW ought to clearly define the scope of the auditor's review of the risk assessment, vulnerability assessment and security plan. FMPA suggests rewording the "Compliance Assessment Approach"portions of the RSAW that call for these reviews to read something like the following (specific to R1):Review the entity's risk assessment to answer the following:a. Were all of the entity's assets, existing and planned to be in service within 24 months of the date of the documented risk assessment, and applicable to the standard (Applicability Section 4.1.1), included in the assessment?b. Was a transmission analysis or transmission analyses identified and documented to evaluate whether any applicable Transmission station(s) and Transmission substation(s), if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection? The auditor is not to evaluate the sufficiency of such analyses; but rather whether such analysis was documented.c. Was the assessment

Organization	Yes or No	Question 4 Comment
		conducted within the timeframes identified in bullet 1.1?d. Was the primary control center(s) identified in accordance with bullet 1.2?
Public Utility District No. 2 of Grant County, WA	Yes	GCPD feels that the implementation schedule is somewhat arbitrary and demonstating compliance with the implementation schedule conflicts with language contained in the proposed RSAW.GCPD supports RSAW edits as proposed by APPA to address these discrepancies.GCPD proposes the following edits to Requirement language addressing implementation timing to allow for enforceable and auditable time lines not dependent upon the unique completion date of the initial risk assessments conducted by the RE.2.2. ...The Transmission Owner shall ensure the verification of the initial risk assessment performed under Requirement R1 is completed within 90 calendar days following the effective date of this Standard.Subsequent risk assessments shall have verifications completed within 90 calendars days of completion of the risk assessment.R5. ...and primary Control Center(s) within 210 calendar days following the effective date of this Standard. Changes to recognized applicable facilities under this Standard as identified under Requirement R1 and verified according to Requirement R2, shall require review of the physical security plan(s) within 90 calendar days of completion of associated risk assessments. ...General commentary: in October 2012 the Cost Effective Analysis Process (CEAP) was approved for a “pilot”. The NERC CEAP was intended to integrate cost consideration and effectiveness into the development of new and revised standards. The first phase of the CEAP was to be implemented during the SAR stage to determine cost impact and identify “order of magnitude” or potentially egregious costs, to determine if a proposed standard will meet or exceed an adequate level of reliability, and what potential risks are being mitigated. The second phase was to be conducted later in the standard development process and afford the industry the opportunity to offer more cost efficient solutions that may be equally effective to achieving the reliability intent of the draft standard. This report would be posted at the time the standard is balloted. The report was intended to present the data collected in a manner which will provide the industry with representative cost implementation and effectiveness information to allow a more informed choice

Organization	Yes or No	Question 4 Comment
		during balloting. Based upon the urgent nature of this Standard, phase two would need to be applied. The CIP-014 Standard requires costs to be incurred to comply with Requirement R5. In addition, there may be substantial costs incurred to implement the Physicial Security Plan(s). The CIP-014 Standard is an ideal standard upon which to exercise the CEAP. The information resulting from the CEAP would be beneficial not only to government officials, but also the industry as a whole.
Georgia System Operations Corporation	Yes	GSOC supports the comments submitted by NRECA
Georgia Transmission Corporation	Yes	-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard.-GTC suggests that in M2 the word “communications” be changed to “notifications” to follow the language of t
GridWise Alliance	Yes	GWA includes electric utilities, information and communications technology service and equipment providers, Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs), academic institutions, and energy consulting firms. GWA appreciates the acknowledgment in the Order of the significant efforts that industry already is undertaking to enhance the resilience of the electric grid and thereby protect the grid from a range of threats, including physical, cyber, natural, and other hazards. Industry has been working in close partnership with various levels of government to enhance grid protection, reliability, resilience, and security. This collaboration is ongoing and should be fostered for the future.As you are aware, the electric grid is dynamic in nature. Electric grid owners and operators are making investments to enhance the reliability and resiliency of the grid, and are actively managing the operation of the grid to prevent outages and to restore power expeditiously, when outages do occur. As this process moves forward, GWA wants to underscore the importance that the result not be overly burdensome or inhibit innovation. It is important that the risk assessment process indeed be limited to truly “critical” infrastructure that is deemed essential to the functioning of the bulk electric

Organization	Yes or No	Question 4 Comment
		system. This will help ensure that protection measures are reasonable and cost-effective, as well as cost-sensitive, to help minimize costs to industry and also to consumers, who ultimately must bear the costs of these investments. Industry is working hard to monitor and stay ahead of the myriad threats that could arise - physical, natural, cyber, and otherwise - recognizing that the types of threats and the motivations of potential actors continue to change over time. NERC should partner with FERC to ensure that an all-hazards approach to addressing risk is undertaken going forward. We appreciate the Order's acknowledgement of the vital need to protect confidential and sensitive information. Yet, we are concerned about the nature of information-sharing under this Order, and what protections and assurances, in fact, would be implemented to prevent the inappropriate sharing of confidential information. While also recognizing the need to protect the confidentiality of such sensitive information, we also note that it is important to ensure that information sharing is facilitated between the government and the private sector, as well as within the private sector. Vendors who supply critical systems and equipment are incorporated into this process, since continued coordination and cooperation among all the stakeholders is essential.
Rayburn Country Electric Cooperative	Yes	I think the standard IF broken up into 2 standards (High, Med) should provide clearer guidance as to the expectations of the plans content. Similar to the issues that arose with the Low assets in CIP V5 . Give basic structure and content to be addressed to give FERC the assurance the specific concerns have been met.
Minnkota Power Cooperative	Yes	In the "Draft_RSAW_CIP-014-1_v1_2014_0409.pdf" document, on page 4 of 22, there is a Note to Auditors Concerning Third Party Verifications and Reviews. In this section there is a mention to the "concept of reliance means using the work of others to avoid duplication of efforts". While the reference to "duplication" was in regards to unaffiliated third party verifications and reviews, we appreciate the SDT be congnitive of "duplication of efforts" as their developing the Standard and the RSAW. With the very restrictive timeframe for which the development of the Standard was required, this concept can get lost. We did see another area in the Standard CIP-014-1 R5.2,

Organization	Yes or No	Question 4 Comment
		which may be considered “duplication of efforts”. CIP-014-1 R5.2 states, the TO/TOP should have in their physical security plan(s) law enforcement contact and coordination information. On June 20, 2013, FERC approved Reliability Standard EOP-004-2, which identified types of reportable events and thresholds for reporting, requires responsible entities to have an operating plan for reporting applicable events to NERC and other entities (including law enforcement), and requires reporting of threshold events with a 24 hour period (Docket No. RD13-3-000). This Standard covers the need to incorporate law enforcement contacts in the operating plan. Requesting this type of information in both the operating plan required in EOP-004-2 and physical security plan in CIP-014-1 is a “duplication of efforts”. MPC believes the intent for CIP-014-1 was to identify and mitigate physical security risks, while the intent for EOP-004-2 is to improve reliability of the BES by requiring the reporting of events by Responsible Entities. MPC suggests removing Requirement 5.2 in CIP-014-1.
Western Area Power Administration	Yes	In the VSL for requirement R5, in all four severity levels, states that the security plans need to be developed for the facilities “identified in requirement R1”. However Requirement R5 only requires the plans to be developed for facilities ‘identified in Requirement R1 and verified according to Requirement R2,”. The VSL should be modified to include the statement ‘and verified according to Requirement R2.The first row in the Table, in the RSAW, describing the evidence required in requirement R1, it states that any risk assessments conducted prior to the effective date of this standard are not relevant. The Implementation Plan states that “The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard.” There appears to be a conflict between these two statements, unless the intent is that the initial risk assessment needs to be completed on the effective date. Also, normally, unless the implementation plan provides a different time line, you need to be compliant by the effective date.In the RSAW for requirement R6 the fourth row in the Evidence Requested table, it asks for evidence that includes the “reasons or compensating mitigating measures for not implementing the recommendations for the reviewing party.” Requirement R6.3 of

Organization	Yes or No	Question 4 Comment
		the standard only requires the Transmission Owner or Transmission Operator to "Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation." These two statements should be clarified in order to ensure consistent enforcement.
American Electric Power	Yes	It is AEP's understanding that regarding R5, the phrase "develop and implement a documented physical security plan...within 120 calendar days" means that, within 120 days, the physical security plan must be completed and that the entity is working toward implementing the plan and does not mean that the plan must be fully implemented within 120 days. AEP urges the clarification of that expectation within R5 so that the requirement is unambiguous. Regarding R6.4, please clarify whether the procedures for protecting sensitive or confidential information would include suitable terms and conditions within a third party contract.
Northeast Power Coordinating Council	Yes	It is NPCC's expectation that RAI concepts will be applied to the operating and enforcement of this standard.
Omaha Public Power District	Yes	OPPD believes that the third-party verifications in requirements R2 and R6, to be performed once every 60 calendar months, not each time when a risk assessment analysis or security plan is changed that does not significantly change the facilities identified or the associated security plan. The transmission entity can still perform analysis and update security plan accordingly as required by this standard, however, the third-party verification should be reserved for major changes to the assessment or the plan or otherwise be done every 60 calender months.
Lincoln Electric System	Yes	R1 - It appears the intent of R1 is for a TO (which meets the applicability section 4.1.1) to perform a risk assessment (as defined in the standard) on only those substations that meet the applicability section 4.1.1, not all substations owned by a TO which meets the applicability section 4.1.1 description; however this is not 100% clear. The verbiage of the second sentence in R1 states "The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses

Organization	Yes or No	Question 4 Comment
		designed to identify any Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection." The use of the word "any" in this sentence has led some to believe that a TO (which meets the applicability section 4.1.1 description) will have to assess all of their substations, even those that do not meet the section 4.1.1 description. To address this possible issue, LES recommends replacing the word "any" in R1 with "applicable".R2 - Smaller TOs may not have the in-house resources to perform the risks assessments required in R1, and may need to contract with a third party to perform these assessments. If the performing third party is not affiliated with the TO, is a second unaffiliated third party verification required as stated in R2? Please revise the requirement to address this situation.
Bureau of Reclamation	Yes	Reclamation is concerned that the term "primary control center" will become confused with the NERC Glossary term "Control Center." As indicated by the use of the term "monitor" in the definition of Control Center, Reclamation does not believe that the concept of "operational control" has been equated with "causing direct physical action" to date. To avoid confusion, Reclamation suggests that the drafting team replace the R1 phrase "primary control center that operationally controls eachTransmission station or Transmission substation" with the phrase "primary control center that physically controls each Transmission station or Transmission substation."
City of Garland	Yes	Recommendation # 1 - Include the timeline diagram located in the FAQ document titled "CIP-014 Physical Security Process Flow" in the Guideline and Technical Basis section of the standard. This diagram clearly demonstrates the timing between the different requirements. Because of the subsequent risk analysis's in R1, verifications in R2, and potentially the processes outlined in R3, R4, R5, & R6, questions on timing (answered by the diagram) potentially will arise throughout the life of the standard. Recommendation # 2 - Add the words "catastrophic failure" to the Purpose statement. On a webinar, there was discussion concerning the Purpose statement and it was stated a number of times that "widespread instability, uncontrolled

Organization	Yes or No	Question 4 Comment
		separation" meant to convey the concept of "catastrophic" - there will be a lot of folks involved in the implementation of the standard who did not hear the webinar comments.Recommendation # 3 - Rather than the term "primary control center" used in all the proposed requirements, use a different term or phrase such as the "facility that has direct Supervisory Control". The word "direct" in the recommendation of "direct Supervisory Control" should replace the need for the word "primary" - primary makes one think of primary and backup (which is not addressed in the standard). The concern with using primary control center, even though "control center" is not capitalized, brings up a mental picture of primary (and backup) Control Centers as defined in the NERC glossary. The standard should be straight forward, not using terms that can be confused.
Seattle City Light	Yes	Seattle City Light supports the Question 4 comments of APPA.
Salt River Project	Yes	Section C "Compliance" 1.4 (page 13) which states "...all evidence will be retained at the TO and TOP facilities." is contradictory with NERC Compliance Monitoring and Enforcement practices which allow data to be exchanged with and sent to Regional Entities such as in pre-Audit data requests and Mitigation Plans. In addition, this would be burdensome for the TO/TOP because the 3rd party verifying/reviewing entities would need to be on-site and potentially incur travel expense.
Con Edison and Orange & Rockland	Yes	Section: PurposeComment: Use of term "primary control center" should be clarified. If an entity has a primary control center and a redundant back up control center, is the back up control center also in scope for CIP-014? Requirement 1: is the intent of the Standard that the R1 risk assessment be applied to transmission stations or substations identified under Applicability 4.1.1.4, as meeting NPIRs? Requirement 4: If under Requirement R4 a Transmission Owner owns or operates a single substation that employs multiple voltage levels, then which portions of that substation would be covered by CIP-014-1 and the Entity's physical security plan, and which would not be covered? Requirement 5: Consideration of transmission system "resiliency" is more

Organization	Yes or No	Question 4 Comment
		appropriate to be applied during the R1 risk assessment, as opposed to the R5 physical security plan. Recommend moving references to resiliency to R1.
Texas RE	Yes	Several places in the standard refer to notifying the Transmission Operator for stations that meet the higher risk profiles. However, the language is not clear as to what is expected from the Transmission Operators when a physical security incident occurs at one of those substations during real-time operations. Finally, this entire process can exceed four hundred days, which is excessive.
Xcel Energy	Yes	Since existing criteria from CIP-002-5.1 is used to identify facilities in scope, Xcel Energy suggests the addition of the proposed requirements be incorporated to CIP-006-5 (rather than in an entirely new standard) to more closely align and standardize the oversight of R3 and R6. In addition, this would centralize all physical security requirements within a single Standard. Additionally, there is a significant amount of language in the requirements to specify the affected parties. We suggest the Standard Drafting Team seek opportunities to more concisely outline the applicability and the subsequent obligations in the requirements, to improve ease of understanding. We see an opportunity for the audit or risk functions of the Regional Entities to align with the third party review criteria established in the proposed standard. Although the expertise to perform this function may not currently be in place, the Regional Entities could easily develop the knowledge and expertise, and the reviews could naturally integrate within their other review and assessment activities.Overall, the standard is very comprehensive as drafted and it is balanced in a manner that allows for maximum flexibility. Consistent with NERC's evolution to results-based standards, it is appropriate for the standard to focus on the desired results of increased security of critical facilities, rather than mandating rigid actions that may or may not be suitable for individual facilities and entities. Allowing industry the latitude to design its own mitigating measures ensures those measures will be the most practical and cost effective as appropriate for the particular nature of each facility. The flexibility of this proposed standard is the best opportunity for the industry to execute a comprehensive solution based on assessments and security

Organization	Yes or No	Question 4 Comment
		that relies on the unique design and characteristics of the operating systems of each utility.
Nebraska Public Power District	Yes	Since we are using CIP-002-5 for identifying Transmission stations and substations, the confidential information for these facilities is already protected under CIP-011-1 Information Protection. CIP-014-1, requirements 2.4 and 6.4 are redundant with already approved requirements and are not needed. Adding requirements for protecting sensitive or confidential information in this standard will create confusion and double jeopardy. CIP-006-5 covers physical security and any information pertaining to the substations identified through the CIP-002-5 criteria. CIP-011-1 already protects this information.Due to the expedited development of this standard, sufficient time isn't available to provide clear requirements in the standard to evaluate compliance. The RSAW does contain language that will help, but the RSAW isn't the enforceable document and can be changed without industry approval. We've learned from implementing the other CIP standards that auditors can take a completely different position than what was meant by the drafting team with little recourse for utilities.
Southwest Power Pool Regional Entity	Yes	SPPRE recommends that subsequent risk assessments should be peformed at least every 36 calendar months regardless of whether previous risk assessments had identified critical facilities. It is more important to identify facilities that should be on the list than those that might not need to be on the list anymore.
PNM Resources	Yes	Support the comments submitted by EEI
Bonneville Power Administration	Yes	The current draft requiring "unaffiliated" third party review is more restrictive than the requirements language in the FERC order and meeting an unaffiliated requirement will be problematic for federally owned power and transmission systems. Paragraph 8 of the order: "Thus, the Reliability Standards should require the owners or operator to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically

Organization	Yes or No	Question 4 Comment
		contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process." BPA's interpretation of the FERC order is that consultation with peer entities would be acceptable methods for review of evaluation processes. In fact the order by its wording encourages such consultations without restriction as to business or corporate relationships. The draft standard limits and excludes highly qualified security and technical expertise found across the industry and within entities corporate and governmental structures, hierarchies and partnerships where vast levels of experience, training and ability exist. The "unaffiliated" requirement forces entities to seek expertise where there may or may not be such expertise and where there is no track record of such expertise. The term "unaffiliated" and any reference to that level of separation between entities are completely void from the order and should be removed from the draft standard.Paragraph 11 of the FERC order: "In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity." BPA believes the draft standard limits and excludes highly qualified security and technical expertise found across the industry and within entities corporate and governmental structures, hierarchies and partnerships where vast levels of experience, training and ability exist. The "unaffiliated" requirement forces entities to seek expertise where there may or may not be such expertise and where there is no track record of such expertise. The term "unaffiliated" and any reference to that level of separation between entities are completely void from the order and should be removed from the draft standard.
Hydro QuÃ©bec TransÃ‰nergie	Yes	The following are suggestions to facilitate reading of the standard, as well as its future translation: All requirements: Replace the expression "Transmission stations and Transmission substations" with "Transmission facilities". Otherwise, please explain why such a distinction is necessary.R1: Remove "transmission analysis" from the sentence "The initial and subsequent risk assessments shall consist of

Organization	Yes or No	Question 4 Comment
		transmission analysis or transmission analyses designed to ..." We believe this repetition is unnecessary.R2.2: The first part applies to an entity that is not subject to the standard and should be removed from the standard.R2.3: Replace the word "identification" with "assessment". Remove the word "either"Rephrase R4, R5 and R6 (add "a"): " ...a transmission substation, or a primary control center".R4 and R5: Remove the part "...that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation". It only complicates the reading of the requirement (the TOP is not notified by the TO unless it has operational control over an asset identified in R1). If the first parts of R4, R5 and R6 are intended to identify the functional entities to which the requirement applies, we suggest "... and each Transmission Operator notified by a Transmission Owner under requirement R3, shall ..." for the TOP portion (line 3 to 6 of R4, R5 and R6). We believe that it would greatly improve clarity and readability of the requirements.R6.1: rephrase to "from one of the following". Furthermore, the numbers 6.1.1 to 6.1.4 should be replaced with bullets as is the case in R1.1, R2.1, and R2.2. Rephrase R6.1 and R6.1.1 to reflect the language used in the rationale. We believe limiting the reviewer to someone with a CPP or PSP certification goes beyond what the FERC order requesting. Suggest rephrasing to "with appropriate expertise of the evaluation performed".Guidelines and Technical Basis on requirement R1: HQT agrees with the fact that the TO has discretion to choose the specific method to establish the risk assessment, and that it is relevant that the Guidelines proposes examples. However, the proposed example of "removing all lines to a single Transmission station" seems to present a very stringent impact considering a physical attack on a facility. We ask the SDT to propose others less stringent examples that would be more in line with realistic physical attack, such as loss of a large section according to physical organisation of the facility, or loss of all main transformers, etc.
NCPA Compliance Management Operating Committee	Yes	The Implementation Plan is too agressive. I cite NCPA experience as described in our response to question 2. I find it interesting the the CIP-version 5 standards have

Organization	Yes or No	Question 4 Comment
		essentially a two year implementation plan for medium and high assets and yet this proposed standard has a 6 month implementation plan.
David Kiguel	Yes	The Implementation Plan obligates applicable entities to complete the initial risk assessment in Requirement R1, on or before the effective date of the standard. While performing and completing the vulnerability assessment before the effective date of the standard may constitute a recommended good practice, from a statutory perspective, compliance with the standard before its effective date may not be enforceable in all jurisdictions. An entity cannot be found in violation of the standard at a time when the standard is not yet effective. Recommend changing the implementation plan to require completion of the assessment after the effective date of the standard.
South Carolina Electric and Gas	Yes	The requirement for unaffiliated third party verification throughout this standard is not consistent with other NERC Reliability Standard verification requirements. SCE&G is concerned that this standard sets precedence for future standard third party verification which would be very costly, confusing and burdensome.
Basin Electric Power Cooperative (BEPC)	Yes	The SDT should be applauded for the diligent work performed in short order to meet the requirements of the FERC order RD14-6-000 while allowing flexibility in the manner the Registered Entity may be compliant.
Idaho Power Co.	Yes	There is great concern related to information protection related to turning over information concerning vulnerabilities of the grid and related facilities to outside parties. Even with the use of NDAs, these third parties are not subject to the same NERC reliability standards (i.e. CIP standards, information protection, etc) as the entities, will not be audited on their information protection practices, and may have no accountability to the regulators in the event of a disclosure of sensitive information, inadvertent or otherwise. It is a concern that the TO is responsible for 3rd party verification to be completed within a tight 90 day window, especially considering the critical infrastructure information being exchanged. Contractual

Organization	Yes or No	Question 4 Comment
		exchanges and negotiations could impede upon the 90 day window. Also, TO's may need time to review the R2 study results and possibly mitigate study discrepancies. The date R1 needs to be performed is unclear. Does it need to be performed within a certain amount of time after the effective date? The implementation plan states that the initial risk assessment must be performed on or before the effective date of the standard. However, the RSAW for R1 states that "any risk assessments conducted prior to the effective date of this standard are not relevant." Does this mean the initial risk assessment must be performed “on” the actual effective date of the standard? Is there a basis for the short notification window in R3? The seven calendar days window for the TO to notify the TOP seems quite short. Additionally, there is a discrepancy in the review timeframes in R1 in which a look ahead of 24 months is required for stations and substations that are in the planning process but the risk assessments are performed every 30 months leaving a 6 month gap in the analysis. It would also seem more intuitive and consistent with other CIP standards to have the risk assessment requirement performed on an even year rather than a 30 month basis (i.e. 36 months.)
Pepco Holdings Inc.	Yes	There seems to be a conflict between the RSAW, Consideration of Issues or Directives and the Timeline included in the FAQ. To meet the overall timeline for the entire standard, the risk assessment must be started prior to the Effective date of the standard. There should be no prohibition for completion of the Risk Assessment prior to the Effective date of the standard.The FAQ Timeline states:”Initial performance of R1 must be complete on or before the effective date of the standard...”The Consideration of Issues or Directives #12: “...This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard...”The RSAW under R1 Evidence Requested states: “Provide the current and the immediately preceding risk

Organization	Yes or No	Question 4 Comment
		assessments conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant)."
EF Cass Consulting Inc.	Yes	This standard has the perceived importance of protecting national security and being so critical as to expedite its development through modification of nearly all associated controls. I agree physical security of critical facilities is of paramount concern but not at the expense of producing a sound standard. After listening to two of the webinars it is clear to me that the majority of the entities responsible for ultimately complying with this standard and those that will enforce the requirements are unclear as to what is required. I would suggest running it past the "Experts" for their review prior to the first vote.
ITC	Yes	Transmission systems tend to have facilities for which inoperability, while not causing immediate system failure or separation, would nonetheless leave the system in a degraded state. This degraded state will require system operators to reconfigure the system in a way to mitigate the loss of such facilities, but at that point, a new group of facilities could effectively become "critical" as that term is currently defined in CIP-014-1. For example, the loss of a given substation may cause several transformers to be inoperable, and with the long lead time for replacement components, the transmission owner would realistically need to plan for the substation to be out of service for an extended period of time. During this time in which the substation is out of service, a second tier of assets may exist for which inoperability would now cause separation or failure of the type that would afford them a "critical" designation as currently defined under CIP-014-1. This condition would persist for as long as the original equipment was out of service. If the SDT were to adopt ITC's proposed modifications to R1 (see above), this would not be an issue, since all CIP-002-5 substations would already be covered by CIP-014-1. However, if the SDT chooses not to adopt ITC's proposal, the SDT should consider whether entities should assess the transmission system in this new degraded condition to determine if new critical assets are created due to the degraded condition (i.e., a reapplication of the analysis performed in the current R1 to determine if the loss of a particular substation causes

Organization	Yes or No	Question 4 Comment
		widespread cascading.) The Standard could also trigger additional transmission system studies to determine if the transmission system remains reliable during the extended period in which the critical assets remain out of service.
Florida Keys Electric Cooperative	Yes	Under the implementation plan for R1, how can compliance with a standard be required prior to the effective date of the standard? The drafting team should reconsider this element of the implementation plan. If included in future drafts, a legal opinion from the NERC General Counsel should accompany this issue for stakeholder consideration.
National Rural Electric Cooperative Association (NRECA)	Yes	Under the implementation plan for R1, how can compliance with a standard be required prior to the effective date of the standard? The drafting team should reconsider this element of the implementation plan. If included in future drafts, a legal opinion from the NERC General Counsel should accompany this issue for stakeholder consideration.
SERC CIPC	Yes	Until the process of the standards has more fully matured there should not be a presecribed methodology for conducting the Security Vulnerability Assesments (SVAs) as long as generally accepted criteria as well as as stated in the standard in 4.1, 4.2, and 4.3 are followed in the development of the evaluation and plan(s).The comments expressed herein represent a consensus of the views of the above named members of the SERC CIPC only and should not be construed as the position of the SERC Reliability Corporation, or its board or its officers.
Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.	Yes	Vectren recognizes that this drafting effort required significant contraction of drafting and approval processes, and Vectren appreciates the work of the drafting team. Vectren is supportive of the goals of the standard, supports R1, R3, R4 and R5. Vectren urges the drafting team, NERC and FERC to remove entirely or add detail to the requirements R2 and R6, and to add specific audit criteria in the RSAWs, so that

Organization	Yes or No	Question 4 Comment
		entities can have some confidence that their risk assessments performed in good faith, will be considered compliant with this Standard.
Foundation for Resilient Societies	Yes	We recognize that FERC has established a 90-day review process, and that NERC has worked to meet the tight deadline. Hence, the Foundation for Resilient Societies asks NERC to develop a SAR for Physical Security Standards - Phase 2. In this process, analytical modeling should be undertaken to identify and prioritize physical security risks that include cyber vulnerabilities, and that relate to the need for reliable warning and communications via redundant channels to control centers and to law enforcement. It should not be acceptable to exclude Regional Coordinators and Balancing Authorities, both groups needing to review and perhaps upgrade their own physical security, and both groups playing key roles in oversight of the operating entities, both TOs and GOs, whose physical security may be essential to prevent long-term outages through coordinated attacks. For additional materials prepared by the Foundation for Resilient Societies, contact the FERC staff designated to assist NERC with standard setting in FERC Docket RD14-6-000.
PPL NERC Registered Affiliates	Yes	We recommend that the SDT include a timeline within the standard which includes all required steps.
Cooper Compliance Corp	Yes	We would like to address proposed comments by APPA that additional Standards are added to address confidentiality. We do not agree with APPA's position. The functional model requires registered functions to work together to secure reliability. Already, as a result of CIP Standards, vital communications between the Distribution Providers/Load Serving Entities and the Balancing Authorities and/or Transmission Operators have been compromised. Often, The Balancing Authorities and Transmission Operators are in fear of sharing important information with the Distribution Providers and/or Load Serving Entities because they feel they could be subject to a CIP violation. In some cases the Distribution Providers and Transmission Operators even share facilities. Having a requirement that prevents sharing vital

Organization	Yes or No	Question 4 Comment
		information on physical security would simply not work and therefore we do not support APPA's comments.
Western Electricity Coordinating Council	Yes	WECC believes that the proposed standard addresses the FERC Order and has voted affirmative to approve CIP-014-1. However, as noted in our comments above we believe there is opportunity for enhancements and clarification that if implemented would improve the standard and still meet the FERC Order. WECC encourages the drafting team to consider implementation of these suggestions prior to the final ballot or NERC to submit a SAR for consideration of these suggestions immediately after approval of the standard.
Tri-State Generation and Transmission Association, Inc.	Yes	While the FERC Order RD14-6 paragraph 13 does require NERC to file a proposed standard within 90 days, footnote 8 only requires that the proposed standard include timelines for certain elements, without specificity for what those timeframes should be. The bright line CIP version 5 applicability that is used within this standard became effective 02-03-14 and was giving industry 24 months to implement. The CIP-014 draft appears to assume those bright line considerations are already completed for industry and provides just over 6 months to complete an additional assessment to remain compliant. Without specific implementation timeframes provided by FERC, and to stay in closer alignment to the expected completion dates for CIP v5, Tri-State is recommending no less than a one year after this standard becomes effective for the R1 risk assessment to be completed.
Hydro One	Yes	Will FERC accept R2.3 and R6.3, which allows the TO or TOP to document why they are not following the recommendations from the verification? The FERC Order did not suggest this.It is extremely important that all jurisdictions follow the same standard, so that the mitigation of risk to physical security is consistent. Having some jurisdictions who follow a more stringent standard will increase costs to ratepayers in those jurisdictions.The standard should provide a definition for "unaffiliated".

Organization	Yes or No	Question 4 Comment
Colorado Springs Utilities	Yes	
Empire District Electric Company	Yes	
OPG	Yes	
The Empire District Electric Company	Yes	
Herb Schrayshuen	Yes	The Implementation Plan can be read that it obligates applicable entities to complete the initial risk assessment in Requirement R1, on or before the effective date of the standard. The implementation plan should be adjusted. The following is a suggestion to facilitate reading of the standard and stay whitn defined terms without introfucing new terms which are undefined: For all requirements: Replace the expression "Transmission stations and Transmission substations" with "Transmission facilities". Otherwise, please explain why such a distinction is necessary. While the requirement for unaffiliated third party verification of the physical security plan is something required by the FERC in its order, the mandate is misguided and will lead to security breaches while at the same time adding no incremental value to the physical security plan. The utility, which owns the assets, is already highly incentivized to put together a good security plan to avoid loss of its facilities to terrorism without third party verification. The utility may decide to use security consultants to help develop the plan if it involves new, state of the art physical security topics outside the utilities experience base. On balance the third party verification requirement outlined in R6 regarding the physical security plan is unneeded.
NIPSCO		In R2 we are not sure who would do the verification. On one of the webinars a member of PJM suggested that another PJM member could be a candidate. However

Organization	Yes or No	Question 4 Comment
		it is likely that a PJM member is not a PC, TP or RC as prescribed in the requirement; that role is performed by PJM itself. Any further guidance would be welcome; we do not consider this a "show stopper".The hard work that went into putting this project together in such a short time frame is appreciated, thanks.

Additional comment received from Marcus Pelt, Southern Company

“The wording of Requirement R2.s, as it stands currently, could be interpreted to place requirements on the unaffiliated third party verifier when the responsible entity is actually the Transmission Owner. Southern recommends that R2.2 be reworded as follows to address this concern:

END OF REPORT

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. Nominations for the Standard Drafting Team (SDT) for Project 2014-04 Physical Security were solicited March 13-18, 2014, and the SDT was appointed by the Standards Committee on March 21, 2014.
2. Technical Conference was held April 1, 2014.
3. The draft standard was posted, pursuant to a Standards Committee authorized waiver, for a 15-day Formal Comment Period with a 5-day Initial Ballot April 10-24, 2014.

Description of Current Draft

This is the second draft of the proposed Reliability Standard, and it is being posted for final ballot. This draft includes proposed requirements to meet the directives issued in the FERC order issued March 7, 2014, in Docket No. RD14-6-000, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

Anticipated Actions	Anticipated Date
5-day Final Ballot, pursuant to a Standards Committee authorized waiver.	May 1, 2014
BOT Adoption.	May 2014
File with applicable Regulatory Authorities.	No later than June 5, 2014

Version History

Version	Date	Action	Change Tracking
1.0	TBD	Effective Date	New

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the NERC Glossary of Terms used in Reliability Standards (Glossary) are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

A. Introduction

1. Title: Physical Security

2. Number: CIP-014-1

3. Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner that owns a Transmission station or Transmission substation that meets any of the following criteria:

4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

4.1.1.3 Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or

Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

5. Effective Dates:

CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

This Reliability Standard addresses the directives from the FERC order issued March 7, 2014, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014), which required NERC to develop a physical security reliability standard(s) to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

B. Requirements and Measures

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or
- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

Rationale for Requirement R1:

This requirement meets the FERC directive from paragraph 6 in the order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through widespread

instability, uncontrolled separation, or cascading failures. It also meets the portion of the directive from paragraph 11 for periodic reevaluation by requiring the risk assessment to be performed every 30 months (or 60 months for an entity that has not identified in a previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection).

After identifying each Transmission station and Transmission substation that meets the criteria in Requirement R1, it is important to additionally identify the primary control center that operationally controls that Transmission station or Transmission substation (*i.e.,* the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or

- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

Rationale for Requirement R2:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring verification by an entity other than the owner or operator of the risk assessment performed under Requirement R1.

This requirement provides the flexibility for a Transmission Owner to select registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term “unaffiliated” means that the selected verifying entity cannot be a corporate affiliate (*i.e.*, the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit. The term “unaffiliated” is not intended to prohibit a governmental entity from using another government entity to be a verifier under Requirement R2.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout the Requirement R1 risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform a Requirement R1 risk assessment to satisfy both Requirement R1 and Requirement R2 concurrently.

Planning Coordinator is a functional entity listed in Part 2.1. The Planning Coordinator and Planning Authority are the same entity as shown in the NERC Glossary of Terms Used in NERC Reliability Standards.

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Rationale for Requirement R3:

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first identifying which Transmission stations and Transmission substations meet the criteria specified by Requirement R1, as verified according to Requirement R2. This requirement is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1, Part 1.2 of a Transmission station or Transmission substation verified according to Requirement R2 receives notice of such identification so that the Transmission Operator may timely fulfill its resulting obligations under Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include notice of the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or the verification process under Requirement R2.

R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement

R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Rationale for Requirement R4:

This requirement meets the FERC directive from paragraph 8 in the order on physical security that the reliability standard must require tailored evaluation of potential threats and vulnerabilities to facilities identified in Requirement R1 and verified according to Requirement R2. Threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections, and attractiveness of the target. As such, the requirement does not mandate a one-size-fits-all approach but requires entities to account for the unique characteristics of their facilities.

Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur or be completed. However, Requirement R5 requires that the entity's security plan(s), which is dependent on the Requirement R4 evaluation, must be completed within 120 calendar days following completion of Requirement R2. Thus, an entity has the flexibility when to complete the Requirement R4 evaluation, provided that it is completed in time to comply with the requirement in Requirement R5 to develop a physical security plan 120 calendar days following completion of Requirement R2.

R5. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical

security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan.

Rationale for Requirement R5:

This requirement meets the FERC directive from paragraph 9 in the order on physical security requiring the development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

R6. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.
- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or
- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Additionally,

examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

Rationale for Requirement R6:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring review by an entity other than the owner or operator with appropriate expertise of the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5.

As with the verification required by Requirement R2, Requirement R6 provides Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout the Requirement R4 evaluation and the development of the Requirement R5 security plan(s). This would allow entities to satisfy their obligations under Requirement R6 concurrent with the satisfaction of their obligations under Requirements R4 and R5.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

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

The Transmission Owner and Transmission Operator shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation.

The responsible entities shall retain documentation as evidence for three years.

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

The CEA shall keep the last audit records and all requested and submitted subsequent audit records, subject to the confidentiality provisions of Section 1500 of the Rules of Procedure and the provisions of Section 1.4 below.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information

Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**High**	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection	Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.	Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.	performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.	uncontrolled separation, or Cascading within an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
R2	**Long-term Planning**	**Medium**	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than or equal to 100 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.	less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.	120 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed	following completion of Requirement R1; OR The Transmission Owner failed to have an unaffiliated third party verify the risk assessment performed under Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by Part 2.3.	
R3	**Long-term Planning**	**Lower**	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.	operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.	of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.	center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						identification in Requirement R1.
R4	**Operations Planning, Long-term Planning**	**Medium**	N/A	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
R5	**Long-term Planning**	**High**	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.	The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						center(s) identified in Requirement R1 and verified according to Requirement 2 but failed to include Parts 5.1 through 5.4 in the plan.
R6	**Long-term Planning**	**Medium**	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed	The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.	under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.	under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not document the reason for not modifying the security plan(s) as specified in Part 6.3.	the security plan(s) developed under Requirement R5; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 Applicability

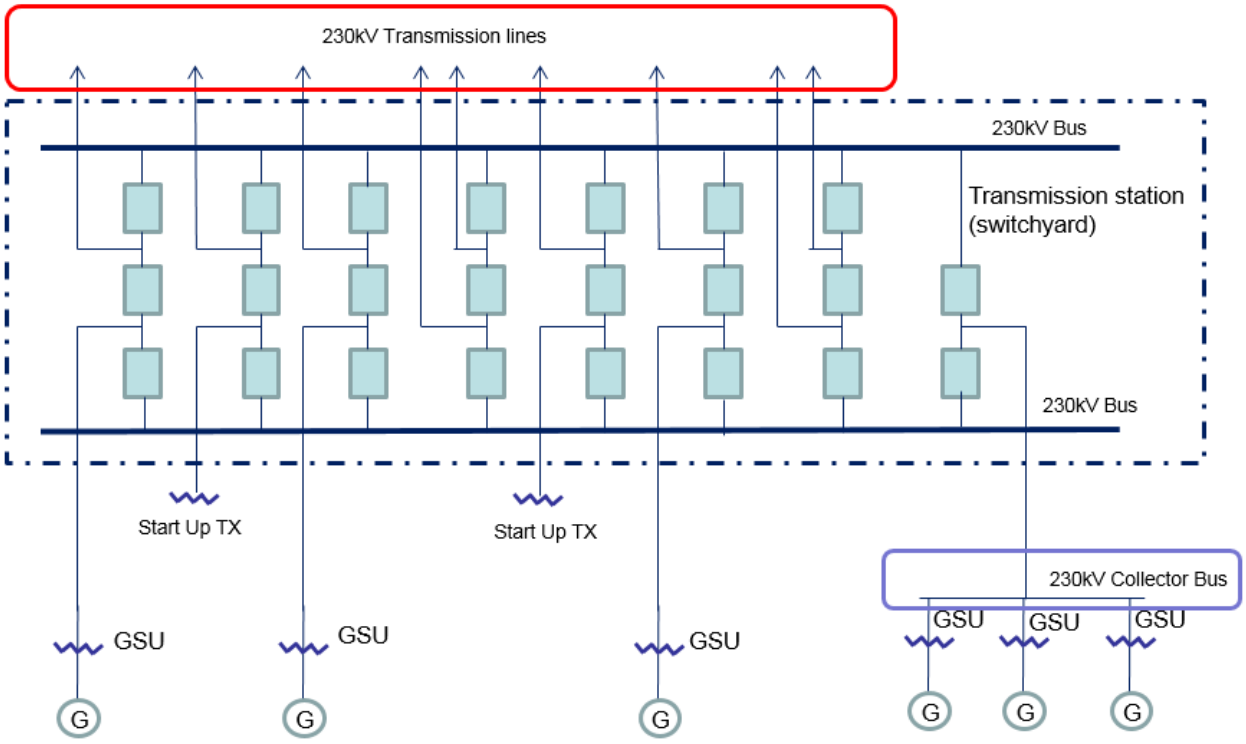
The purpose of Reliability Standard CIP-014-1 is to protect Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014-1 first applies to Transmission Owners that own Transmission Facilities that meet the specific criteria in Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4 mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1. Each Transmission Owner that owns Transmission Facilities that meet the criteria in Section 4.1.1.1 through 4.1.1.4 is required to perform a risk assessment as specified in Requirement R1 to identify its Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Standard Drafting Team (SDT) expects this population will be small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities. Only those Transmission Owners with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6.

This standard also applies to Transmission Operators. A Transmission Operator's obligations under the standard, however, are only triggered if the Transmission Operator is notified by an applicable Transmission Owner under Requirement R3 that the Transmission Operator operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the Requirement R1 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only Transmission Operators who are notified that they have primary control centers under this standard have performance obligations under Requirements R4 through R6. In other words, primary control center for purposes of this Standard is the control center that the Transmission Owner or Transmission Operator, respectively, uses as its primary, permanently-manned site to physically operate a Transmission station or Transmission substation that is identified in Requirement R1 and verified in Requirement R2. Control centers that provide back-up capability are not applicable, as they are a form of resiliency and intentionally redundant.

The SDT considered several options for bright line criteria that could be used to determine applicability and provide an initial threshold that defines the set of Transmission stations and Transmission substations that would meet the directives of the FERC order on physical security (*i.e.*, those that could cause widespread instability, uncontrolled separation, or Cascading within

an Interconnection). The SDT determined that using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. Additionally, the SDT concluded that using the CIP-002-5.1 Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment. As described in CIP-002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). The SDT understands that using this bright line criteria to determine applicability may require some Transmission Owners to perform risk assessments under Requirement R1 that will result in a finding that none of their Transmission stations or Transmission substations would pose a risk of widespread instability, uncontrolled separation, or Cascading within an Interconnection. However, the SDT determined that higher bright lines could not be technically justified to ensure inclusion of all Transmission stations and Transmission substations, and their associated primary control centers that, if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Further guidance and technical basis for the bright line criteria for Medium Impact Facilities can be found in the Guidelines and Technical Basis section of CIP-002-5.1.

Additionally, the SDT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. First, Transmission stations or Transmission substations interconnecting generation facilities are considered when determining applicability. Transmission Owners will consider those Transmission stations and Transmission substations that include a Transmission station on the high side of the Generator Step-up transformer (GSU) using Applicability Section 4.1.1.1 and 4.1.1.2. As an example, a Transmission station or Transmission substation identified as a Transmission Owner facility that interconnects generation will be subject to the Requirement R1 risk assessment if it operates at 500kV or greater or if it is connected at 200 kV – 499kV to three or more other Transmission stations or Transmission substations and has an "aggregate weighted value" exceeding 3000 according to the table in Applicability Section 4.1.1.2. Second, the Transmission analysis or analyses conducted under Requirement R1 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities. The diagram below shows an example of a station.



Also, the SDT uses the phrase "Transmission stations or Transmission substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (switching stations or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

On the issue of joint ownership, the SDT recognizes that this issue is not unique to CIP-014-1, and expects that the applicable Transmission Owners and Transmission Operators will develop memorandums of understanding, agreements, Coordinated Functional Registrations, or procedures, etc., to designate responsibilities under CIP-014-1 when joint ownership is at issue, which is similar to what many entities have completed for other Reliability Standards.

The language contained in the applicability section regarding the collector bus is directly copied from CIP-002-5.1, Attachment 1, and has no additional meaning within the CIP-014-1 standard.

Requirement R1

The initial risk assessment required under Requirement R1 must be completed on or before the effective date of the standard. Subsequent risk assessments are to be performed at least once every 30 or 60 months depending on the results of the previous risk assessment per Requirement R1, Part 1.1. In performing the risk assessment under Requirement R1, the

Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Applicability Section 4.1.1. Requirement R1 then requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The standard does not mandate the specific analytical method for performing the risk assessment. The Transmission Owner has the discretion to choose the specific method that best suites its needs. As an example, an entity may perform a Power Flow analysis and stability analysis at a variety of load levels.

Performing Risk Assessments

The Transmission Owner has the discretion to select a transmission analysis method that fits its facts and system circumstances. To mandate a specific approach is not technically desirable and may lead to results that fail to adequately consider regional, topological, and system circumstances. The following guidance is only an example on how a Transmission Owner may perform a power flow and/or stability analysis to identify those Transmission stations and Transmission substations that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. An entity could remove all lines, without regard to the voltage level, to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a significant area of the Interconnection. Using engineering judgment, the Transmission Owner (possibly in consultation with regional planning or operation committees and/or ISO/RTO committee input) should develop criteria (e.g. imposing a fault near the removed Transmission station or Transmission substation) to identify a contingency or parameters that result in potential widespread instability, uncontrolled separation, or Cascading within an Interconnection. Regional consultation on these matters is likely to be helpful and informative, given that the inputs for the risk assessment and the attributes of what constitutes widespread instability, uncontrolled separation, or Cascading within an Interconnection will likely vary from region-to-region or from ISO-to-ISO based on topology, system characteristics, and system configurations. Criteria could also include post-contingency facilities loadings above a certain emergency rating or failure of a power flow case to converge. Available special protection systems (SPS), if any, could be applied to determine if the system experiences any additional instability which may result in uncontrolled separation. Example criteria may include:

(a) Thermal overloads beyond facility emergency ratings;

(b) Voltage deviation exceeding ± 10%; or

(c) Cascading outage/voltage collapse; or

(d) Frequency below under-frequency load shed points

Periodicity

A Transmission Owner who identifies one or more Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection is required to conduct a risk assessment at least once every 30 months. This period ensures that the risk assessment remains current with projected conditions and configurations in the planned system. This risk assessment, as the initial assessment, must consider applicable planned Transmission stations and Transmission substations to be in service within 24 months. The 30 month timeframe aligns with the 24 month planned to be in service date because the Transmission Owner is provided the flexibility, depending on its planning cycle and the frequency in which it may plan to construct a new Transmission station or Transmission substation to more closely align these dates. The requirement is to conduct the risk assessment at least once every 30 months, so for a Transmission Owner that believes it is better to conduct a risk assessment once every 24 months, because of its planning cycle, it has the flexibility to do so.

Transmission Owners that have not identified any Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection are unlikely to see changes to their risk assessment in the Near-Term Planning Horizon. Consequently, a 60 month periodicity for completing a subsequent risk assessment is specified.

Identification of Primary Control Centers

After completing the risk assessment specified in Requirement R1, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center "operationally controls" a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

Requirement R2

This requirement specifies verification of the risk assessment performed under Requirement R1 by an entity other than the owner or operator of the Requirement R1 risk assessment.

A verification of the risk assessment by an unaffiliated third party, as specified in Requirement R2, could consist of:

1. Certifying that the Requirement R1 risk assessment considers the Transmission stations and Transmission substations identified in Applicability Section 4.1.1.

2. Review of the model used to conduct the risk assessment to ensure it contains sufficient system topology to identify Transmission stations and Transmission substations that if rendered inoperable or damaged could cause widespread instability, uncontrolled separation, or Cascading within an Interconnection.
3. Review of the Requirement R1 risk assessment methodology.

This requirement provides the flexibility for a Transmission Owner to select from unaffiliated registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term unaffiliated means that the selected verifying entity cannot be a corporate affiliate (*i.e.,* the verifying or third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

The prohibition on registered entities using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. For instance, a U.S. federal power marketing agency may select as its verifier another U.S. federal agency to conduct its verification so long as the selected entity has transmission planning or analysis experience. Similarly, a Transmission Owner owned by a Canadian province can use a separate agency of that province to perform the verification. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

Requirement R2 also provides that the "verification may occur concurrent with or after the risk assessment performed under Requirement R1." This provision is designed to provide the Transmission Owner the flexibility to work with the verifying entity throughout (*i.e.,* concurrent with) the risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could collaborate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently. The intent of Requirement R2 is to have an entity other than the owner or operator of the facility to be involved in the risk assessment process and have an opportunity to provide input. Accordingly, Requirement R2 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the risk assessment and subsequently has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the risk assessment.

Characteristics to consider in selecting a third party reviewer could include:

- Registered Entity with applicable planning and reliability functions.
- Experience in power system studies and planning.
- The entity's understanding of the MOD standards, TPL standards, and facility ratings as they pertain to planning studies.

- The entity's familiarity with the Interconnection within which the Transmission Owner is located.

With respect to the requirement that Transmission owners develop and implement procedures for protecting confidential and sensitive information, the Transmission Owner could have a method for identifying documents that require confidential treatment. One mechanism for protecting confidential or sensitive information is to prohibit removal of sensitive or confidential information from the Transmission Owner's site. Transmission Owners could include such a prohibition in a non-disclosure agreement with the verifying entity.

A Technical feasibility study is not required in the Requirement R2 documentation of the technical basis for not modifying the identification in accordance with the recommendation.

On the issue of the difference between a verifier in Requirement R2 and a reviewer in Requirement R6, the SDT indicates that the verifier will confirm that the risk assessment was completed in accordance with Requirement R1, including the number of Transmission stations and substations identified, while the reviewer in Requirement R6 is providing expertise on the manner in which the evaluation of threats was conducted in accordance with Requirement R4, and the physical security plan in accordance with Requirement R5. In the latter situation there is no verification of a technical analysis, rather an application of experience and expertise to provide guidance or recommendations, if needed.

Parts 2.4 and 6.4 require the entities to have procedures to protect the confidentiality of sensitive or confidential information. Those procedures may include the following elements:

1. Control and retention of information on site for third party verifiers/reviewers.
2. Only "need to know" employees, etc., get the information.
3. Marking documents as confidential
4. Securely storing and destroying information when no longer needed.
5. Not releasing information outside the entity without, for example, General Counsel sign-off.

Requirement R3

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first completing the risk assessment specified by Requirement R1 and the verification specified by Requirement R2. Requirement R3 is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 receive notice so that the Transmission Operator may fulfill the rest of the obligations required in Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include within the notice the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk

assessment under Requirement R1 or as a result of the verification process under Requirement R2.

Requirement R4

This requirement requires owners and operators of facilities identified by the Requirement R1 risk assessment and that are verified under Requirement R2 to conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process. Threats and vulnerabilities may vary from facility to facility based on any number of factors that include, but are not limited to, location, size, function, existing physical security protections, and attractiveness as a target.

In order to effectively conduct a threat and vulnerability assessment, the asset owner may be the best source to determine specific site vulnerabilities, but current and evolving threats may best be determined by others in the intelligence or law enforcement communities. A number of resources have been identified in the standard, but many others exist and asset owners are not limited to where they may turn for assistance. Additional resources may include state or local fusion centers, U.S. Department of Homeland Security, Federal Bureau of Investigations (FBI), Public Safety Canada, Royal Canadian Mounted Police, and InfraGard chapters coordinated by the FBI.

The Responsible Entity is required to take a number of factors into account in Parts 4.1 to 4.3 in order to make a risk-based evaluation under Requirement R4.

To assist in determining the current threat for a facility, the prior history of attacks on similarly protected facilities should be considered when assessing probability and likelihood of occurrence at the facility in question.

Resources that may be useful in conducting threat and vulnerability assessments include:

- NERC Security Guideline for the Electricity Sector: Physical Security.
- NERC Security Guideline: Physical Security Response.
- ASIS International General Risk Assessment Guidelines.
- ASIS International Facilities Physical Security Measure Guideline.
- ASIS International Security Management Standard: Physical Asset Protection.
- Whole Building Design Guide - Threat/Vulnerability Assessments.

Requirement R5

This requirement specifies development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Requirement R5 specifies the following attributes for the physical security plan:

- *Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.*

  Resiliency may include, among other things:

  a. System topology changes,

  b. Spare equipment,

  c. Construction of a new Transmission station or Transmission substation.

  While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site.

- *Law enforcement contact and coordination information.*

  Examples of such information may be posting 9-1-1 for emergency calls and providing substation safety and familiarization training for local and federal law enforcement, fire department, and Emergency Medical Services.

- *A timeline for executing the physical security enhancements and modifications specified in the physical security plan.*

  Entities have the flexibility to prioritize the implementation of the various resiliency or security enhancements and modifications in their security plan according to risk, resources, or other factors. The requirement to include a timeline in the physical security plan for executing the actual physical security enhancements and modifications does not also require that the enhancements and modifications be completed within 120 days. The actual timeline may extend beyond the 120 days, depending on the amount of work to be completed.

- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

  A registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various sources. Some of these sources could include the ERO, ES-ISAC, and US and/or Canadian federal agencies. This information should be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in R5.

  Incremental changes made to the physical security plan prior to the next required third party review do not require additional third party reviews.

Requirement R6

This requirement specifies review by an entity other than the Transmission Owner or Transmission Operator with appropriate expertise for the evaluation performed according to

Requirement R4 and the security plan(s) developed according to Requirement R5. As with Requirement R2, the term unaffiliated means that the selected third party reviewer cannot be a corporate affiliate (*i.e.,* the third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Operator). A third party reviewer also cannot be a division of the Transmission Operator that operates as a functional unit.

As noted in the guidance for Requirement R2, the prohibition on registered entities using a corporate affiliate to conduct the review, however, does not prohibit a governmental entity from selecting as the third party reviewer another governmental entity within the same political subdivision. For instance, a city or municipality may use its local enforcement agency, so long as the local law enforcement agency satisfies the criteria in Requirement R6. The third party reviewer, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

The Responsible Entity can select from several possible entities to perform the review:

- *An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.*

  In selecting CPP and PSP for use in this standard, the SDT believed it was important that if a private entity such as a consulting or security firm was engaged to conduct the third party review, they must tangibly demonstrate competence to conduct the review. This includes electric industry physical security experience and either of the premier security industry certifications sponsored by ASIS International. The ASIS certification program was initiated in 1977, and those that hold the CPP certification are board certified in security management. Those that hold the PSP certification are board certified in physical security.

- *An entity or organization approved by the ERO.*

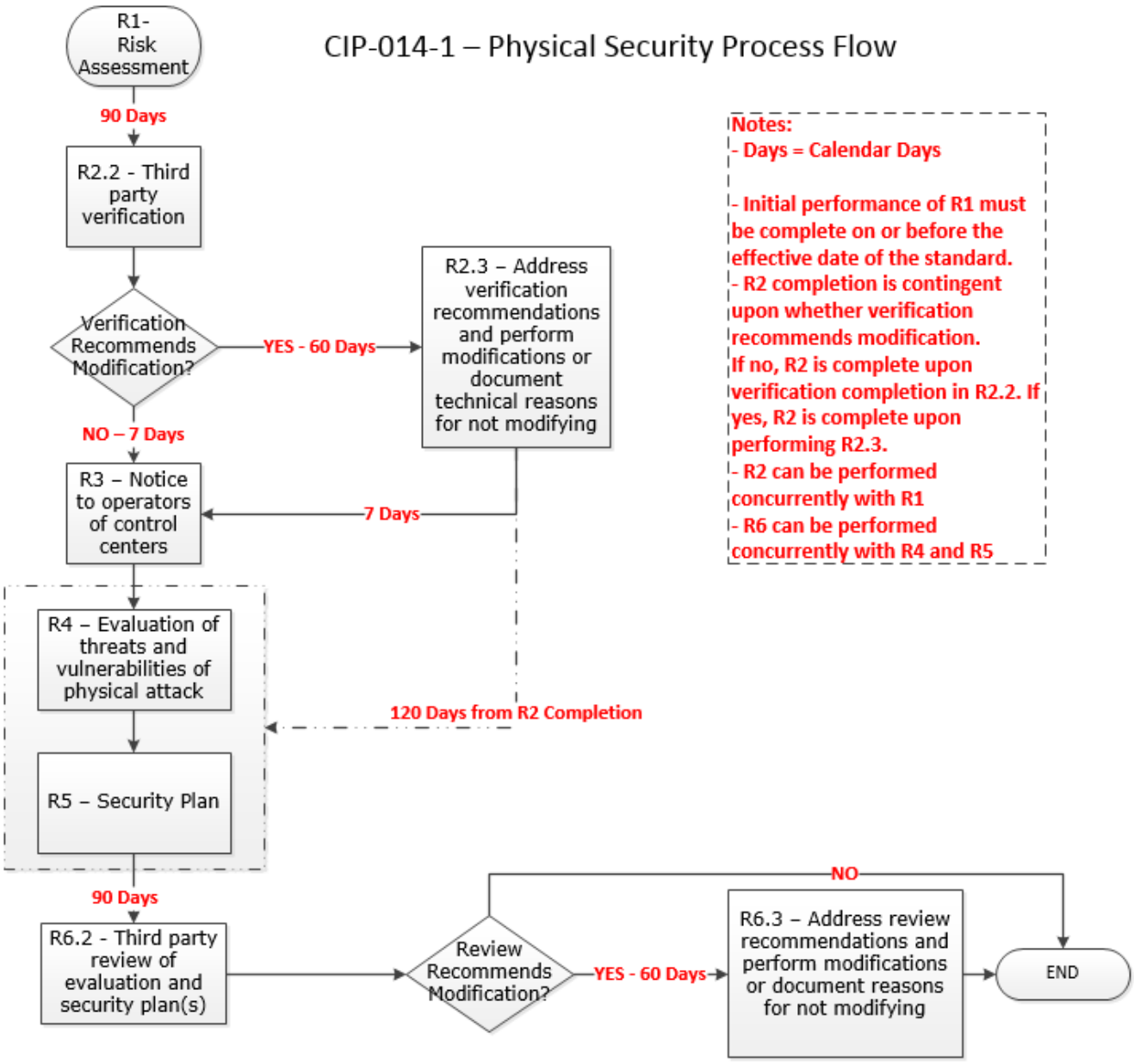
- *A governmental agency with physical security expertise.*

- *An entity or organization with demonstrated law enforcement, government, or military physical security expertise.*

As with the verification under Requirement R2, Requirement R6 provides that the "review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5." This provision is designed to provide applicable Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout (*i.e.,* concurrent with) the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5, which for some Responsible Entities may be more efficient and effective. In other words, a Transmission Owner or Transmission Operator could collaborate with their unaffiliated third party reviewer to perform an evaluation of potential threats and vulnerabilities (Requirement R4) and develop a security plan (Requirement R5) to satisfy Requirements R4 through R6 simultaneously. The

intent of Requirement R6 is to have an entity other than the owner or operator of the facility to be involved in the Requirement R4 evaluation and the development of the Requirement R5 security plans and have an opportunity to provide input on the evaluation and the security plan. Accordingly, Requirement R6 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the evaluation and develops the security plan itself and then has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the evaluation and develop the security plan.

Timeline


CIP-014-1 – Physical Security Process Flow
R1- Risk Assessment
90 Days
R2.2 - Third party verification
Verification Recommends Modification?
YES - 60 Days
R2.3 – Address verification recommendations and perform modifications or document technical reasons for not modifying
NO – 7 Days
R3 – Notice to operators of control centers
7 Days
R4 – Evaluation of threats and vulnerabilities of physical attack
120 Days from R2 Completion
R5 – Security Plan
90 Days
R6.2 - Third party review of evaluation and security plan(s)
Review Recommends Modification?
YES - 60 Days
NO
R6.3 – Address review recommendations and perform modifications or document reasons for not modifying
END
Notes:
- Days = Calendar Days
- Initial performance of R1 must be complete on or before the effective date of the standard.
- R2 completion is contingent upon whether verification recommends modification. If no, R2 is complete upon verification completion in R2.2. If yes, R2 is complete upon performing R2.3.
- R2 can be performed concurrently with R1
- R6 can be performed concurrently with R4 and R5

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. Nominations for the Standard Drafting Team (SDT) for Project 2014-04 Physical Security were solicited March 13-18, 2014, and the SDT was appointed by the Standards Committee on March 21, 2014.
2. Technical Conference was held April 1, 2014.
3. The draft standard was posted, pursuant to a Standards Committee authorized waiver, for a 15-day Formal Comment Period with a 5-day Initial Ballot April 10-24, 2014.

Description of Current Draft

This is the ~~first~~second draft of the proposed Reliability Standard, and it is being posted for ~~stakeholder comment and initial~~final ballot. This draft includes proposed requirements to meet the directives issued in the FERC order issued March 7, 2014, in Docket No. RD14-6-000, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

Anticipated Actions	Anticipated Date
~~15-day Formal Comment Period with a 5-day Initial Ballot, pursuant to a Standards Committee authorized waiver.~~	~~April 10, 2014~~
~~10-day Formal Comment Period with a~~ 5-day ~~Additional~~Final Ballot ~~(if necessary),~~ pursuant to a Standards Committee authorized waiver.	May 1, 2014
~~5-day Final Ballot, pursuant to a Standards Committee authorized waiver.~~	~~May 2014~~
BOT Adoption.	May 2014
File with applicable Regulatory Authorities.	No later than June 5, 2014

Version History

Version	Date	Action	Change Tracking
1.0	TBD	Effective Date	New

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the NERC Glossary of Terms used in Reliability Standards (Glossary) are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

A. Introduction

1. **Title:** Physical Security

2. **Number:** CIP-014-1

3. **Purpose:** To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

4. **Applicability:**

4.1. Functional Entities:

4.1.1 Transmission Owner that owns a Transmission station or Transmission substation that meets any of the following criteria:

4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

4.1.1.3 Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or

Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission ~~or~~are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

5. Effective Dates:

CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

This Reliability Standard addresses the directives from the FERC order issued March 7, 2014, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014), which required NERC to develop a physical security reliability standard(s) to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

B. Requirements and Measures

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify ~~any~~the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or

- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

Rationale for Requirement R1:

This requirement meets the FERC directive from paragraph 6 in the order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through widespread

instability, uncontrolled separation, or cascading failures. It also meets the portion of the directive from paragraph 11 for periodic reevaluation by requiring the risk assessment to be performed every 30 months (or 60 months for an entity that has not identified in a previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection).

After identifying each Transmission station and Transmission substation that meets the criteria in Requirement R1, it is important to additionally identify the primary control center that operationally controls that Transmission station or Transmission substation (*i.e.,* the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated ~~verifying entity~~third party verification shall ~~either~~ verify the Transmission Owner's risk assessment performed under Requirement R1 ~~or recommend~~, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or

- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged with~~made available to the unaffiliated third party ~~verif~~verifier ~~ying entity~~ and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

Rationale for Requirement R2:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring verification by an entity other than the owner or operator of the risk assessment performed under Requirement R1.

This requirement provides the flexibility for a Transmission Owner to select registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term "unaffiliated" means that the selected verifying entity cannot be a corporate affiliate (*i.e.*, the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit. The term "unaffiliated" is not intended to prohibit a governmental entity from using another government entity to be a verifier under Requirement R2.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout the Requirement R1 risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform a Requirement R1 risk assessment to satisfy both Requirement R1 and Requirement R2 concurrently.

Planning Coordinator is functional entity listed in Part 2.1. The Planning Coordinator and Planning Authority are the same entity as shown in the NERC Glossary of Terms Used in NERC Reliability Standards.

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1 ~~and~~ , Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2 ~~that~~ , and b) is not under the operational control of the Transmission Owner~~,~~ : the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Rationale for Requirement R3:

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first identifying which Transmission stations and Transmission substations meet the criteria specified by Requirement R1, as verified according to Requirement R2. This requirement is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 ~~and~~ , Part 1.2 of a Transmission station or Transmission substation verified according to Requirement R2 receives notice of such identification so that the Transmission Operator may timely fulfill its resulting obligations under Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include notice of the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or the verification process under Requirement R2.

R4. Each Transmission Owner that ~~owns or operates~~ identified a Transmission station, Transmission substation, or a primary control center ~~identified~~ in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall conduct an evaluation of the potential threats and

vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history ~~or~~of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Rationale for Requirement R4:

This requirement meets the FERC directive from paragraph 8 in the order on physical security that the reliability standard must require tailored evaluation of potential threats and vulnerabilities to facilities identified in Requirement R1 and verified according to Requirement R2. Threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections, and attractiveness of the target. As such, the requirement does not mandate a one-size-fits-all approach but requires entities to account for the unique characteristics of their facilities.

Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur or be completed. However, Requirement R5 requires that the entity's security plan(s), which is dependent on the Requirement R4 evaluation, must be completed within 120 calendar days following completion of Requirement R2. Thus, an entity has the flexibility when to complete the Requirement R4 evaluation, provided that it is completed in time to comply with the requirement in Requirement R5 to develop a physical security plan 120 calendar days following completion of Requirement R2.

R5. Each Transmission Owner that ~~owns or has operational control of~~ identified a Transmission station, Transmission substation, or primary control center ~~identified~~ in

Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s~~)~~). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2~~.~~ and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on the results of~~identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for ~~implementing~~executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating ~~implementation~~ execution of the physical security plan according to the timeline specified in the physical security plan.

Rationale for Requirement R5:

This requirement meets the FERC directive from paragraph 9 in the order on physical security requiring the development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

R6. Each Transmission Owner that ~~owns or operates~~ identified a Transmission station, Transmission substation, or primary control center ~~identified~~ in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or~~

~~Transmission substation~~, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

~~**6.1.1.**~~ An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.

~~**6.1.2.**~~ An entity or organization approved by the ERO.

~~**6.1.3.**~~ A governmental agency with physical security expertise.

~~**6.1.4.**~~ An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated ~~reviewing entity~~third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or
- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged with~~made available to the unaffiliated third party reviewer~~ing entity and from any other form of public disclosure~~ and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

Rationale for Requirement R6:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring review by an entity other than the owner or operator with appropriate expertise of the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5.

As with the verification required by Requirement R2, Requirement R6 provides Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer~~ing entity~~ throughout the Requirement R4 evaluation and the development of the Requirement R5 security plan(s). This would allow entities to satisfy their obligations under Requirement R6 concurrent with the satisfaction of their obligations under Requirements R4 and R5.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

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

The Transmission Owner and Transmission Operator shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation.

The responsible entities shall retain documentation as evidence for three years.

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

The CEA shall keep the last audit records and all requested and submitted subsequent audit records, subject to the confidentiality provisions of Section 1500 of the Rules of Procedure and the provisions of Section 1.4 below.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information

Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**High**	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection	Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.	Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.	performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.	uncontrolled separation, or Cascading within an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
R2	**Long-term Planning**	**Medium**	The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but	The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but	The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to	The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than or equal to 100 calendar days following completion of Requirement R1; OR The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by ~~part~~Part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.	less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by ~~part~~Part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.	120 calendar days following completion of Requirement R1; OR The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by ~~part~~Part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed	following completion of Requirement R1; OR The Transmission Owner failed to have ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1; OR The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by ~~part~~Part 2.3.	
R3	**Long-term Planning**	**Lower**	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.	operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.	of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.	center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						identification in Requirement R1.
R4	**Operations Planning, Long-term Planning**	**Medium**	N/A	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
R5	**Long-term Planning**	**High**	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.	The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						center(s) identified in Requirement R1 and verified according to Requirement 2 but failed to include Parts 5.1 through 5.4 in the plan.
R6	**Long-term Planning**	**Medium**	The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days; OR The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement	The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed	The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed	The Responsible Entity failed to have ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.	under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.	under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not ~~and modify or~~ document the reason for not modifying the security plan(s) as specified in Part 6.3.	the security plan(s) developed under Requirement R5; OR The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 Applicability

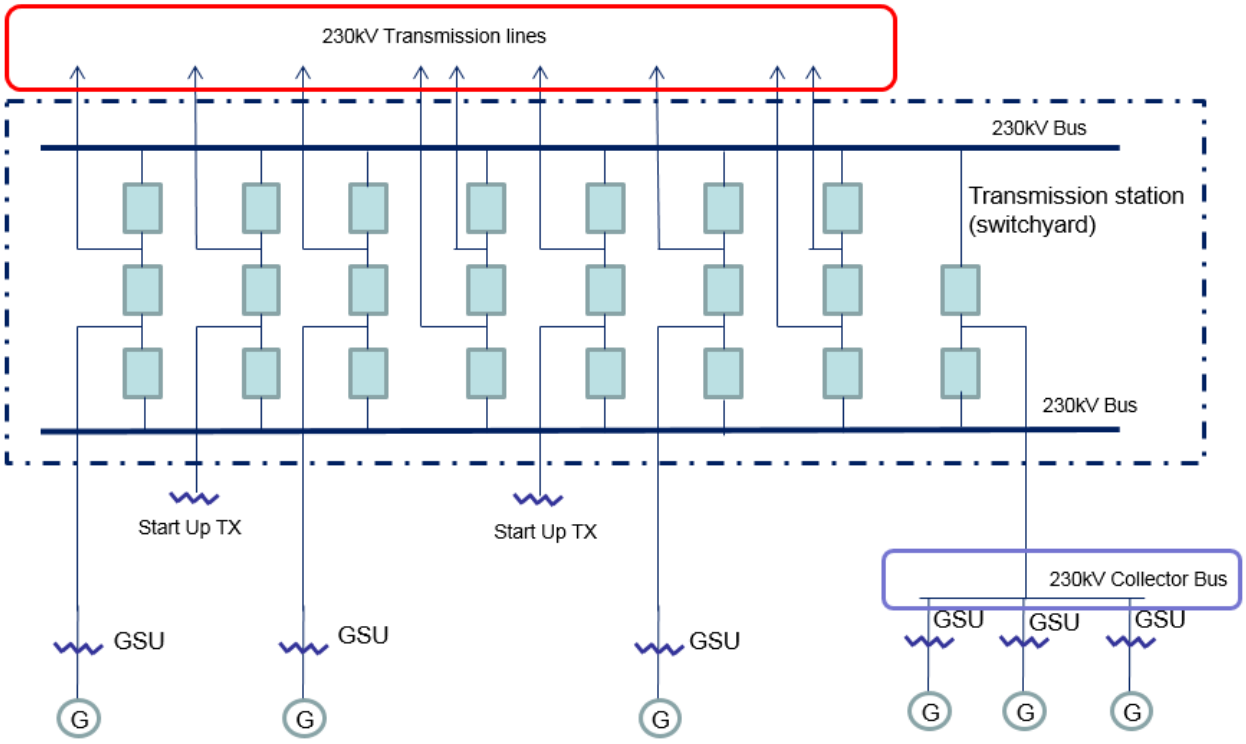
The purpose of Reliability Standard CIP-014-1 is to protect Transmission stations and Transmission substations, and their associated primary control centers~~,~~ that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014-1 first applies to Transmission Owners ~~(TO)~~ that own Transmission Facilities that meet the specific criteria in Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4 mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1. Each ~~TO~~Transmission Owner that owns Transmission Facilities that meet the criteria in Section 4.1.1.1 through 4.1.1.4 is required to perform a risk assessment as specified in Requirement R1 to identify its Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Standard Drafting Team (SDT) expects this population will be small and that many ~~TOs~~Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities. Only those ~~TOs~~Transmission Owners with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6.

This standard also applies to Transmission Operators ~~(TOP).~~ A ~~TOP's~~Transmission Operator's obligations under the standard, however, are only triggered if the ~~TOP~~Transmission Operator is notified by an applicable ~~TO~~Transmission Owner under Requirement R3 that the ~~TOP~~Transmission Operator operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the Requirement R1 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only ~~TOPs~~Transmission Operators who are notified that they have primary control centers under this standard have performance obligations under Requirements R4 through R6. In other words, primary control center for purposes of this Standard is the control center that the Transmission Owner or Transmission Operator, respectively, uses as its primary, permanently-manned site to physically operate a Transmission station or Transmission substation that is identified in Requirement R1 and verified in Requirement R2. Control centers that provide back-up capability are not applicable, as they are a form of resiliency and intentionally redundant.

The ~~drafting team~~SDT considered several options for bright line criteria that could be used to determine applicability and provide an initial threshold that defines the set of Transmission stations and Transmission substations that would meet the directives of the FERC order on

physical security (*i.e.*, those that could cause widespread instability, uncontrolled separation, or Cascading within an Interconnection). The SDT determined that using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. Additionally, the SDT concluded that using the CIP-002-5.1 Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment. As described in CIP-~~005-2~~002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). The SDT understands that using this bright line criteria to determine applicability may require some Transmission Owners to perform risk assessments under Requirement R1 that will result in a finding that none of their Transmission stations or Transmission substations would pose a risk of widespread instability, uncontrolled separation, or Cascading within an Interconnection. However, the SDT determined that higher bright lines could not be technically justified to ensure inclusion of all Transmission stations and Transmission substations, and their associated primary control centers~~,~~ that, if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Further guidance and technical basis for the bright line criteria for Medium Impact Facilities can be found in the Guidelines and Technical Basis section of CIP-002-5.1.

Additionally, the SDT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. ~~First, the transmission analysis or analyses conducted under Requirement R1 will~~First, Transmission stations or Transmission substations interconnecting generation facilities are considered when determining applicability. Transmission Owners will consider those Transmission stations and Transmission substations that include a Transmission station on the high side of the Generator Step-up transformer (GSU) using Applicability Section Parts 4.1.1.1 and 4.1.1.2. As an example, a Transmission station or Transmission substation identified as a Transmission Owner facility that interconnects generation will be subject to the Requirement R1 risk assessment if it operates at 500kV or greater or if it is connected at 200 kV – 499kV to three or more other Transmission stations or Transmission substations and has an "aggregate weighted value" exceeding 3000 according to the table in Applicability Section Part 4.1.1.2. Second, the Transmission analysis or analyses conducted under Requirement R1 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations~~..~~. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities. The diagram below shows an example of a station.



Also, the SDT uses the phrase "Transmission stations or Transmission substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (switching stations or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

On the issue of joint ownership, the SDT recognizes that this issue is not unique to CIP-014-1, and expects that the applicable Transmission Owners and Transmission Operators will develop memorandums of understanding, agreements, Coordinated Functional Registrations, or procedures, etc., to designate responsibilities under CIP-014-1 when joint ownership is at issue, which is similar to what many entities have completed for other Reliability Standards.

The language contained in the applicability section regarding the collector bus is directly copied from CIP-002-5.1, Attachment 1, and has no additional meaning within the CIP-014-1 standard.

Requirement R1

The initial risk assessment required under Requirement R1 must be completed on or before the effective date of the standard. Subsequent risk assessments are to be performed at least once

every 30 or 60 months depending on the results of the previous risk assessment per Requirement R1, Part 1.1. In performing the risk assessment under Requirement R1, the Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Applicability Section 4.1.1. Requirement R1 then requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The standard does not mandate the specific analytical method for performing the risk assessment. The Transmission Owner has the discretion to choose the specific method that best suites its needs. As an example, an entity may perform a Power Flow analysis and stability analysis at a variety of load levels.

Performing Risk Assessments

The Transmission Owner has the discretion to select a transmission analysis method that fits its facts and system circumstances. To mandate a specific approach is not technically desirable and may lead to results that fail to adequately consider regional, topological, and system circumstances. The following ~~is~~ guidance is only an example on how a Transmission Owner may perform a ~~traditional~~ power flow and/or stability analysis to identify those Transmission stations and Transmission substations that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. An entity could remove all lines, without regard to the voltage level, to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a ~~wide~~significant area~~.~~ of the Interconnection. Using engineering judgment, the Transmission Owner (possibly in consultation with regional planning or operation committees and/or ISO/RTO committee input) should develop criteria (e.g. imposing a fault near the removed Transmission station or Transmission substation) to identify a contingency or parameters that result~~ing~~ in potential widespread instability, uncontrolled separation, or Cascading within an Interconnection. ~~For example, the criteria~~Regional consultation on these matters is likely to be helpful and informative, given that the inputs for the risk assessment and the attributes of what constitutes widespread instability, uncontrolled separation, or Cascading within an Interconnection will likely vary from region-to-region or from ISO-to-ISO based on topology, system characteristics, and system configurations. Criteria could also include post-contingency facilities loadings above a certain emergency rating or failure of a power flow case to converge. Available ~~remedial action schemes (RAS) or~~ special protection systems (SPS), if any, could be applied to determine if the system experiences any additional instability which may result in uncontrolled separation. Example criteria may include:

(a) Thermal overloads beyond facility emergency ratings;

(b) Voltage deviation exceeding ± 10%; or

(c) Cascading outage/voltage collapse; or

(d) Frequency below under-frequency load shed points

Periodicity

~~A TO~~A Transmission Owner who identifies one or more Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection is required to conduct a risk assessment at least once every 30 months. This period ensures that the risk assessment remains current with projected conditions and configurations in the planned system. This risk assessment, as the initial assessment, must consider applicable planned Transmission stations and Transmission substations to be in service within 24 months. The 30 month timeframe aligns with the 24 month planned to be in service date because the Transmission Owner is provided the flexibility, depending on its planning cycle and the frequency in which it may plan to construct a new Transmission station or Transmission substation to more closely align these dates. The requirement is to conduct the risk assessment at least once every 30 months, so for a Transmission Owner that believes it is better to conduct a risk assessment once every 24 months, because of its planning cycle, it has the flexibility to do so.

~~TOs who~~Transmission Owners that have not identified any Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection are unlikely to see changes to their risk assessment in the Near-Term Planning Horizon. Consequently, a 60 month periodicity for completing a subsequent risk assessment is specified.

Identification of Primary Control Centers

After completing the risk assessment specified in Requirement R1, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center "operationally controls" a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

Requirement R2

This requirement specifies verification of the risk assessment performed under Requirement R1 by an entity other than the owner or operator of the Requirement R1 risk assessment.

A verification of the risk assessment by an unaffiliated third party, as specified in Requirement R2, could consist of:

1. Certifying that the Requirement R1 risk assessment considers the Transmission stations and Transmission substations identified in Applicability Section 4.1.1.
2. Review of the model used to conduct the risk assessment to ensure it contains sufficient system topology to identify Transmission stations and Transmission substations that if

rendered inoperable or damaged could cause widespread instability, uncontrolled separation, or Cascading within an Interconnection.

3. Review of the Requirement R1 risk assessment ~~method, which may include, for example, consideration of factors such as the following system performance criteria:~~methodology.

   ~~a. Thermal overloads beyond facility emergency ratings;~~

   ~~b. Voltage deviation exceeding ± 10%,~~

   ~~c. Cascading outage/Voltage collapse,~~

   ~~Frequency below under-frequency load shed points.~~

This requirement provides the flexibility for a Transmission Owner to select from unaffiliated registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term unaffiliated means that the selected verifying entity cannot be a corporate affiliate (*i.e.,* the verifying or ~~reviewing entity~~third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

The prohibition on registered entities using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. For instance, a U.S. federal power marketing agency may select as its verifier another U.S. federal agency to conduct its verification so long as the selected entity has transmission planning or analysis experience. Similarly, a Transmission Owner owned by a Canadian province can use a separate agency of that province to perform the verification. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

Requirement R2 also provides that the "verification may occur concurrent with or after the risk assessment performed under Requirement R1." This provision is designed to provide the Transmission Owner the flexibility to work with the verifying entity throughout (*i.e.,* concurrent with) the risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could ~~coordinate~~collaborate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently. The intent of Requirement R2 is to have an entity other than the owner or operator of the facility to be involved in the risk assessment process and have an opportunity to provide input. Accordingly, Requirement R2 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the risk assessment and subsequently has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the risk assessment.

Characteristics to consider in selecting a ~~reviewing entity~~third party reviewer could include:

- Registered Entity with applicable planning and reliability functions.
- Experience in power system studies and planning.
- The entity's understanding of the MOD standards, TPL standards, and facility ratings as they pertain to planning studies.
- The entity's familiarity with the Interconnection within which the ~~transmission owner~~Transmission Owner is located.

With respect to the requirement that Transmission owners develop and implement procedures for protecting confidential and sensitive information, the Transmission Owner could have a method for identifying documents that require confidential treatment. One mechanism for protecting confidential or sensitive information is to prohibit removal of sensitive or confidential information from the ~~TO's~~Transmission Owner's site. Transmission Owners could include such a prohibition in a non-disclosure agreement with the verifying entity.

A Technical feasibility study is not required in the Requirement R2 documentation of the technical basis for not modifying the identification in accordance with the recommendation.

On the issue of the difference between a verifier in Requirement R2 and a reviewer in Requirement R6, the SDT indicates that the verifier will confirm that the risk assessment was completed in accordance with Requirement R1, including the number of Transmission stations and substations identified, while the reviewer in Requirement R6 is providing expertise on the manner in which the evaluation of threats was conducted in accordance with Requirement R4, and the physical security plan in accordance with Requirement R5. In the latter situation there is no verification of a technical analysis, rather an application of experience and expertise to provide guidance or recommendations, if needed.

Parts 2.4 and 6.4 require the entities to have procedures to protect the confidentiality of sensitive or confidential information. Those procedures may include the following elements:

1. Control and retention of information on site for third party verifiers/reviewers.
2. Only "need to know" employees, etc., get the information.
3. Marking documents as confidential
4. Securely storing and destroying information when no longer needed.
5. Not releasing information outside the entity without, for example, General Counsel sign-off.

Requirement R3

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first completing the risk assessment specified by Requirement R1 and the verification specified by Requirement R2. Requirement R3 is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 receive notice so that the Transmission Operator may fulfill the rest of the obligations required in Requirements

R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include within the notice the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or as a result of the verification process under Requirement R2.

Requirement R4

This requirement requires owners and operators of facilities identified by the Requirement R1 risk assessment and that are verified under Requirement R2 to conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process. Threats and vulnerabilities may vary from facility to facility based on any number of factors that include, but are not limited to, location, size, function, existing physical security protections, and attractiveness as a target.

In order to effectively conduct a threat and vulnerability assessment, the asset owner may be the best source to determine specific site vulnerabilities, but current and evolving threats may best be determined by others in the intelligence or law enforcement communities. A number of resources have been identified in the standard, but many others exist and asset owners are not limited to where they may turn for assistance. Additional resources may include state or local fusion centers, U.S. Department of Homeland Security, Federal Bureau of Investigations (FBI), Public Safety Canada, Royal Canadian Mounted Police, and InfraGard chapters coordinated by the FBI.

The Responsible Entity is required to take a number of factors into account in Parts 4.1 to 4.3 in order to make a risk-based evaluation under Requirement R4.

To assist in determining the current threat for a facility, the prior history of attacks on similarly protected facilities should be considered when assessing probability and likelihood of occurrence at the facility in question.

Resources that may be useful in conducting threat and vulnerability assessments include:

- NERC Security Guideline for the Electricity Sector: Physical Security.
- NERC Security Guideline: Physical Security Response.
- ASIS International General Risk Assessment Guidelines.
- ASIS International Facilities Physical Security Measure Guideline.
- ASIS International Security Management Standard: Physical Asset Protection.
- Whole Building Design Guide - Threat/Vulnerability Assessments.

Requirement R5

This requirement specifies development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Requirement R5 specifies the following attributes for the physical security plan:

- *Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on~~identified during the ~~results of the assessment~~evaluation conducted in Requirement R4.~~.~~.*

  Resiliency may include, among other things:

  a. System topology changes,

  b. Spare equipment,

  c. Construction of a new Transmission station or Transmission substation.

  While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site.

- *Law enforcement contact and coordination information.*

  Examples of such information may be posting 9-1-1 for emergency calls and providing substation safety and familiarization training for local and federal law enforcement, fire department, and ~~EMS~~Emergency Medical Services.

- *A timeline for ~~implementing~~executing the physical security ~~resiliency or security measures~~enhancements and modifications specified in the physical security plan.*

  Entities have the flexibility to prioritize the implementation of the various resiliency or security ~~measures~~enhancements and modifications in their security plan according to risk, resources, or other factors. The requirement to include a timeline in the physical security plan for executing the actual physical security enhancements and modifications does not also require that the enhancements and modifications be completed within 120 days. The actual timeline may extend beyond the 120 days, depending on the amount of work to be completed.

- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

  A registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various sources. Some of these sources could include the ERO, ES-ISAC, and US and/or Canadian federal agencies. This information should be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in R5.

Incremental changes made to the physical security plan prior to the next required third party review do not require additional third party reviews.

Requirement R6

This requirement specifies review by an entity other than the ~~TO~~Transmission Owner or ~~TOP~~Transmission Operator with appropriate expertise for the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5. As with Requirement R2, the term unaffiliated means that the selected ~~reviewing entity~~third party reviewer cannot be a corporate affiliate (*i.e.,* the ~~reviewing entity~~third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Operator). A ~~reviewing entity~~third party reviewer also cannot be a division of the Transmission Operator that operates as a functional unit.

As noted in the guidance for Requirement R2, the prohibition on registered entities using a corporate affiliate to conduct the review, however, does not prohibit a governmental entity from selecting as the third party reviewer another governmental entity within the same political subdivision. For instance, a city or municipality may use its local enforcement agency, so long as the local law enforcement agency satisfies the criteria in Requirement R6. The third party reviewer, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

The Responsible Entity can select from several possible entities to perform the review:

- *An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.*

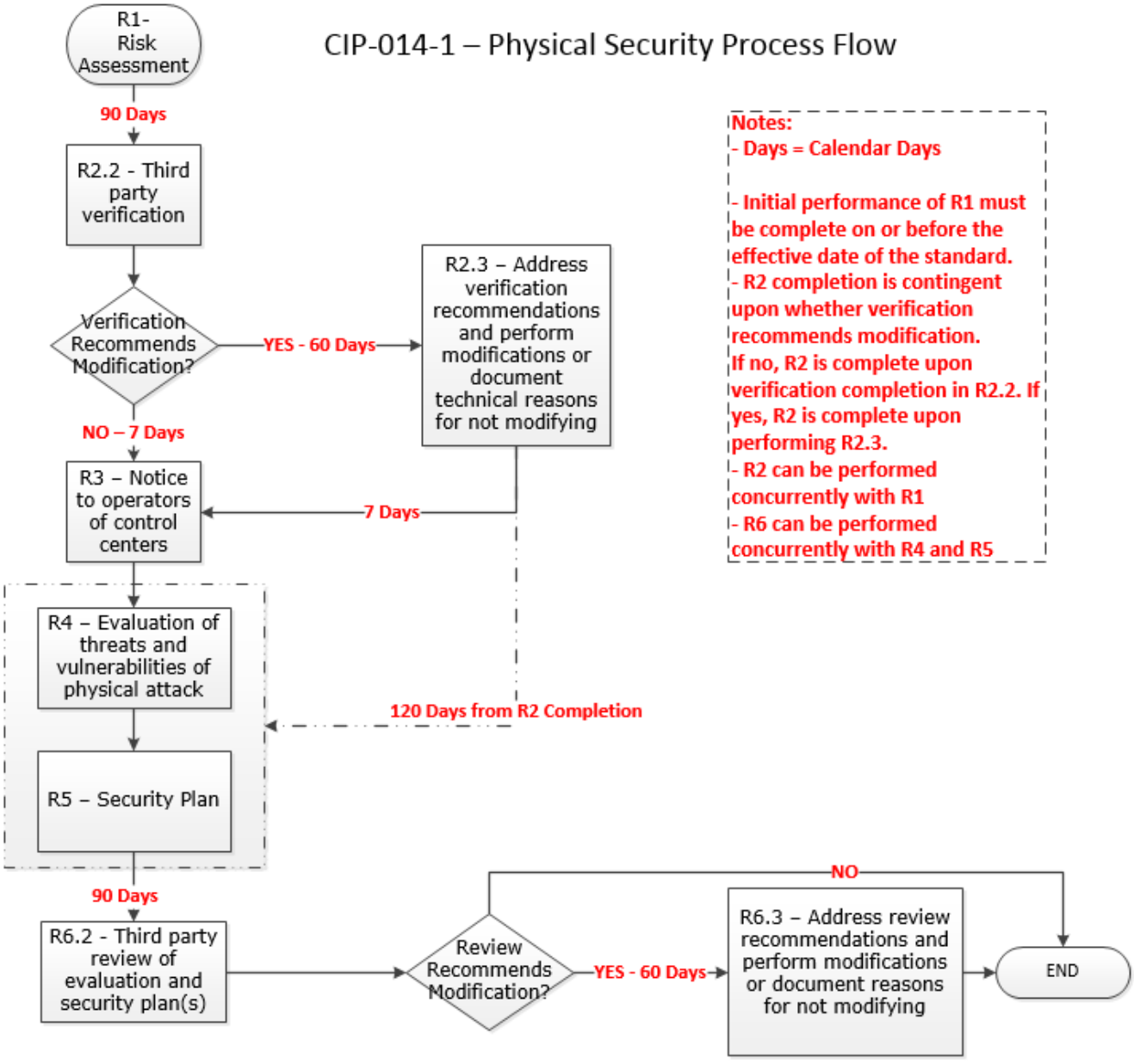
  In selecting CPP and PSP for use in this standard, the ~~drafting team~~SDT believed it was important that if a private entity such as a consulting or security firm was engaged to conduct the third party review, they must tangibly demonstrate competence to conduct the review. This includes electric industry physical security experience and either of the premier security industry certifications sponsored by ASIS International. The ASIS certification program was initiated in 1977, and those that hold the CPP certification are board certified in security management. Those that hold the PSP certification are board certified in physical security.

- *An entity or organization approved by the ERO.*
- *A governmental agency with physical security expertise.*
- *An entity or organization with demonstrated law enforcement, government, or military physical security expertise.*

~~A third party that contributes to the threat assessment and development of the security plan may also serve as the reviewer. As with Requirement R2, the Responsible Entity has~~As with the verification under Requirement R2, Requirement R6 provides that the "review may occur

concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5." This provision is designed to provide applicable Transmission Owners and Transmission Operators the flexibility to work with the ~~reviewing entity~~third party reviewer throughout (*i.e.,* concurrent with) the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5, which for some Responsible Entities may be more efficient and effective. In other words, a ~~TO~~Transmission Owner or ~~TOP~~Transmission Operator could ~~coordinate~~collaborate with their unaffiliated ~~reviewing entity~~third party reviewer to perform an evaluation of potential threats and vulnerabilities (Requirement R4) and develop a security plan (Requirement R5) ~~concurrently with review to satisfy Requirements R4 through R6 simultaneously.~~to satisfy Requirements R4 through R6 simultaneously. The intent of Requirement R6 is to have an entity other than the owner or operator of the facility to be involved in the Requirement R4 evaluation and the development of the Requirement R5 security plans and have an opportunity to provide input on the evaluation and the security plan. Accordingly, Requirement R6 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the evaluation and develops the security plan itself and then has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the evaluation and develop the security plan.

~~Timeline~~


CIP-014-1 – Physical Security Process Flow
R1- Risk Assessment
90 Days
R2.2 - Third party verification
Verification Recommends Modification?
YES - 60 Days
R2.3 – Address verification recommendations and perform modifications or document technical reasons for not modifying
NO – 7 Days
R3 – Notice to operators of control centers
7 Days
R4 – Evaluation of threats and vulnerabilities of physical attack
120 Days from R2 Completion
R5 – Security Plan
90 Days
R6.2 - Third party review of evaluation and security plan(s)
Review Recommends Modification?
YES - 60 Days
NO
R6.3 – Address review recommendations and perform modifications or document reasons for not modifying
END
Notes:
- Days = Calendar Days
- Initial performance of R1 must be complete on or before the effective date of the standard.
- R2 completion is contingent upon whether verification recommends modification. If no, R2 is complete upon verification completion in R2.2. If yes, R2 is complete upon performing R2.3.
- R2 can be performed concurrently with R1
- R6 can be performed concurrently with R4 and R5

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Project 2014-04

May 1, 2014

Approvals Requested
CIP-014-1 Physical Security

Prerequisite Approvals
None

Effective Date

New or Revised Standards
CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Standards for Retirement
None

Initial Performance of Periodic Requirements
The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard. Subsequent risk assessments shall be performed according to the timelines specified in CIP-014-1, Requirement R1.

The initial performance of CIP-014-1, Requirements R2 through R6, must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows:

- Requirement R2 shall be completed as follows:
    - Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard.
    - Part 2.3 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2.

- Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2.
- Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2.
- Requirement R6 shall be completed as follows:
    - Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5.
    - Part 6.3 shall be completed within 60 calendar days of Requirement R6 part 6.2.

Consideration of Issues and Directives

Project 2014-04 - Physical Security

May 1, 2014

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
P.6. The Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the Bulk-Power System. First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities." A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards. Instead, the Commission is directing NERC to develop Reliability	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring Transmission Owners to perform a risk assessment of its Transmission stations and substations that meet the criteria in Attachment 1 of CIP-002-5.1 for a Medium Impact rating to identify which of those Transmission stations and substations, if rendered inoperable or damaged as a result of a physical attack, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Transmission Owner must also identify the primary control centers that operationally controls each identified Transmission station or Transmission substation. The standard drafting team (SDT) determined that the CIP-002-5 bright line would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. If the Transmission Owner does not have any Transmission stations or Transmission substations that meet the Medium

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System and thereby warrant the directive imposed here.		Impact rating, it is not subject to the proposed Reliability Standard and, in turn, would not have to conduct the risk assessment. Consistent with the Commission's directive, Requirement R1 does not require a specific methodology for identifying facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; rather, the requirement mandates that the risk assessment shall consist of a transmission analysis or transmission analyses to ensure that the risk assessment is based on objective analysis, technical expertise, and experienced judgment. Lastly, Requirement R1 identifies the periodicity for conducting the risk assessments.
7. Issuance of this directive will help provide for the resiliency and reliable operation of the Bulk-Power System. To that end, the proposed Reliability Standards should allow owners or operators to consider resilience of the grid in the risk assessment when identifying critical facilities, and the elements that make up those facilities, such as transformers that typically require significant time to repair or replace. As part of this process, owners or operators may consider elements of resiliency such as how the system is designed,	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 provides Transmission Owners the flexibility to consider the resilience of their system when conducting their risk assessments. As noted above, Requirement R1 does not require a specific methodology for identifying their critical facilities and, in turn, allows an entity to use a methodology that considers how their system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
operated, and maintained, and the sophistication of recovery plans and inventory management.		
8. In the second step, the Reliability Standards should require owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities. The threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target. Thus, the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R4 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that the applicable Transmission Owner or Transmission Operator of facilities identified in accordance with Requirement R1 and verified in accordance with Requirement R2 conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive to "tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated," Requirement R4 states that the evaluation must consider: (1) the unique characteristics of the identified facilities; (2) prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and (3) intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U. S. federal and/or Canadian governmental agencies, or their successors.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Consistent with the Commission's statement that NERC should consider requiring owners and operators of identified facilities to consult with entities with appropriate expertise, Requirement R6 requires applicable Transmission Owners and Transmission Operators to select a third party to review their evaluation. This review may occur concurrently with or after the evaluation.
9. Third and finally, the Reliability Standards should require those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Reliability Standards themselves need not dictate specific steps an entity must take to protect against attacks on the identified facilities. However, the Reliability Standards need to require that owners or operators of identified critical facilities have a plan that results in an adequate level of protection against the potential physical threats and vulnerabilities they face at the identified critical facilities.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R5 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring the applicable Transmission Owner or Transmission Operator of facilities identified in accordance with Requirement R1 and verified in accordance with Requirement R2 to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive, Requirement R5 does not dictate specific steps an entity must take to protect against attacks on the identified facilities but requires applicable entities to develop a security plan that includes the following attributes to help ensure an adequate level of protection: (1) resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4; (2) law enforcement

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		contact and coordination information; (3) a timeline for executing the physical security enhancements and modifications specified in the physical security plan; and (4) provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).
10. All three steps of compliance with the Reliability Standard described above could contain sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure. Therefore, NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information that is needed to ensure compliance with the Reliability Standards.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	To protect confidential or sensitive information, the Compliance Monitoring section of the standard provides that evidence demonstrating compliance with the standard must be retained at the applicable entities' facilities. Additionally, Requirements R2 and R6 require applicable entities to implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to third party verifiers and reviewers and to protect or exempt sensitive or confidential information developed pursuant to the standard from public disclosure.
11. In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a	*Reliability Standards for Physical Security*	Requirements R2 and R6 respond to this directive. Under Requirement R3 Transmission Owners must have an unaffiliated third party verify the risk assessment performed under Requirement R1. The third party verifier must be either (1) a

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Reliability Coordinator, or another entity. The Reliability Standards should include a procedure for the verifying entity, as well as the Commission, to add or remove facilities from an owner's or operator's list of critical facilities. Similarly, the determination of threats and vulnerabilities and the security plan should also be reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise. Finally, the Reliability Standards should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. NERC should establish a timeline for when such reevaluations should occur.	*Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or (2) an entity that has transmission planning or analysis experience. The requirement provides that the verification shall either verify the Transmission Owner's risk assessment or include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The verification may occur concurrently with the Requirement R1 risk assessment but must be completed within 90 calendar days of the risk assessment. The Transmission Owner is required to either modify its identification based on the verifier's recommendation or, if it disagrees with the verifier's recommendations, document the technical basis for not modifying its identification. Similarly, under Requirement R6, applicable Transmission Owners and Operators must have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The reviewing entity must be (1) an entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification; (2) an entity or organization approved by the ERO; (3) a governmental agency with physical security expertise; or (4) an entity or organization with demonstrated law

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		enforcement, government, or military physical security expertise. The third party review must be completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The applicable Transmission Owners and Transmission Operators are required to either modify their evaluation or security plan(s) consistent with the reviewer's recommendations or, if they disagree with the recommendations, document the reasons for not modifying. Consistent with the directive to establish a timeline for periodic reevaluation of the identification of facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection, the assessment of the potential risks and vulnerabilities, and the security plans, the standard provides that Requirement R1 risk assessment should be performed at least once every 30 calendar months for those Transmission Owners that identified facilities in their previous risk assessment and once every 60 calendar months for those Transmission Owners that did not identify facilities in their previous risk assessment. Upon completion of each subsequent risk assessment, the applicable entities must satisfy the obligations under the remaining requirements.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
12. Under the Reliability Standards, we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard. We also recognize that the industry has engaged in longstanding efforts to address the physical security of its critical facilities. Thus, NERC should develop an implementation plan that requires owners or operators of the Bulk-Power System to implement the Reliability Standards in a timely fashion, balancing the importance of protecting the Bulk-Power System from harm while giving the owners or operators adequate time to meaningfully implement the requirements. NERC should file the plan with the Reliability Standards for Commission review.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	The proposed Implementation Plan addresses this directive. As provided in the Implementation Plan, the standard becomes effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows: - Requirement R2, Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard. Requirement R2, Part 2.3 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2. - Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		- Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2. - Requirement R6, Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5. Requirement R6, Part 6.3 shall be completed within 60 calendar days of Requirement R6 Part 6.2.

Consideration of Issues and Directives

Project 2014-04 - Physical Security

~~April 9~~May 1, 2014

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
P.6. The Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the Bulk-Power System. First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities." A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards. Instead, the Commission is directing NERC to develop Reliability	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring ~~that each~~ Transmission ~~Owner~~Owners to perform a risk assessment of its Transmission stations and substations that meet the criteria in Attachment 1 of CIP-002-5.1 for a Medium Impact rating to identify which of those Transmission stations and substations, if rendered inoperable or damaged as a result of a physical attack, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Transmission Owner must also identify the primary control centers that operationally controls each identified Transmission station or Transmission substation. The standard drafting team (SDT) determined that the CIP-002-5 bright line ~~was appropriate because it has been vetted with stakeholders, and approved by NERC and FERC. The SDT concluded it was~~would provide a ~~technically sound basis to determine~~conservative threshold for defining which

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System and thereby warrant the directive imposed here.		Transmission ~~Owners should conduct~~stations and Transmission substations must be included in the risk assessment~~.~~ in Requirement R1 of CIP-014-1. If the Transmission Owner does not have any Transmission stations or Transmission substations that meet the Medium Impact rating, it is not subject to the proposed Reliability Standard and, in turn, would not have to conduct the risk assessment. Consistent with the Commission's directive, Requirement R1 does not require a specific methodology for identifying facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; rather, the requirement mandates that the risk assessment shall consist of a transmission analysis or transmission analyses to ensure that the ~~methodology~~risk assessment is based on objective analysis, technical expertise, and experienced judgment. Lastly, Requirement R1 identifies the periodicity for conducting the risk assessments.
7. Issuance of this directive will help provide for the resiliency and reliable operation of the Bulk-Power System. To that end, the proposed Reliability Standards should allow owners or operators to consider resilience of the grid in the risk assessment when identifying critical facilities, and the	*Reliability Standards for Physical Security Measures*, 146	Requirement R1 provides Transmission Owners the flexibility to consider the resilience of their system when conducting their risk assessments. As noted above, Requirement R1 does not require a specific methodology for identifying their critical facilities and, in turn, allows an entity to use a methodology that

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
elements that make up those facilities, such as transformers that typically require significant time to repair or replace. As part of this process, owners or operators may consider elements of resiliency such as how the system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.	FERC ¶ 61,166 (Mar. 7, 2014).	considers how their system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.
8. In the second step, the Reliability Standards should require owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities. The threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target. Thus, the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R4 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that ~~each~~the applicable Transmission Owner ~~and~~or Transmission Operator ~~that owns or operates~~of facilities identified in accordance with Requirement R1 ~~(~~and verified ~~under~~in accordance with Requirement R2~~)~~ conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive to "tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated," Requirement R4 states that the evaluation must consider: (1) the unique characteristics of the identified facilities; (2) prior history ~~or~~of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and (3) intelligence or

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U. S. federal and/or Canadian governmental agencies, or their successors. Consistent with the Commission's statement that NERC should consider requiring owners and operators of identified facilities to consult with entities with appropriate expertise, Requirement R6 requires applicable Transmission Owners and Transmission Operators to select a third party to review their evaluation. This review may occur concurrently with or after the evaluation.
9. Third and finally, the Reliability Standards should require those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Reliability Standards themselves need not dictate specific steps an entity must take to protect against attacks on the identified facilities. However, the Reliability Standards need to require that owners or operators of identified critical facilities have a plan that results in an adequate level of protection against the	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R5 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring ~~that each~~the applicable Transmission Owner ~~and~~or Transmission Operator ~~that owns or operates~~of facilities identified in accordance with Requirement R1 ~~(~~and verified ~~under~~in accordance with Requirement R2~~)~~ to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive, Requirement R5 does not dictate specific steps an entity must take to protect against attacks on the identified facilities but requires applicable entities to develop a security plan that includes the following attributes to help ensure an adequate level of protection: (1)

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
potential physical threats and vulnerabilities they face at the identified critical facilities.		resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on the results of~~identified during the evaluation conducted in Requirement R4; (2) law enforcement contact and coordination information; (3) a timeline for ~~implementing~~executing the physical security enhancements and modifications specified in the physical security plan; and (4) provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).
10. All three steps of compliance with the Reliability Standard described above could contain sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure. Therefore, NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	To protect confidential or sensitive information, the Compliance Monitoring section of the standard provides that evidence demonstrating compliance with the standard must be retained at the applicable entities' facilities. Additionally, Requirements R2 and R6 require applicable entities to implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged with the~~ made available to third party ~~verifier under Requirement R2~~verifiers and reviewers and to protect or ~~the reviewing entity under Requirement R6. These steps will help ensure that lists of critical facilities or other~~exempt sensitive ~~documents remain~~ or

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
that is needed to ensure compliance with the Reliability Standards.		confidential~~.~~ information developed pursuant to the standard from public disclosure.
11. In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity. The Reliability Standards should include a procedure for the verifying entity, as well as the Commission, to add or remove facilities from an owner's or operator's list of critical facilities. Similarly, the determination of threats and vulnerabilities and the security plan should also be reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise. Finally, the Reliability Standards should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. NERC should establish a timeline for when such reevaluations should occur.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirements R2 and R6 respond to this directive. Under Requirement R3 Transmission Owners must have an unaffiliated ~~entity~~third party verify the risk assessment performed under Requirement R1. The third party verifier must be either (1) a registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or (2) an entity that has transmission planning or analysis experience. The requirement provides that the ~~verifying entity~~verification shall either verify the Transmission Owner's risk assessment or ~~recommend~~include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The verification may occur concurrently with the Requirement R1 risk assessment but must be completed within 90 calendar days of the risk assessment. The Transmission Owner is required to either modify its identification based on the verifier's recommendation or, if it disagrees with the verifier's recommendations, document the technical basis for not modifying its identification. Similarly, under Requirement R6, applicable Transmission Owners and Operators must have an unaffiliated third party review the evaluation performed under Requirement R4 and the

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		security plan(s) developed under Requirement R5. The reviewing entity must be ~~either~~ (1) an entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification; (2) an entity or organization approved by the ERO; (3) a governmental agency with physical security expertise; or (4) an entity or organization with demonstrated law enforcement, government, or military physical security expertise. The third party review must be completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The applicable Transmission Owners and Transmission Operators are required to either modify their evaluation or security plan(s) consistent with the reviewer's recommendations or, if they disagree with the recommendations, document the reasons for not modifying. Consistent with the directive to establish a timeline for periodic reevaluation of the identification of facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection, the assessment of the potential risks and vulnerabilities, and the security plans, the standard provides that Requirement R1 risk assessment should be performed at least once every 30 calendar months for those

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Transmission Owners that identified facilities in their previous risk assessment and once every 60 calendar months for those Transmission Owners that did not identify facilities in their previous risk assessment. Upon completion of each subsequent risk assessment, the applicable entities must satisfy the obligations under the remaining requirements.
12. Under the Reliability Standards, we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard. We also recognize that the industry has engaged in longstanding efforts to address the physical security of its critical facilities. Thus, NERC should develop an implementation plan that requires owners or operators of the Bulk-Power System to implement the Reliability Standards in a timely fashion, balancing the importance of protecting the Bulk-Power System from harm while giving the owners or operators adequate time to meaningfully implement the requirements. NERC should file	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	The proposed Implementation Plan addresses this directive. As provided in the Implementation Plan, the standard becomes effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows: - Requirement R2, Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard. Requirement R2, Part 2.3

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
the plan with the Reliability Standards for Commission review.		shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2. - Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2. - Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2. - Requirement R6, Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5. Requirement R6, Part 6.3 shall be completed within 60 calendar days of Requirement R6 ~~part~~Part 6.2.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2014-04: Physical Security

VRF and VSL Justifications for CIP-014-1

VRF and VSL Justifications – CIP-014-1, R1	
Proposed VRF	High
NERC VRF Discussion	Initial and subsequent risk assessments identify Transmission stations or Transmission substations that need to be assessed for threats and vulnerabilities and potential physical security measures. Since this is a Requirement in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition. This justifies a High VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the risk assessment periodicity and the identification of the primary control center that has operational control of Transmission stations and/or Transmission substations.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable CIP-002-5.1 R1, which deals with categorizing cyber systems, is assigned a High VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date;

VRF and VSL Justifications – CIP-014-1, R1	
	OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.
Proposed Moderate VSL	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.
Proposed High VSL	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in

VRF and VSL Justifications – CIP-014-1, R1	
	the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.
Proposed Severe VSL	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within

VRF and VSL Justifications – CIP-014-1, R1	
	an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if the risk assessment is not performed or if the risk assessment is not performed within required intervals.
FERC VSL G3 Violation Severity Level	The language of the VSL directly mirrors the language in the corresponding requirement.

VRF and VSL Justifications – CIP-014-1, R1	
Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to submit perform a risk assessment.

VRF and VSL Justifications – CIP-014-1, R2	
Proposed VRF	Medium
NERC VRF Discussion	Unaffiliated third party verification of initial and subsequent risk assessments provides reinforcement that the risk assessment was performed with due consideration to risk to the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of this requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. This justifies a Medium VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the unaffiliated third party verification including entities that may perform the verification, provisions for adding or removing Transmission stations and/or Transmission substations, and provisions for confidentiality of sensitive information.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable EOP-005-2 R6, which deals with verifying that its restoration plan accomplishes its intended function is assigned a medium VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but less than or equal to 100 calendar days following completion of Requirement R1;

VRF and VSL Justifications – CIP-014-1, R2	
	OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.
Proposed Moderate VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.
Proposed High VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to 120 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by part 2.3.
Proposed Severe VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days following completion of Requirement R1; OR The Transmission Owner failed to have an unaffiliated third party

VRF and VSL Justifications – CIP-014-1, R2	
	verify the risk assessment performed under Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if an unaffiliated third party verification is not performed or if the verification is not performed within prescribe timelines. The VSLs are also written indicating violation of the Requirement Part regarding protection of information.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based	The VSL is assigned for a single instance of failing to have an unaffiliated third party verification performed; or failing to perform the verification within prescribe timelines; or failing to implement procedures to protect information.

VRF and VSL Justifications – CIP-014-1, R2	
on A Single Violation, Not on A Cumulative Number of Violations	

VRF and VSL Justifications – CIP-014-1, R3	
Proposed VRF	Lower
NERC VRF Discussion	Notifying the Transmission Operator that it has operational control of a Transmission station or Transmission substation identified in Requirement R1 and verified in Requirement R2 is necessary so that the Transmission Operator may begin performance of subsequent physical security requirements for the primary control center. This is a requirement that is administrative in nature and in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. This justifies a Lower VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the notification of the Transmission Operator regarding the removal of a Transmission station or Transmission substation.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable INT-006-4 R6, which deals with notifying other entities so that Confirmed Interchange may be implemented, is assigned a Lower VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar

VRF and VSL Justifications – CIP-014-1, R3	
	days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.
Proposed Moderate VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.
Proposed High VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.
Proposed Severe VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1.

VRF and VSL Justifications – CIP-014-1, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if notification is not made subject to the conditions of the requirement.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to make the appropriate notification.

VRF and VSL Justifications – CIP-014-1, R4	
Proposed VRF	Medium
NERC VRF Discussion	Performing an evaluation of potential threats and vulnerabilities of a physical attack to each of respective Transmission station(s), Transmission substation(s), and primary control center(s) is necessary to ensure the physical security of those assets as well as the reliability of the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of this requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. This justifies a Medium VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the evaluation of potential threats and vulnerabilities of a physical attack to Transmission stations and/or Transmission substations.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable CIP-007-5 R2, which deals with a patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets, is assigned a Medium VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	N/A

VRF and VSL Justifications – CIP-014-1, R4	
Proposed Moderate VSL	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.
Proposed High VSL	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.
Proposed Severe VSL	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if a responsible entity fails to conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) or failed to consider any of the Requirement Parts 4.1-4.3.

VRF and VSL Justifications – CIP-014-1, R4	
Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) or failing to consider any of the Requirement Parts 4.1-4.3.

VRF and VSL Justifications – CIP-014-1, R5	
Proposed VRF	High
NERC VRF Discussion	Development, implementation and execution of a documented physical security plan(s) that covers applicable Transmission station(s), Transmission substation(s), and primary control center(s) is necessary to ensure the physical security of those assets as well as the reliability of the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition. This justifies a High VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the physical security plan for applicable Transmission stations, Transmission substations, or primary control centers.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable CIP-003-3 R4, which deals with implementing and documenting a program to identify, classify, and protect information associated with Critical Cyber Assets, is assigned a High VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2;

VRF and VSL Justifications – CIP-014-1, R5	
	OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.
Proposed Moderate VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.
Proposed High VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.
Proposed Severe VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission

VRF and VSL Justifications – CIP-014-1, R5	
	station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include Parts 5.1 through 5.4 in the plan.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if a responsible entity fails to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) or if the responsible entity failed to include any of the Requirement Parts 5.1-5.4.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level	The VSL is assigned for a single instance of failing to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and

VRF and VSL Justifications – CIP-014-1, R5	
Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	primary control center(s) or failing to include any of the Requirement Parts 5.1-5.4.

VRF and VSL Justifications – CIP-014-1, R6	
Proposed VRF	Medium
NERC VRF Discussion	Unaffiliated third party review of the threat evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 provides reinforcement that these requirements were performed with due consideration to risk to the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of this requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. This justifies a Medium VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the unaffiliated third party review including entities that may perform the review, timelines for completing the review and provisions for confidentiality of sensitive information.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable EOP-005-2 R6, which deals with verifying that its restoration plan accomplishes its intended function is assigned a medium VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days;

VRF and VSL Justifications – CIP-014-1, R6	
	OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.
Proposed Moderate VSL	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.
Proposed High VSL	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not and modify or document the reason for not modifying the security plan(s) as specified in Part 6.3.
Proposed Severe VSL	The Responsible Entity failed to have an unaffiliated third party

VRF and VSL Justifications – CIP-014-1, R6	
	review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.3.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if an unaffiliated third party review is not performed or if the review is not performed within prescribe timelines. The VSLs are also written indicating violation of the Requirement Part regarding protection of information.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The language of the VSL directly mirrors the language in the corresponding requirement.

VRF and VSL Justifications – CIP-014-1, R6	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to have an unaffiliated third party review performed; or failing to perform the review within prescribe timelines; or failing to implement procedures to protect information.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Reliability Standard Audit Worksheet[1]

CIP-014-1 – Physical Security

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC orders, and the language included in this document, FERC orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Applicability of Requirements *[RSAW developer to insert correct applicability]*

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1												X[3,4]			
R2												X[3,4]			
R3												X[3,4]			
R4												X[3,4]	X[4]		
R5												X[3,4]	X[4]		
R6												X[3,4]	X[4]		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

DRAFT

[3] Applicability is further defined to owners of transmission Facilities operated at 500 kV or higher (see section 4.1.1.1 of the Standard) and owners of certain transmission Facilities operating between 200 kV and 499 kV where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations, per section 4.1.1.2 of the Standard. In addition, sections 4.1.1.3 and 4.1.1.4 bring additional transmission Facilities identified as either critical to the derivation of Interconnection Reliability Operating Limits and Nuclear Plant Interface, respectively, within the purview of the standard. Please see the referenced sections of the Standard for additional details regarding applicability of the Requirements to Transmission Owners.

[4] Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

DRAFT

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Note to Auditors Concerning Third Party Verifications and Reviews

Requirements R2 and R6 prescribe, respectively, unaffiliated third party verifications for Requirement R1 and unaffiliated third party reviews for Requirements R4 and R5. Auditors are encouraged to rely on the verifications and reviews performed in cases where the verifying or reviewing entities are qualified, unaffiliated with the audited entity, and the scope of their verification or review is clear. The concept of reliance means using the work of others to avoid duplication of efforts and is consistent with recognized professional auditing standards, which are required for Compliance Audits per NERC's Rules of Procedure. Reliance in the context of this Reliability Standard means using the Requirement R2 verifications and Requirement R6 reviews to reduce audit risk and the related rigor of audit testing for Requirements R1, R4, and R5. However, in cases where the verifying or reviewing entity lacks the qualifications specified in Requirement R2 for verifications or Requirement R6 for reviewers, the required unaffiliation from the audited entity, or where the scope of the third party entity's verification or review is unclear, auditors may need to apply audit testing of Requirements R1, R4, or R5. For this reason, the Evidence Requested and Compliance Assessment Approach Sections are still present in this RSAW for Requirements R1, R4, and R5. We anticipate those sections will also facilitate expectations for entities and their unaffiliated third party verifiers and reviewers, assist Electric Reliability Organization (ERO) auditors to understand the audit procedures applied by unaffiliated third party verifiers and reviewers, and provide transparency between ERO auditors and Industry, should circumstances require audit testing of Requirements R1, R4, or R5. Further, it is an objective of the ERO to have transparent Evidence Requests and Compliance Assessment Approaches for every enforceable standard, whether they are in audit scope or not.

DRAFT

R1 Supporting Evidence and Documentation

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1.The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2)one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or
- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

Registered Entity Response (Required):

Question: Do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of Section 4.1.1? ☐ Yes ☐ No

☐ This entity does not have any applicable Transmission stations/substations.

☐ Other: [Provide explanation below]

[Include additional information regarding the question here, including the type of response and format of the response requested, as appropriate.]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R1) Provide the current and the immediately preceding dated risk assessments.
(R1) List of existing Transmission stations/substations that meet the criteria specified in Section 4.1.1.
(R1) List of Transmission stations/substations planned in the next 24 months that meet criteria specified in Section 4.1.1.
(R1 Part 1.2) List of primary control centers that operationally control each identified Transmission station/substation.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R1

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R1) Review entity's process for determining Transmission stations/substations subject to identification in accordance with Requirement R1, including weighting described in Section 4.1.1.2.
	(R1) Review entity's risk assessment process to determine the Transmission stations/substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection.
	(R1) Ensure entity's risk assessment process includes Transmission stations/substations planned in the next 24 months.

	(R1) Ensure risk assessment(s) covers each Transmission station/substation meeting applicability described in Section 4.1.
	(R1 Part 1.1) If applicable, review any prior risk assessments and verify whether or not Transmission stations/substations were identified.
	(R1 Part 1.1) Review evidence that risk assessment was performed and verify that it occurred within the past 30 months where items were identified in the previous risk assessment and 60 months where no items were identified in the previous risk assessment.

Note to Auditor: Review entity's answer to the above Question and if the auditor can verify the answer is 'no,' Requirements R3-R6 do not apply and no further audit testing of Requirements R3-R6 is necessary, unless the entity performs the Transmission Operator function for a station/substation meeting the criteria of Requirement R1 Part 1.2.

The 24 month period referenced for Transmission stations/substations planned to be in service is as of the date of the risk assessment not the date of the audit.

See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement.

Auditor Notes:

DRAFT

R2 Supporting Evidence and Documentation

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1.

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator;
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a s Transmission station or Transmission substation::

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated verifying entity and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R2) Dated evidence of third party verification of the entity's risk assessment performed under Requirement R1.
(R2 Part 2.1) Documented qualifications of the verifying party.
(R2 Part 2.3) Recommendations, if any, of the verifying party related to Requirement R1 risk assessments.
(R2 Part 2.3) Documentation of modifications and implementation of recommendations or technical basis for not implementing recommendations of the verifying party.
(R2 Part 2.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R2

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R2) Review evidence of third party verification of the entity's risk assessment and verify the following:
	(R2 Part 2.1) The reviewing entity is registered in accordance with Part 2.1 or has transmission planning or analysis experience.
	(R2 Part 2.2) Verification was completed within 90 calendar days of risk assessment.
	(R2 Part 2.3) Verifying entity's recommendations, if any, were used to modify the entity's Requirement R1 identification or the technical basis for not modifying the Requirement R1 identification is documented within 60 calendar days of completion of the verification.
	(R2 Part 2.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between the entity and third party were implemented.
Note to Auditor See Guidelines and Technical Basis section of the standard and Rationale for Requirement R2 associated with the Standard for additional details regarding the term 'unaffiliated.'	

The third party verification may occur concurrent with or after the risk assessment performed under Requirement R1.

Auditor Notes:

DRAFT

R3 Supporting Evidence and Documentation

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2.

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Registered Entity Response (Required):

Question: Are there any primary control centers identified in Requirement R1, Part 1.2 that are not under operational control of your NERC registration? ☐ Yes ☐ No

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R3) If applicable, dated communications with Transmission Operators demonstrating notification and the date of completion of Requirement R2.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R3

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R3) For each applicable primary control center identified in Requirement R1 Part 1.2 not under the control of the entity's registration, verify notification exists and contains the date of completion of Requirement R2.
	(R3 Part 3.1) For each Transmission station/substation removed under Part 3.1, ensure the responsible Transmission Operator was notified of the removal within seven calendar days of removal from identification.
Note to Auditor: Note the entity's response to the above Question. If auditor can verify the entity's answer of 'No,' then Requirement R3 is not applicable and no further audit testing is required.	

Auditor Notes:

.

R4 Supporting Evidence and Documentation

R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R4) A description of the entity's process for executing the evaluation prescribed in Requirement R4.
(R4) Dated evidence of the evaluation prescribed in Requirement R4.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R4

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R4) Review evidence of evaluation and verify it considers the following:
	(R4) Potential threats and vulnerabilities as described in Requirement R4.
	(R4 Part 4.1) Unique characteristics as described in Requirement R4 Part 4.1.
	(R4 Part 4.2) Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events.
	(R4 Part 4.3) Intelligence or warnings as described in Part 4.3.
Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement. Auditor should cross reference the Transmission stations/substations and primary control centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 to ensure it is complete.	

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R5) Dated physical security plan(s).

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R5

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R5) Review evidence and verify the physical security plan(s) covers the Transmission stations/substations and primary controls identified in Requirements R1 and/or R2, and verify plan was developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). In addition, verify the plan includes the following attributes:
	(R5 Part 5.1) Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.
	(R5 Part 5.2) Law enforcement contact and coordination information.
	(R5 Part 5.3) A timeline for executing physical security enhancements and modifications specified in the physical security plan.
	(R5 Part 5.4) Provisions to evaluate evolving physical threats, and their corresponding security measures in accordance with R5 Part 5.4
	(R5) Verify implementation of physical security plan(s). See 'Note to Auditor' for details.
Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement. Auditor should cross reference the Transmission stations/substations and primary control centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 and the security plan(s) prescribed in Requirement R5 to ensure the plan addresses vulnerabilities to	

physical attacks per the evaluation conducted in Requirement R4.

Requirement R5 includes implementation of the security plan(s), which is not within the scope of the third party review described in Requirement R6. Auditors can gain reasonable assurance security plan(s) was/were implemented by determining if specific actions prescribed by the plan(s) have taken place within the timelines established by the plan(s). For example, if the plan calls for certain procedures to occur, then auditors could ask for evidence demonstrating the procedure has been implemented within the timeline established in the security plan. Also, if the plan calls for construction of a barrier, an auditor could verify evidence that such a barrier was constructed in accordance with the entity's timeline. As auditors should obtain reasonable, not absolute, assurance the plan(s) was/were implemented, testing implementation on a sample basis may be appropriate.

Auditor Notes:

DRAFT

R6 Supporting Evidence and Documentation

R6. Each Transmission Owner identifies a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.
- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its security plan(s) consistent with the recommendation; or
- Document the reason for not modifying the security plan(s) consistent with the recommendation

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated reviewing entity and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security

plan(s) in accordance with a recommendation under Part 6.3. Examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R6) Dated Evidence of unaffiliated third party review of entity's Requirement R4 evaluation and Requirement R5 security plan(s).
(R6 Part 6.1) Evidence that reviewing entity staff meets qualifications identified in Part 6.1.
(R6 Part 6.3) Recommendations of reviewing party related to Requirement R4 evaluation and Requirement R5 security plan.
(R6 Part 6.3) Dated documentation of modifications and implementation of recommendations or reasons and compensating mitigating measures for not implementing recommendations of the reviewing party.
(R6 Part 6.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R6

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R6) Review evidence and verify the physical security plan(s) and the Requirement R4 evaluation have been reviewed by an unaffiliated third party. Also, review evidence and verify the following:
	(R6 Part 6.1) Reviewing party has the qualifications identified in Part 6.1.
	(R6 Part 6.2) Review is dated within 90 calendar days of completion of the Requirement R5 security plan.
	(R6 Part 6.3) Reviewing entity recommended changes to security plan(s) were made by entity or the reason(s) for not making the change(s) was/were documented within 60 calendar days of the completion of the unaffiliated third party review.
	(R6 Part 6.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between entity and third party were implemented.
Note to Auditor: The third party review may occur concurrent with or after the evaluation performed under Requirement R4 or the security plan develop under Requirement R5. See Guidelines and Technical Basis associated with the Standard for additional details related to qualifications of reviewing entities that may inform audited entities selection of a reviewing entity.	

Auditor Notes:

Additional Information:

Reliability Standard

The RSAW developer should provide the following information without hyperlinks. Update the information below as appropriate.

The full text of CIP-014-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology [If developer deems reference applicable]

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language [Developer to ensure RSAW has been provided to NERC Legal for links to appropriate Regulatory Language – See example below]

E.g. FERC Order No. 742 paragraph 34: "Based on NERC's…….

E.g. FERC Order No. 742 Paragraph 55, Commission Determination: "We affirm NERC's…….

Selected Glossary Terms [If developer deems applicable]

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
1	04/09/2014	Physical Security RSAW Task Force	New Document
2	05/01/2014	Physical Security RSAW Task Force	Revisions based on comments and changes to the standard.

[i] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

DRAFT

DRAFT Reliability Standard Audit Worksheet[1]

CIP-014-1 – Physical Security

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC orders, and the language included in this document, FERC orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Applicability of Requirements *[RSAW developer to insert correct applicability]*

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1												X[3,4]			
R2												X[3,4]			
R3												X[3,4]			
R4												X[3,4]	X[4]		
R5												X[3,4]	X[4]		
R6												X[3,4]	X[4]		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

DRAFT

[3] Applicability is further defined to owners of transmission Facilities operated at 500 kV or higher (see section 4.1.1.1 of the Standard) and owners of certain transmission Facilities operating between 200 kV and 499 kV where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations, per section 4.1.1.2 of the Standard. In addition, sections 4.1.1.3 and 4.1.1.4 bring additional transmission Facilities identified as either critical to the derivation of Interconnection Reliability Operating Limits and Nuclear Plant Interface, respectively, within the purview of the standard. Please see the referenced sections of the Standard for additional details regarding applicability of the Requirements to Transmission Owners.

[4] Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.~~Facilities regulated by the Nuclear Regulatory Commission or Canadian Nuclear Safety Commission are not subject to this Standard.~~

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

DRAFT

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Note to Auditors Concerning Third Party Verifications and Reviews

Requirements R2 and R6 prescribe, respectively, unaffiliated third party verifications for Requirement R1 and unaffiliated third party reviews for Requirements R4 and R5. Auditors are encouraged to rely on the verifications and reviews performed in cases where the verifying or reviewing entities are qualified, unaffiliated with the audited entity, and the scope of their verification or review is clear. The concept of reliance means using the work of others to avoid duplication of efforts and is consistent with recognized professional auditing standards, which are required for Compliance Audits per NERC's Rules of Procedure. Reliance in the context of this Reliability Standard means using the Requirement R2 verifications and Requirement R6 reviews to reduce audit risk and the related rigor of audit testing for Requirements R1, R4, and R5. However, in cases where the verifying or reviewing entity lacks the qualifications specified in Requirement R2 for verifications or Requirement R6 for reviewers, the required unaffiliation from the audited entity, or where the scope of the third party entity's verification or review is unclear, auditors may need to apply audit testing of Requirements R1, R4, or R5. For this reason, the Evidence Requested and Compliance Assessment Approach Sections are still present in this RSAW for Requirements R1, R4, and R5. We anticipate those sections will also facilitate expectations for entities and their unaffiliated third party verifiers and reviewers, assist Electric Reliability Organization (ERO) auditors to understand the audit procedures applied by unaffiliated third party verifiers and reviewers, and provide transparency between ERO auditors and Industry, should circumstances require audit testing of Requirements R1, R4, or R5. Further, it is an objective of the ERO to have transparent Evidence Requests and Compliance Assessment Approaches for every enforceable standard, whether they are in audit scope or not.

DRAFT

R1 Supporting Evidence and Documentation

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1.The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify ~~any~~ the Transmission station(s) and Transmission substation(s) that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2)one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or
- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, e~~E~~xamples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

Registered Entity Response (Required):

Question: ~~As a result of your risk assessment,~~ D~~d~~o you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of Section 4.1.1? ☐ Yes ☐ No

☐ This entity does not have any applicable Transmission stations/substations.

☐ Other: [Provide explanation below]

[Include additional information regarding the question here, including the type of response and format of the response requested, as appropriate.]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R1) Provide the current and the immediately preceding dated risk assessments ~~conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant).~~.
(R1) List of existing Transmission stations/substations that meet the criteria specified in Section 4.1.1.
(R1) List of Transmission stations/substations planned in the next 24 months that meet criteria specified in Section 4.1.1.
(R1 Part 1.2) List of primary control centers that operationally control each identified Transmission station/substation.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R1

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R1) Review entity's process for determining Transmission stations/substations subject to identification in accordance with Requirement R1, including weighting described in Section 4.1.1.2.
	(R1) Review entity's risk assessment process to determine the Transmission stations/substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection.

	(R1) Ensure entity's risk assessment process includes Transmission stations/substations planned in the next 24 months.
	(R1) Ensure ~~a~~ risk assessment(s) covers~~was performed for~~ each Transmission station/substation meeting applicability described in Section 4.1.
	(R1 Part 1.1) If applicable, review any prior risk assessments and verify whether or not Transmission stations/substations were identified.
	(R1 Part 1.1) Review evidence that risk assessment was performed and verify that it occurred within the past 30 months where items were identified in the previous risk assessment and 60 months where no items were identified in the previous risk assessment.
Note to Auditor: Review entity's answer to the above Question and if the auditor can verify the answer is 'no,' Requirements R3-R6 do not apply and no further audit testing of Requirements R3-R6 is necessary, unless the entity performs the Transmission Operator function for a station/substation meeting the criteria of Requirement R1 Part 1.2 ~~and no further audit testing of Requirements R3-R6 is necessary~~. The 24 month period referenced for Transmission stations/substations planned to be in service is as of the date of the risk assessment not the date of the audit. **See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement.**	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1.

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator;
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated third party verification~~ying entity~~ shall ~~either~~ verify the Transmission Owner's risk assessment performed under Requirement R1, which may include ~~or~~ recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a s Transmission station or Transmission substation::

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to ~~exchanged with~~ the unaffiliated verifying entity and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, e~~E~~xamples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R2) Dated evidence of third party verification of the entity's risk assessment performed under Requirement R1.
(R2 Part 2.1) Documented qualifications of the verifying party.
(R2 Part 2.3) Recommendations, if any, of the verifying party related to Requirement R1 risk assessments.
(R2 Part 2.3) Documentation of modifications and implementation of recommendations or technical basis for not implementing recommendations of the verifying party.
(R2 Part 2.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R2

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R2) Review evidence of third party verification of the entity's risk assessment and verify the following:
	(R2 Part 2.1) The reviewing entity is registered in accordance with Part 2.1 or has transmission planning or analysis experience.
	(R2 Part 2.2) Verification was completed within 90 calendar days of risk assessment.
	(R2 Part 2.3) Verifying entity's recommendations, if any, were used to modify the entity's Requirement R1 identification or the technical basis for not modifying the Requirement R1 identification is documented within 60 calendar days of completion of the verification.
	(R2 Part 2.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between the entity and third party were implemented.
Note to Auditor See Guidelines and Technical Basis section of the standard and Rationale for Requirement R2 associated with the Standard for additional details regarding the term 'unaffiliated.'	

The third party verification may occur concurrent with or after the risk assessment performed under Requirement R1.

Auditor Notes:

DRAFT

R3 Supporting Evidence and Documentation

R3. For ~~a~~the primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation ~~and~~ verified according to Requirement R2, and b) ~~that~~ is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2.

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Registered Entity Response (Required):

Question: Are there any primary control centers identified in Requirement R1, Part 1.2 that are not under operational control of your NERC registration? ☐ Yes ☐ No

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R3) If applicable, dated communications with Transmission Operators demonstrating notification and the date of completion of Requirement R2.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R3

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R3) For each applicable primary control center identified in Requirement R1 Part 1.2 not under the control of the entity's registration, verify notification exists and contains the date of completion of Requirement R2.
	(R3 Part 3.1) For each Transmission station/substation removed under Part 3.1, ensure the responsible Transmission Operator was notified of the removal within seven calendar days of removal from identification.
Note to Auditor: Note the entity's response to the above Question. If auditor can verify the entity's answer of 'No,' then Requirement R3 is not applicable and no further audit testing is required.	

Auditor Notes:

.

R4 Supporting Evidence and Documentation

R4. Each Transmission Owner that ~~owns or operates~~ identified a Transmission station, Transmission substation, or a primary control center ~~identified~~ in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of ~~f~~ attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R4) A description of the entity's process for executing the evaluation prescribed in Requirement R4.
(R4) Dated evidence of the evaluation prescribed in Requirement R4.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R4

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R4) Review evidence of evaluation and verify it considers the following:
	(R4) Potential threats and vulnerabilities as described in Requirement R4.
	(R4 Part 4.1) Unique characteristics as described in Requirement R4 Part 4.1.
	(R4 Part 4.2) Prior history of ~~r~~ attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events.
	(R4 Part 4.3) Intelligence or warnings as described in Part 4.3.
Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement. Auditor should cross reference the Transmission stations/substations and primary c~~C~~ontrol c~~C~~enters identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 to ensure it is complete.	

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Transmission Owner that identified ~~owns or has operational control of~~ a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on the results of~~identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for ~~implementing~~ executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating ~~implementation~~ execution of the physical security plan according to the timeline specified in the physical security plan.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R5) Dated physical security plan(s).

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R5

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R5) Review evidence and verify the physical security plan(s) covers the Transmission stations/substations and primary controls identified in Requirements R1 and/or R2, and verify plan was ~~implemented~~ developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). In addition, verify the plan includes the following attributes:
	(R5 Part 5.1) Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on the results of~~identified during the evaluation conducted in Requirement R4.
	(R5 Part 5.2) Law enforcement contact and coordination information.
	(R5 Part 5.3) A timeline for ~~implementing~~ executing physical security enhancements and modifications specified in the physical security plan.
	(R5 Part 5.4) Provisions to evaluate evolving physical threats, and their corresponding security measures in accordance with R5 Part 5.4
	(R5) Verify implementation of physical security plan(s). See 'Note to Auditor' for details.
Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement. Auditor should cross reference the Transmission stations/substations and primary c~~C~~ontrol c~~C~~enters	

identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 and the security plan(s) prescribed in Requirement R5 to ensure the plan addresses vulnerabilities ~~that would facilitate~~to physical attacks ~~that have a high probability or likelihood of occurrence~~per the evaluation conducted in Requirement R4.

Requirement R5 includes implementation of the security plan(s), which is not within the scope of the third party review described in Requirement R6. Auditors can gain reasonable assurance security plan(s) was/were implemented by determining if specific actions prescribed by the plan(s) have taken place within the timelines established by the plan(s). For example, if the plan calls for certain procedures to occur, then auditors could ask for evidence demonstrating the procedure has been implemented within the timeline established in the security plan. Also, if the plan calls for construction of a barrier, an auditor could verify evidence that such a barrier was constructed in accordance with the entity's timeline. As auditors should obtain reasonable, not absolute, assurance the plan(s) was/were implemented, testing implementation on a sample basis may be appropriate.

Auditor Notes:

DRAFT

R6 Supporting Evidence and Documentation

R6. Each Transmission Owner ~~that owns or operates~~identifies a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.
- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer~~ing entity~~ recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its security plan(s) consistent with the recommendation; or
- Document the reason for not modifying the security plan(s) consistent with the recommendation

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged~~ made available to ~~with~~ the unaffiliated reviewing entity ~~and from any other form of public disclosure~~ and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation

performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R6) Dated Evidence of unaffiliated third party review of entity's Requirement R4 evaluation and Requirement R5 security plan(s).
(R6 Part 6.1) Evidence that reviewing entity staff meets qualifications identified in Part 6.1.
(R6 Part 6.3) Recommendations of reviewing party related to Requirement R4 evaluation and Requirement R5 security plan.
(R6 Part 6.3) Dated documentation of modifications and implementation of recommendations or reasons and compensating mitigating measures for not implementing recommendations of the reviewing party.
(R6 Part 6.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R6

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R6) Review evidence and verify the physical security plan(s) and the Requirement R4 evaluation have been reviewed by an unaffiliated third party. Also, review evidence and verify the following:
	(R6 Part 6.1) Reviewing party has the qualifications identified in Part 6.1.
	(R6 Part 6.2) Review is dated within 90 calendar days of completion of the Requirement R5 security plan.
	(R6 Part 6.3) Reviewing entity recommended changes to security plan(s) were made by entity or the reason(s) for not making the change(s) was/were documented within 60 calendar days of the completion of the unaffiliated third party review.
	(R6 Part 6.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between entity and third party were implemented.
Note to Auditor: The third party review may occur concurrent with or after the evaluation performed under Requirement R4 or the security plan develop under Requirement R5. See Guidelines and Technical Basis associated with the Standard for additional details related to qualifications of reviewing entities that may inform audited entities selection of a reviewing entity.	

Auditor Notes:

Additional Information:

Reliability Standard

The RSAW developer should provide the following information without hyperlinks. Update the information below as appropriate.

The full text of CIP-014-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology [If developer deems reference applicable]

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language [Developer to ensure RSAW has been provided to NERC Legal for links to appropriate Regulatory Language – See example below]

E.g. FERC Order No. 742 paragraph 34: "Based on NERC's…….

E.g. FERC Order No. 742 Paragraph 55, Commission Determination: "We affirm NERC's…….

Selected Glossary Terms [If developer deems applicable]

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
1	04/09/2014	Physical Security RSAW Task Force	New Document
2	05~~4~~/01~~XX~~/2014	Physical Security RSAW Task Force	Revisions based on comments and changes to the standard.

[i] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

DRAFT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security
CIP-014-1

Final Ballot Now Open through May 5, 2014

Now Available

A final ballot of **CIP-014-1 – Physical Security** is now open through **8 p.m. Eastern on Monday, May 5, 2014.**

In an order issued March 7, 2014, the Federal Energy Regulatory Commission directed NERC to file a physical security standard within 90 days of the order (i.e. by June 5, 2014). On March 21, 2014, the NERC Standards Committee (SC) authorized a waiver of the standard development process, in accordance with Section 16 of the Standard Processes Manual, to meet this pending regulatory deadline. The SC approved to shorten this final ballot period from 10 days to 5 calendar days. (Section 4.9)

If you have questions please contact Stephen Crutchfield via email or by telephone at (609) 651-9455. Background information for this project can be found on the project page.

Instructions for Balloting

In the final ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their previously cast votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the final ballot window. If a ballot pool member does not participate in the final ballot, that member's vote cast in the previous ballot will be carried over as that member's vote in the final ballot.

Members of the ballot pool associated with this project may log in and submit their vote for the standard by clicking here.

Next Steps

Voting results for the standard will be posted and announced after the ballot window closes. If approved, it will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security
CIP-014-1

Final Ballot Results

Now Available

A final ballot for **CIP-014-1 – Physical Security** concluded at **8 p.m. Eastern on Monday, May 5, 2014.**

The standard achieved a quorum and sufficient affirmative votes for approval. Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results for the ballot.

Standard	Quorum / Approval
CIP-014-1	92.53% / 85.61%

Background information for this project can be found on the project page.

Next Steps
The standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

For information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller (via email), Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results	
Ballot Name:	2014-04_Physical_Security_CIP-014-1
Ballot Period:	5/1/2014 - 5/5/2014
Ballot Type:	Final
Total # Votes:	421
Total Ballot Pool:	455
Quorum:	**92.53 % The Quorum has been reached**
Weighted Segment Vote:	85.61 %
Ballot Results:	**A quorum was reached and there were sufficient affirmative votes for approval.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	121	1	97	0.858	16	0.142	0	3	5
2 - Segment 2	8	0.6	6	0.6	0	0	0	1	1
3 - Segment 3	104	1	85	0.924	7	0.076	0	4	8
4 - Segment 4	38	1	31	0.912	3	0.088	0	1	3
5 - Segment 5	101	1	76	0.905	8	0.095	0	5	12
6 - Segment 6	60	1	55	0.965	2	0.035	0	1	2
7 - Segment 7	5	0.3	3	0.3	0	0	0	0	2
8 - Segment 8	6	0.6	2	0.2	4	0.4	0	0	0
9 - Segment 9	3	0.1	1	0.1	0	0	0	2	0

10 - Segment 10	9	0.6	4	0.4	2	0.2	0	2	1
Totals	**455**	**7.2**	**360**	**6.164**	**42**	**1.036**	**0**	**19**	**34**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke		
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Negative	COMMENT RECEIVED
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Hudson Gas & Electric Corp.	Frank Pace	Negative	
1	Central Iowa Power Cooperative	Kevin J Lyons	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	East Kentucky Power Coop.	Amber Anderson	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Edison Electric Institute	David Batz	Affirmative	
1	El Paso Electric Company	Pablo Onate	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Negative	COMMENT RECEIVED
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Affirmative	
1	Gainesville Regional Utilities	Richard Bachmeier	Affirmative	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Negative	
1	Idaho Power Company	Molly Devine	Negative	
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	

1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John Chin	Abstain	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Los Angeles Department of Water & Power	John Burnett	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Affirmative	COMMENT RECEIVED
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton	Negative	
1	Network & Security Technologies	Nicholas Lauriat	Abstain	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Negative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Chelan County	Chad Bowman	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Negative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Southwestern Power Administration	Angela L Summer	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	

1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blue Ridge Electric	James L Layton		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	Central Hudson Gas & Electric Corp.	James J McCloskey		
3	City of Anaheim Public Utilities Department	Dennis M Schmidt	Abstain	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Abstain	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Negative	COMMENT RECEIVED
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	East Kentucky Power Coop.	Patrick Woods	Negative	SUPPORTS THIRD PARTY COMMENTS
3	El Paso Electric Company	Rhonda Bryant	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	Entergy	Kevin Weber	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		

3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes		
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Mace D Hunter	Affirmative	
3	Lee County Electric Cooperative	David A Hadzima		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	National Rural Electric Cooperative Association	Patricia E Metro	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	North Carolina Municipal Power Agency #1	Kathy Moyer	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Chelan County	Steve Wickel	Affirmative	
3	Public Utility District No. 1 of Clallam County	Doug Adams	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Southern Indiana Gas and Electric Co.	Fred Frederick	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave		
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell	Affirmative	

4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Negative	COMMENT RECEIVED
4	DTE Electric	Daniel Herring	Affirmative	
4	Eugene Water & Electric Board	Dean Ahlsten	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	COMMENT RECEIVED
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas	Affirmative	
4	Garkane Energy	Mike Avant		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney	Affirmative	
4	Southern Minnesota Municipal Power Agency	Richard L Koch		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	Acciona Energy North America	George E Brown	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke		
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Negative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Negative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Abstain	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy Power Management, LLC	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Negative	COMMENT RECEIVED
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	

5	East Kentucky Power Coop.	Stephen Ricker	Negative	SUPPORTS THIRD PARTY COMMENTS
5	El Paso Electric Company	Gustavo Estrada	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Empire District Electric Co.	mike l kidwell	Affirmative	
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Hydro-Québec Production	Roger Dufresne	Negative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lafayette Utilities System	Jamie B Webb		
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Chelan County	John Yale	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Illinois Power Coop.	Alvis D Lanton		
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	

5	Tennessee Valley Authority	David Thompson	Negative	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot	Affirmative	
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	El Paso Electric Company	Luis Rodriguez	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley		
6	New York Power Authority	Saul Rojas	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative	
6	Northern California Power Agency	Steve C Hill	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp	Affirmative	
6	Powerex Corp.	Gordon Dobson-Mack	Abstain	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard	Affirmative	
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	

6	Westar Energy	Grant L Wilkerson		
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Wisconsin Public Service Corp.	David Hathaway	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Eastman Chemical Company	David L Moore		
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Praxair Inc.	David Meade		
7	Siemens Energy, Inc.	Frank R. McElvain	Affirmative	
7	Valero Services, Inc.	Lee W Morris	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner	Negative	COMMENT RECEIVED
8		David L Kiguel	Negative	
8	Foundation for Resilient Societies	William R Harris	Negative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Idaho State Public Utilities Commission	Johanna Bell	Affirmative	
9	National Association of Regulatory Utility Commissioners	Jerry M Maio	Abstain	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Negative	
10	Southwest Power Pool RE	Bob Reynolds	Negative	
10	Texas Reliability Entity, Inc.	Derrick Davis	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2014 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Exhibit G

Standard Drafting Team Roster

Project 2014-04 Physical Security

Standard Drafting Team

Name and Title	Company and Address	Contact Info	Bio
Susan Ivey Chair	2301 Market St. Philadelphia, PA 19103	215-841-4706 SusanO'Brien.Ivey@exeloncorp.com	Ms. Ivey is Vice President of the Transmission Strategy & Compliance of Exelon. She is responsible for oversight of the electric transmission systems of the Exelon Utilities of BGE, ComEd and PECO located in Baltimore, Chicago and Philadelphia, respectively. Ms. Ivey coordinates the efforts for electric transmission operations and long-term planning for all three companies, and manages the interface with regulatory authorities and all transmission interconnected third parties. Ms. Ivey oversees and administers the NERC Compliance Program for Exelon. She also leads the coordination of physical security practices across the Exelon Utilities to ensure alignment of strategies and programs for addressing security risks associated with the electric and gas businesses.
Lou Oberski Vice-Chair	Dominion Resources Services, Inc. 120 Tredegar St Richmond, VA 23219	804-819-2837 Lou.Oberski@dom.com	Mr. Oberski is Managing Director of the Regulation and NERC Compliance Policy for Dominion Resources Services, Inc. He is responsible for administration of all aspects of Dominion's corporate NERC compliance assurance programs and oversees Dominion's involvement at NERC and its sub-regions as well as FERC and RTO policy coordination for Dominion at PJM, ISO-New England and the MidContinent ISO. Prior to Mr. Oberski's current position, his career at Dominion covered increasing management responsibilities in transmission engineering, operations, planning and maintenance. The most recent 10 years have focused on developing, establishing and coordinating NERC and RTO policy at Dominion with a particular emphasis on generation supplier policy at NERC and RTOs. Mr. Oberski is a member of the North American Energy Standards Board, Board of Directors and past chair of its Executive Committee. He is also a member of EEI's Reliability Executive Advisory Committee, the SERC Board of Directors and SERC Board Executive Committee. Mr. Oberski has been employed by Dominion for 30 years and holds a Bachelor's degree in electrical engineering from Western Michigan University.
John Breckenridge	KCP&L 1200 Main Street 18th Floor KCMO 64106	816-654-1725 john.breckenridge@kcpl.com	Mr. Breckenridge is the Senior Manager of Corporate Security for Kansas City Power & Light based in Kansas City, MO. In his current capacity, Mr. Breckenridge directs the overall Corporate Security function to ensure security operations are in compliance with legal, regulatory, and company requirements. Corporate Security responsibilities

			include physical security, investigations, guard force management, protection operations, law enforcement liaison, enterprise-wide crisis management and business continuity planning. To be effective, Mr. Breckenridge uses his 25 plus years of military, criminal justice and industrial security experience to work with each functional department and business unit. Mr. Breckenridge began his career while in the U.S. Army, where he was instrumental in supporting many special security operations throughout the U.S. and in many countries, especially during his assignment in Europe. In addition to his eight-year career in the military, Mr. Breckenridge worked for six years in the Jackson County, MO. criminal justice system. During this time, Mr. Breckenridge specialized in security systems, close protection operations and special event security functions first with the Department of Corrections and then in conjunction with the Jackson County Courts. From 1993 until 2008, Mr. Breckenridge was the Director of Security and Chief Security Officer for Aquila Energy until Aquila was purchased by Kansas City Power & Light. Mr. Breckenridge is Board Certified in Security Management as a Certified Protection Professional, holds a BLA degree and a degree with an emphasis in Criminal Justice, and is a Licensed Private Investigator and an active member of several security related professional organizations. Mr. Breckenridge has been featured as a Guest Lecturer for successful business approaches to security issues and has also been featured in several trade and regional publications.
Ross Johnson	Capital Power	(780) 405-5542 rjohnson@capitalpower.com	Mr. Johnson, CPP is the Senior Manager of Security and Contingency Planning for Capital Power. He served in the Canadian Forces as an infantry and intelligence officer for 24 years. Since leaving the service in 2001, Mr. Johnson has been employed in several security-related leadership positions in aviation security, the offshore oil industry, and the electricity sector. Prior to joining Capital Power in 2009, Mr. Johnson was the Director of Security and Contingency Planning with EPCOR Utilities. Mr. Johnson is the author of Antiterrorism Planning and Threat Response, a book on the prevention of terrorist attacks. Mr. Johnson is a member of the NERC Critical Infrastructure Protection Committee, where he sits on the Executive Committee. He is also Chair of the Committee's Physical Security Working Group, and the leader of the Physical Security Roundtable Group. Mr. Johnson is Chair of the Canadian Electricity Association's Security and Infrastructure Protection Committee, and Chair of ASIS

			International's Petrochemical, Chemical, and Extractive Industries Security Council. Mr. Johnson has a Baccalaureate in Military Arts and Sciences with Distinction, and is board-certified in security management by ASIS International.
Kathleen Judge	National Grid 939 Southbridge Street, Worcester, MA 01610	(508) 860-6040 Kathleen.judge@nationalgrid.com	Ms. Judge is Director of Risk and Compliance for Security at National Grid, where she has worked for 25+ years. She is responsible for managing National Grid's strategies and best practices required to protect energy delivery facilities in accordance with governing security regulations in the US. As part of this Ms. Judge is actively engaged with state and federal regulatory authorities to shape policies and procedures. For example, at the federal level she works with the Infrastructure Security Compliance Division of DHS, the United States Coast Guard and the Pipeline Security Division of the Transportation Security Administration. Ms. Judge was also the chair of the American Gas Association Security Committee and currently serves as an AGA representative on the Oil & Natural Gas Sector Coordinating Council. She is also actively involved in the EEI Security Committee and serves on the Executive Steering Committee for the Long Island Sound Area Maritime Security Committee. In prior roles, she was responsible for, and a key member on, delivering Company's business plan for a deregulated energy market, serving as the strategic and operational expert on electricity restructuring for Massachusetts, Rhode Island, New Hampshire and New York. She was also an active member of the North American Energy Standards Board Retail Electric Quadrant, developing model business practices for deregulated marketplaces. Leading up to this, Ms. Judge was a key developer and implementer of an award winning renewable energy program in Massachusetts and Rhode Island. Ms. Judge holds a Masters of Business Administration degree from Nichols College.
Mike O'Neil	Florida Power & Light 700 Universe Blvd., Juno Beach, Fl. 33408	(561) 904-3503 mco0hwz@fpl.com	Mr. O'Neil is Director of the Power Delivery Compliance & Regulatory. He is responsible for business unit execution compliance to transmission based FERC requirements for FPL and NERC transmission reliability standards for FPL and NEER facilities throughout the country.
Stephen Pelcher	Santee Cooper One Riverwood Drive Moncks Corner, SC 29461	843-761-4016 srpelche@santeecooper.com	Mr. Pelcher is Deputy General Counsel Nuclear and Regulatory Compliance at Santee Cooper. Mr. Pelcher joined Santee Cooper in 1996. Prior to working for Santee Cooper, he was Senior Attorney for Duquesne Light Company in Pittsburgh (1990 to 1996). Mr. Pelcher has been a practicing attorney

			for more than 31 years and has worked in the electric utility industry for 24 years. Among other duties, Mr. Pelcher is the lead Santee Cooper company attorney in all matters within the jurisdiction of the FERC under Part II of the Federal Power Act; the lead company attorney relating to interpretation of requirements embedded within standards established by NERC under Section 215 of the Federal Power Act and current Chair of Santee Cooper's internal Reliability Standards Compliance Coordination Committee. Mr. Pelcher has a Bachelor of Arts degree in Philosophy from the University of Pittsburgh, College of Arts and Sciences; a Juris Doctor from the University of Pittsburgh, School of Law; and an LL.M (Taxation) from the Dickinson School of Law, Pennsylvania State University.
John Pespisa	Southern California Edison 2244 Walnut Grove Ave. Rosemead, Ca 91770	626-688-6291 John.pespisa@sce.com	Mr. Pespisa is Director of SCE's NERC Compliance program and Acting Director of SCE's Security Technology & Compliance group. Mr. Pespisa started his career with Southern California Edison in 1987, starting in transmission operations and electrical substations. Since then he has worked in positions of increasing responsibility including operation of SCE's bulk electric and distribution systems, and supervisory positions at SCE's Energy Control Center, including Manager of short term power marketing, and Manager of Real-Time Power Operations. In 2011, he moved to his current position as the Director of SCE's NERC Compliance Program In his current role he oversees SCE's compliance with federal Reliability Standards, which have been promulgated to ensure the safe, reliable operation of the power grid, and to protect the grid's critical infrastructure against cyber threats. Mr. Pespisa is a graduate of California State Los Angeles and hold degrees in Electrical Engineering and Business Management.
Robert Rhodes	Southwest Power Pool 201 Worthen Drive Little Rock, AR 72223	501-614-3241 rrhodes@spp.org	Mr. Rhodes is the Manager of Reliability Standards at Southwest Power Pool (SPP) where he has been employed since 2000. In his previous role at SPP he was Manager of Reliability Coordination for over 10 years. Prior to joining SPP, Mr. Rhodes worked at Progress Energy (Carolina Power & Light Company) in Raleigh, NC for over 26 years in various positions in transmission maintenance, operations and planning. In his current capacity, Mr. Rhodes works with SPP members, SPP staff and other industry experts to ensure that reliability standards necessary to maintain a reliable bulk electric system are in place. He coordinates SPP members and registered entities in the development, refinement, maintenance, communication, training and implementation of national and regional reliability standards and policies.

			Mr. Rhodes is active at NERC currently serving on the Operating Reliability Subcommittee (ORS), the ORS Executive Committee, the Resources Subcommittee, the Standards Committee Process Subcommittee, the Reliability Coordination Standard Drafting Team, the Operating Personnel Communications Protocols Standard Drafting Team and the TOP/IRO Revisions Standard Drafting Team. He has previously served on the Reliability Coordinator Working Group, the Interchange Distribution Calculator Working Group and was Vice Chair of the Distribution Factor Working Group. Additionally, he has served on committees, working groups and task forces in SPP, SERC and VACAR. Mr. Rhodes received an Associate in Science degree from Rockingham Community College in 1970, a Bachelor of Science degree in Electrical Engineering from North Carolina State University in 1972 and a Master of Engineering degree from Rensselaer Polytechnic Institute in 1974. He is a member of Tau Beta Pi, Eta Kappa Nu, Order of the Engineer, the Institute of Electrical and Electronics Engineers and its Power Engineering Society and the National Society of Professional Engineers. He is a NERC Certified System Operator (Reliability) and is a registered professional engineer in the State of North Carolina.
Allan Wick	Tri-State Generation & Transmission Association, Inc. 1100 W. 116th Ave., Westminster, CO 80234	303-254-3341 awick@tristategt.org	Mr. Wick is a 30 year security executive, 13 in the energy sector with a comprehensive industry perspective after working for an investor owned utility, independent system operator and now at a cooperative generation and transmission company - where he serves as their Enterprise Security Manager & Chief Security Officer. He is a member of the ASIS International Utilities Security Council and the WECC Physical Security Working Group since 2005. He also served for six years on the ASIS International Certification Board of Directors. Mr. Wick has designed and implemented enterprise-wide physical security programs for three different organizations, served as a drafting team member for five ANSI standards, and has authored a number of security related magazine articles and white papers. Mr. Wick received his MBA from Webster University and holds multiple security and business continuity certifications, including CPP, PSP, CBCP, CFE, and PCI.
Manho Yeung	Pacific Gas and Electric Company Mail Code N9G, P.O. Box 770000 San Francisco, California, 94177	415-973-7649 MxY6@pge.com	Mr. Yeung is Senior Director of System Planning and Reliability, for Pacific Gas and Electric Company and is responsible for electric transmission and distribution planning, asset and risk management and reliability improvements. Mr. Yeung oversees PG&E's capital investment plan in expanding, upgrading and modernizing its 18,500

			miles of electric transmission lines, 850 substations, and 140,000 miles of distribution lines. Mr. Yeung has been with Pacific Gas and Electric Company since 1980 and has over 30 years of energy policy, electric generation planning, electric T&D planning, asset and risk management, project management, engineering, and operations experience. Mr. Yeung received his Bachelor of Science degree in electric engineering from the Georgia Institute of Technology, and a Master of Science degree in electric engineering from the Santa Clara University. Manho is a registered professional electric engineer in the State of California.
Stephen Crutchfield Standards Developer	North American Electric Reliability Corporation 3353 Peachtree Road, NE, Suite 600 - North Tower Atlanta, GA 30326	609-651-9455 Stephen.crutchfield@nerc.net	Mr. Crutchfield is the lead NERC Staff Coordinator for Project 2014-04, Physical Security. Stephen began his career with NERC in May 2007. Prior to joining NERC, Mr. Crutchfield was a Project Manager with Shaw Energy Delivery Services, managing engineering and construction projects in the substation and transmission line fields. Mr. Crutchfield's background also includes experience with PJM as Manager of RTO Integration, working on the operations and markets integration of new members (AEP, ComEd, Dayton, Dominion and Duquesne) into PJM and southern seams operations issues with Progress Energy, Duke and TVA. Stephen also helped lead the team that was developing GridSouth in the dual roles of Organization Architect and Manager of Customer Support. Prior to GridSouth, Mr. Crutchfield was the Manager of Power System Operations Training at Progress Energy where he spent over 10 years training System Operators and Engineers. Overall, Stephen was with Progress Energy for 16 years. Mr. Crutchfield received his Bachelor of Arts in Physics from the University of Virginia and Masters of Science in Electrical Engineering from North Carolina State University. Stephen holds a Master of Science in Management degree, also from North Carolina State University. Mr. Crutchfield is also a member of the Institute of Electrical and Electronic Engineers and the Power and Energy Society.
Steven Noess Associate Director of Standards Development, Standards	North American Electric Reliability Corporation 3353 Peachtree Road, NE, Suite 600 - North Tower Atlanta, GA 30326	404-217-9691 steven.noess@nerc.net	Mr. Noess is Associate Director of Standards Development at the North American Electric Reliability Corporation (NERC) in Atlanta, GA, and has been employed by NERC since 2011. Prior to joining NERC, Mr. Noess was an attorney at the Minnesota Legislature. Before becoming an attorney, Mr. Noess was an officer in the United States Army. Mr. Noess has a bachelor's of science degree from the U.S. Military Academy, West Point, NY, and a law degree from the University of Minnesota Law School.

Mark Olson Standards Developer	North American Electric Reliability Corporation 3353 Peachtree Road, NE, Suite 600 - North Tower Atlanta, GA 30326	404-446-9760 Mark.olson@nerc.net	Mr. Olson is a Standards Developer at the North American Electric Reliability Corporation (NERC), and has been employed by NERC since 2012. Previously he was a career officer in the U.S. Navy where he served in various positions related to the operations and management of surface ships and naval personnel. Mr. Olson has a master's degree in electrical engineering from the Naval Postgraduate School and a bachelor's degree from the U.S. Naval Academy.
Brian Harrell Director, ES-ISAC Operations	Electricity Sector Information Sharing and Analysis Center North American Electric Reliability Corporation 1325 G Street NW, Suite 600 Washington, DC 20005	202-400-3003 office | 609-651-0671 (c) Brian.Harrell@nerc.net	Mr. Harrell is the Director, ES-ISAC Operations for the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) at the North American Electric Reliability Corporation (NERC), joining NERC in August 2010. In this capacity he is responsible for managing situational awareness, incident management, and security coordination for the electricity sector through timely, reliable and secure information exchange. Mr. Harrell has 18 years of experience in the security industry serving in organizations such as law enforcement, military, and corporate security, among others. Mr. Harrell is formerly the NERC Director of Critical Infrastructure Protection Programs, as well as the CIP Manager for the SERC Reliability Corporation, where he oversaw electricity security related matters. Prior to joining SERC, Mr. Harrell was the Sector Security Specialist for the Infrastructure Security Compliance Division at the U.S. Department of Homeland Security (DHS). Brian specialized in securing high risk facilities and Continuity of Operations (COOP) for DHS. Mr. Harrell also served in the US Marine Corps as an Anti-Terrorism and Force Protection Instructor.
Bob Canada Manager, Outreach & Training	North American Electric Reliability Corporation 3353 Peachtree Road, NE, Suite 600 - North Tower Atlanta, GA 30326	404-446-9709 bob.canada@nerc.net	Mr. Canada presently serves as the Manager, Outreach and Training, at the NERC and is the staff support and Secretary to the Critical Infrastructure Protection Committee standing committee. Mr. Canada was previously employed in the electric industry for 32 years with Southern Company in various roles with corporate security and was Manager of Corporate Security at Georgia Power Company from March 1995 - December 2002. Responsibilities included corporate and internal investigations, physical security of employees and corporate assets. Mr. Canada directed alarm systems design and installation as well and was responsible for the overall corporate response for security at Georgia Power Co. He also directed the Georgia Power and Southern Company Security Planning for the Atlanta Olympic Games. Responsible for the development of the corporate security plan along with the

			implementation and daily operations included physical security of the transmission and distribution facilities supporting the Olympic venues, monitoring the protective countermeasures in place, consulting with Federal, State and Local Law Enforcement Agencies to protect the State, Metropolitan and Atlanta Electrical Infrastructure. Mr. Canada served two terms for the Southeastern Reliability Council (SERC) as the first Chairman of the Critical Infrastructure Protection Committee and represented SERC on the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Committee (CIPC) as the Physical Security voting member. Subsequently, he was elected by the CIPC as a Vice Chair for four terms. Mr. Canada received his Bachelor's degree from West Georgia State University and also holds a Juris Doctor from the Woodrow Wilson College of Law.

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)**	**Docket No. RM14-10-000**

SUPPLEMENTAL INFORMATION TO PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF RELIABILITY STANDARD BAL-001-2—REAL POWER BALANCING CONTROL PERFORMANCE

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

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

Counsel for the North American Electric Reliability Corporation

May 9, 2014

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. RM14-10-000**

SUPPLEMENTAL INFORMATION TO PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF RELIABILITY STANDARD BAL-001-2—REAL POWER BALANCING CONTROL PERFORMANCE

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA")[1] and Section 39.5[2] of the Federal Energy Regulatory Commission's ("FERC" or "Commission") regulations, the North American Electric Reliability Corporation ("NERC")[3] hereby submits supplemental information to its April 2, 2014 petition for approval of proposed Reliability Standard BAL-001-2—Real Power Balancing Control Performance ("Petition").[4] NERC is providing this supplemental information in order to address the status of a Commission directive in Order No. 693 and update the Commission regarding the status of the field trial for proposed Reliability Standard BAL-001-2.

I. SUMMARY OF PROPOSED RELIABILITY STANDARD BAL-001-2

Proposed Reliability Standard BAL-001-2 defines Balancing Authority ACE Limits ("BAAL") which are unique for each Balancing Authority and provide dynamic limits for the Balancing Authority's ACE value as a function of the Interconnection frequency.[5] These ACE

---

1 16 U.S.C. § 824o (2006).

2 18 C.F.R. § 39.5 (2013).

3 The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006).

4 The BAL-001 Reliability Standard is also commonly referred to as the "Control Performance Standard" and its two requirements are known as "Control Performance Standard 1" or "CPS 1" and "Control Performance Standard 2" or "CPS2." In the proposed BAL-001-2 Reliability Standard, the underlying performance aspect of the Requirement is unchanged and Requirement R1 is still commonly referred to as "CPS 1." Requirement R2 of the proposed BAL-001-2 Reliability Standard has been substantively changed and is commonly referred to as "BAAL."

5 "Balancing Authority ACE Limit" or "BAAL" was derived based on reliability studies and analysis which defined a Frequency Trigger Limit bound measured in Hz. The Frequency Trigger Limit is equal to Scheduled

limits are pre-established, vary as a function of the deviation of actual Interconnection frequency from the scheduled Interconnection frequency, and become more limiting as deviations become larger. One of the reliability benefits of the proposed Reliability Standard is that it allows Balancing Authorities to calculate their position within these boundaries on a Real-time basis and take action to support reliability. While the proposed BAL-001-2 Reliability Standard is applicable to Balancing Authorities, it is functionally an Interconnection-wide Reliability Standard.

Proposed Reliability Standard BAL-001-2 consists of two requirements that work together to ensure both long-term and short-term reliability. Requirement R1 (also commonly referred to as "CPS 1") is intended to measure how well a Balancing Authority is able to control its generation and load management programs, as measured by its ACE, to support its Interconnection's frequency over a rolling one-year period. Requirement R2 (also commonly referred to as "BAAL") is intended to enhance the reliability of each Interconnection by maintaining frequency within predefined limits under all conditions and includes a 30 consecutive clock-minute component.

The body of NERC Reliability Standards work together as an integrated whole to protect and preserve the reliability of the Bulk-Power System. In particular, the Resource and Demand Balancing ("BAL") Reliability Standards work together to address various aspects of interconnection frequency as it pertains to reliable operations. Reliability Standard BAL-001 controls Interconnection frequency within defined limits. Reliability Standard BAL-002 ensures

---

Frequency, plus or minus three times an Interconnection's Epsilon 1 value. Epsilon 1 is the root mean square targeted frequency error for each Interconnection, as recommended by the NERC Resources Subcommittee and approved by the NERC Operating Committee. Epsilon 1 values for each Interconnection are unique. When a Balancing Authority exceeds its BAAL, it is providing more than its share of risk that the Interconnection will exceed its Frequency Trigger Limit. When all Balancing Authorities are within their BAAL (high and low), the Interconnection frequency will be within its Frequency Trigger Limits.

that Balancing Authorities or Reserve Sharing Groups balance resources and demand and return Area Control Error to defined values. Reliability Standard BAL-003 provides consistent methods for measuring Frequency Response and determining the Frequency Bias Setting. In particular, these three BAL Reliability Standards work together because the components of Operating Reserve – frequency responsive reserve, Regulating Reserve and Contingency Reserve are always used in conjunction with one another.

II. SUPPLEMENTAL INFORMATION

A. The Proposed Reliability Standard BAL-001-2 Addresses a Commission Directive in Order No. 693

The proposed BAL-001-2 Reliability Standard addresses a Commission directive in Order No. 693 (at P 355) in an equally efficient and effective manner. In Order No. 693, the Commission noted that the BAL-002-0 Reliability Standard did not define a significant deviation or a reportable event. The Commission stated:

> we direct the ERO, through the Reliability Standards development process, to modify this Reliability Standard to define a significant deviation and a reportable event, taking into account all events that have an impact on frequency, e.g., loss of supply, loss of load and significant scheduling problems, which can cause frequency disturbances and to address how balancing authorities should respond. As suggested by NRC, this or a related Reliability Standard should also include a frequency response requirement. The present Control Performance Standards represent the monthly and yearly averages which are appropriate for measuring long-term trends but may not be appropriate for measuring short-term events. In addition, the measures should be available to the balancing authorities to assist in real-time operations.[6]

As the Commission noted in Paragraph 355 of Order No. 693, loss of supply, loss of load and significant scheduling problems, can cause frequency disturbances – all of which are captured by the limits established in proposed Reliability Standard BAL-001-2. By establishing safe

[6] Order No. 693 at P 355 (internal citation omitted).

operating frequency ranges, events that cause frequency disturbances are captured as deviations. While the Commission directed NERC to modify the BAL-002-0 Reliability Standard to address this issue, the revisions to proposed Reliability Standard BAL-001-2 are equally efficient and effective.

Under BAL-001-2, BAAL and CPS 1 work together to support Interconnection frequency. An entity is in violation of Requirement R2 of proposed Reliability Standard BAL-001-2 when it exceeds its BAAL for 30 consecutive clock-minutes or more. While entities could be out of limits for a time period less than that, this performance is captured by Requirement R1, which measures long-term trends. For example, if a Balancing Authority ACE is exactly equal to its BAAL, its CPS 1 under Requirement R1 is -700%. For each minute that the Balancing Authority exceeds its BAAL, or is operating close to its BAAL, it is accumulating substantial negative values of CPS 1 (under Requirement R1). Such negative values must then be balanced by substantially better performance by an entity -- and all of this performance is factored into compliance, given the manner in which Requirements R1 and R2 are interrelated.

When a Balancing Authority's operation is hurting Interconnection frequency, the BAAL gets tighter for the BA as the frequency moves away from 60 Hz. While an entity might not be in violation of Requirement R2 if it exceeds its BAAL for less than 30 consecutive clock-minutes, it may be in violation of Requirement R1. To the extent that a BA's operation is supporting frequency, both CPS 1 and BAAL do not require corrective action. However, operations in support of Interconnection frequency also cannot be excessive, as any change in Interconnection frequency could render such action outside of limits. The proposed Reliability Standard incentivizes applicable entities to stay within these limits.

One of the reliability benefits of the proposed BAL-001-2 Reliability Standard is that it now contains real-time requirements necessary for proper control by allowing Balancing Authorities

to calculate their position within pre-established boundaries on a real-time basis. The Commission noted in Order No. 693 that "while the control performance standard metric is useful in identifying trends relating to poor regulating practices, specification of minimum reserve requirements to be maintained at all times would complement the control performance standard metrics by providing real-time requirements necessary for proper control."[7] The proposed Reliability Standard allows Balancing Authorities to calculate their position within pre-established boundaries on a real-time basis and take action to support reliability. Proposed Requirement R1 addresses long-term reliability and proposed Requirement R2 addresses short-term reliability. Collectively, the two Requirements of the proposed Reliability Standard define limits and significant deviations that impact frequency.

As noted herein, the BAL Reliability Standards work closely together. Revisions to the BAL-002 Reliability Standard are currently in development and will complement the proposed revisions to the BAL-001-2 Reliability Standard and will also address the Commission's concerns in Order No. 693 regarding the need to define reportable events.

B. Status of Field Trial for Proposed Reliability Standard BAL-001-2

As NERC noted in its Petition, the field trial for proposed Reliability Standard is ongoing.[8] The participation of Balancing Authorities in the field trial is in the interest of reliability due to the improvements proposed in Reliability Standard BAL-001-2, which requires a Balancing Authority to balance its resources and demand in real-time. There are significant costs for

---

[7] Order No. 693 at P 397.

[8] Petition at p. 6. In January 2013, the Western Electricity Coordinating Council presented a report on the field trial at its Board of Directors meeting. *Available at*: http://www.wecc.biz/committees/BOD/20130123/Lists/Minutes/1/2013%2001%2023%20Board%20Packet.pdf, beginning at p. 32. The report states that no trends were noticed in both NERC Inadvertent Interchange and the Primary Inadvertent Interchange accumulations for the participating BAs in the Western Interconnection during the field trial.

entities that are associated with changing between the currently-effective BAL-001-1 Reliability Standard and the proposed BAL-001-2 Reliability Standard because energy management system ("EMS") changes are required and there may also be associated information technology changes required. In some cases, operators may require training to implement these changes. The widespread participation of Balancing Authorities has provided insight into how the changes in proposed Reliability Standard BAL-001-2 will impact reliability. Currently, there are 47 Balancing Authorities participating in the field trial (16 in the Eastern Interconnection, 29 in the Western Interconnection, ERCOT and Quebec). For these reasons, NERC supports the participation of additional Balancing Authorities in the field trial. A report on the field trial will be submitted to the Commission in this proceeding for informational purposes, by no later than July 31, 2014. The field trial will end for participating entities upon the effective date of Reliability Standard BAL-001-2.

III. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[9]

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

Valerie Agnew
Director of Standards Development
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595 – facsimile
valerie.agnew@nerc.net

[9] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203 (2013), to allow the inclusion of more than two persons on the service list in this proceeding.

IV. CONCLUSION

NERC respectfully requests that the Commission consider the comments submitted herein.

Respectfully submitted,

/s/ Stacey Tyrewala

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

Counsel for the North American Electric Reliability Corporation

Date: May 9, 2014

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

May 15, 2014

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: Revisions to the Violation Risk Factors and Violation Severity Levels Assigned to Certain Critical Infrastructure Protection Reliability Standards
Docket No. RM13-5-000

Dear Secretary Bose:

In accordance with Order No. 791,[1] the North American Electric Reliability Corporation ("NERC") submits proposed revisions to certain Violation Risk Factors ("VRFs") and Violations Severity Levels ("VSLs") assigned to certain Critical Infrastructure Protection ("CIP") Reliability Standards for Federal Energy Regulatory Commission ("FERC" or "Commission") approval. Specifically, NERC proposes revisions to the VRFs assigned to:

- CIP-006-5, Requirement R3
- CIP-004-5.1, Requirement R4

NERC is also proposing revisions to the VSLs assigned to:

- CIP-003-5, Requirements R1 and R2
- CIP-004-5.1, Requirement R4
- CIP-008-5, Requirement R2
- CIP-009-5, Requirement R3

The proposed VRF and VSL revisions, provided in Attachment A hereto, are consistent with the Commission's directives in Order No. 791. NERC respectfully requests that the Commission approve the proposed VRF and VSL revisions as just, reasonable, not unduly discriminatory or preferential, and in the public interest.

[1] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

I. Background

In Order No. 791, FERC approved new and modified CIP Reliability Standards, referred to as the CIP version 5 Reliability Standards. Among other things, FERC directed NERC to file revisions to certain VRFs and VSLs assigned to certain CIP Reliability Standards.[2] In particular, FERC directed NERC to modify the VRF assignments for Reliability Standards CIP-006-5, Requirement R3 and CIP-004-5, Requirement R4 from Lower to Medium.[3] Additionally, the Commission directed "modification to the VSLs for certain CIP Reliability Standards to: (1) remove the "identify, assess, and correct" language from the text of the VSLs for the affected requirements; (2) address typographical errors; and (3) clarify certain unexplained elements."[4]

The Commission directed NERC to file the VRF revisions within 90 days of the effective date of Order No. 791.[5] The Commission did not set a timeframe for filing the VSL modifications. On March 19, 2014, the Commission granted NERC an extension of time until May 15, 2014 to file the VRF modifications.[6] The NERC Board of Trustees approved the proposed VRF and VSL revisions on May 7, 2014.

II. Notices and Communications

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

Holly A. Hawkins
Assistant General Counsel
Shamai Elstein
Counsel
North American Electric Reliability Corporation
1325 G St., NW, Suite 600
Washington, DC 20005
202-400-3000
holly.hawkins@nerc.net
shamai.elstein@nerc.net

III. Proposed VRF and VSL Revisions

Consistent with the Commission's directives in Order No. 791, NERC is proposing to modify (i) the VRFs for CIP-006-5, Requirement R3 and CIP-004-5.1, Requirement R4; and (ii) the VSLs for CIP-003-5,

---

2 Order No. 791 at PP 181-84, 192-196, 205-210.

3 *Id*. at PP 181-84, 192-196.

4 *Id*. at P 205-210.

5 *Id*. at PP 184, 196.

6 *Notice of Extension of Time*, Docket No. RM13-5-000 (March 19, 2014).

Requirements R1 and R2; CIP-004-5.1, Requirement R4; CIP-008-5, Requirement R2; and CIP-009-5, Requirement R3. The following is a discussion of each of the proposed VRF and VSL Revisions.

With respect to the directive to modify the VSLs associated with the requirements that include the "identify, assess, and correct" language, NERC will submit such modifications when it modifies those requirements consistent with FERC's directive from Order No. 791 to remove or modify that language. There is a NERC standards development project, Project 2014-02 CIP Version 5 Revisions, underway to address the Commission directives from Order No. 791.

a. VSL for CIP-003-5, Requirements R1, R2 and R4

Reliability Standard CIP-003-5 addresses security management controls for cyber security. Requirement R1 of that standard governs management approval of policies on topics addressed in other CIP standards for medium and high impact BES Cyber Systems. Requirement R2 governs policies for low impact BES Cyber Systems. Consistent with the Commission directive,[7] proposes to revise the VSLs in CIP-003-5, Requirements R1 and R2 to eliminate redundant language.

The Commission also directed NERC to clarify that the VSLs assigned to Requirement R4 of CIP-003-5 include timeline gradations as set forth in the VSL contained in Exhibit A to the petition for approval of the CIP version 5 Reliability Standards.[8] NERC hereby clarifies that VSLs for CIP-003-5, Requirement R4 include the timeline gradations reflected in Exhibit A to the CIP version 5 petition and as reflected in Attachment A hereto.

b. VRF and VSL for CIP-004-5.1, Requirement R4

Reliability Standard CIP-004-5.1 addresses cyber security personnel and training requirements, and Requirement R4 of that standard obligates a responsible entity to have a process for authorizing access to BES Cyber System Information, including periodic verification that users and accounts are authorized and necessary. Consistent with the Commission's directive,[9] NERC proposes to revise the VRF for CIP-004-5.1, Requirement R4 from a "Lower" designation to a "Medium" designation. Additionally, NERC proposes to revise the VSL assignment for CIP-004-5.1, Requirement R4 to a percentage-based gradation consistent with the Commission's directive.[10]

c. VRF for CIP-006-5, Requirement R3

Reliability Standard CIP-006-5 addresses physical security of BES Cyber Systems, and Requirement R3 of that standard governs implementation of Physical Access Control System maintenance

7 Order No. 791 at P 206.

8 *Id*. at P 207.

9 *Id*. at PP 192-196.

10 *Id*. at P 208.

and testing programs. Consistent with the Commission's directive,[11] NERC proposes to revise the VRF for CIP-006-5, Requirement R3 from a "Lower" designation to a "Medium" designation.

d. VSL for CIP-008-5, Requirement R2

Reliability Standard CIP-008-5 addresses incident reporting and response planning for cyber security. Requirement R2 of that standard governs implementation of documented Cyber Security Incident response plans. Consistent with the Commission's directive,[12] NERC proposed to revise the severe VSL to reduce a gap in months between the high VSL and severe VSL.

e. CIP-009-5, Requirement R3

Reliability Standard CIP-009-5 addresses recovery plans for BES Cyber Systems. Requirement R3 of that standard governs maintenance of the recovery plans. Consistent with the Commission's directive,[13] NERC proposed to revise the timeframes contained in the VSLs from 90-210 days to 90-120 days, where appropriate.

IV. Conclusion

For the foregoing reasons, NERC respectfully requests that the Commission approve the proposed VRF and VSL revisions as just, reasonable, not unduly discriminatory or preferential, and in the public interest.

Respectfully submitted,

/S. Shamai Elstein

Holly A. Hawkins
Assistant General Counsel
Shamai Elstein
Counsel
North American Electric Reliability Corporation
1325 G St., NW, Suite 600
Washington, DC 20005
202-400-3000
holly.hawkins@nerc.net
shamai.elstein@nerc.net

[11] *Id*. at PP 181-184.

[12] *Id*. at P 209.

[13] *Id*. at P 210.

Attachment A

CIP-003-5 Violation Risk Factor and Violation Severity Level Revisions

Clean and Redline

Clean

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects

are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- **2.1** Cyber security awareness;
- **2.2** Physical security controls;
- **2.3** Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
- **2.4** Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate within 18 calendar months of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies.	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one	required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager within 17 calendar months but did complete this approval	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	in less than or equal to 18 calendar months of the previous approval. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			40 calendar days of the change. (R3)	50 calendar days of the change. (R3)		changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and has Identified deficiencies but did not assess or correct the deficiencies.(R4) OR The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not identify, assess, or correct the deficiencies.(R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

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

Rationale for R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5. (Order becomes effective 2/3/14.)	
5	5/7/14	Adopted by the NERC Board of Trustees to modify VSLs for Requirements R1 and R2.	

Redline

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects

are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- **2.1** Cyber security awareness;
- **2.2** Physical security controls;
- **2.3** Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
- **2.4** Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate ~~according to Requirement R1~~ within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate ~~according to Requirement R1~~ within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate ~~according to Requirement R1~~ within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate ~~according to Requirement R1~~ within 18 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1)	the previous approval. (R1)		months of the previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify,	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its	the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its	assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager ~~according to~~	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager ~~according to Requirement R2~~ within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	~~Requirement R2~~ within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change in less than 40 calendar days of the change. (R3)	document this change in less than 50 calendar days of the change. (R3)	less than 60 calendar days of the change. (R3)	by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and has Identified deficiencies but did not assess or correct the deficiencies.(R4) OR The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					process to delegate actions from the CIP Senior Manager, but did not identify, assess, or correct the deficiencies.(R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

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

Rationale for R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5. (Order becomes effective 2/3/14.)	

CIP-004-5.1 Violation Risk Factor and Violation Severity Level Revisions

Clean and Redline

Clean

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-5.1

3. Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-5.1:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-004-5.1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-004-5.1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-004-5.1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of

implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5.1 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-5.1 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-5.1 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5.1 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-5.1 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized	and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date, and did not identify, assess and correct the deficiencies. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted	correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter, and did not identify, assess and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	Information is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Information is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)			were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted	physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4) OR The Responsible Entity has implemented	physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances, and did not identify, assess, and correct the deficiencies. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include

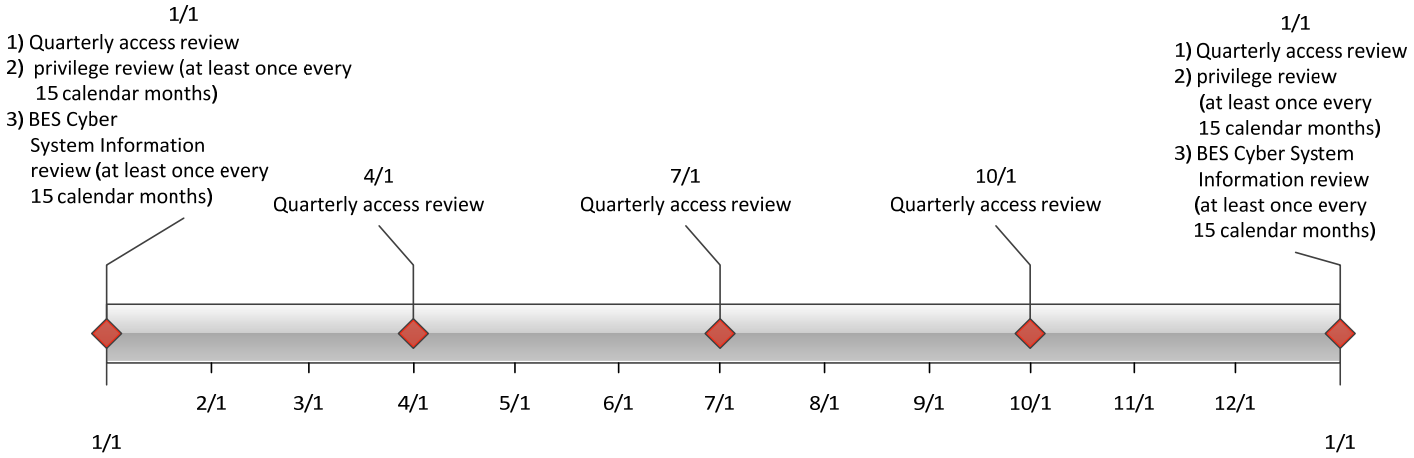
individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function



(i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.

Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

Reference to prior version: (Part 1.1) CIP-004-4, R1

Change Rationale: (Part 1.1)

Changed to remove the need to ensure or prove everyone with authorized electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that security awareness has been reinforced.*

Moved example mechanisms to guidance.

Rationale for R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:
    - The visitor control program
    - Electronic interconnectivity supporting the operation and control of BES Cyber Systems
    - Storage media as part of the handling of BES Cyber Systems information

2. Change references from Critical Cyber Assets to BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP004-4, R2.2.1

Change Rationale: (Part 2.1)

Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was

focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.

Reference to prior version: (Part 2.2) CIP004-4, R2.1

Change Rationale: (Part 2.2)

Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.

Reference to prior version: (Part 2.3) CIP004-4, R2.3

Change Rationale: (Part 2.3)

Updated to replace "annually" with "once every 15 calendar months."

Rationale for R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

Reference to prior version: (Part 3.1) CIP004-4, R3.1

Change Rationale: (Part 3.1)

Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.

Reference to prior version: (Part 3.2) CIP004-4, R3.1

Change Rationale: (Part 3.2)

Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added

additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.

Reference to prior version: (Part 3.3) New

Change Rationale: (Part 3.3)

There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.

Reference to prior version: (Part 3.4) CIP-004-4, R3.3

Change Rationale: (Part 3.4)

Separated into its own table item.

Reference to prior version: (Part 3.5) CIP-004-3, R3, R3.3

Change Rationale: (Part 3.5)

Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment. CIP-004-3, R3, R3.3

Rationale for R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account

databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

Reference to prior version: (Part 4.1) CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1

Change Rationale: (Part 4.1)

Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*

Reference to prior version: (Part 4.2) CIP 004-4, R4.1

Change Rationale: (Part 4.2)

Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

Reference to prior version: (Part 4.3) CIP 007-4, R5.1.3

Change Rationale: (Part 4.3)

Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.

Reference to prior version: (Part 4.4) CIP-003-4, R5.1.2

Change Rationale: (Part 4.4)

Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to

confirm access privileges are correct and the minimum necessary for performing assigned work functions.

Rationale for R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."

Reference to prior version: (Part 5.1) CIP 004-4, R4.2

Change Rationale: (Part 5.1)

The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards ***to require immediate revocation*** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*

Reference to prior version: (Part 5.2) CIP-004-4, R4.2

Change Rationale: (Part 5.2)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Reference to prior version: (Part 5.3) New

Change Rationale: (Part 5.3)

FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.

Reference to prior version: (Part 5.4) New

Change Rationale: (Part 5.4)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

Reference to prior version: (Part 5.5) CIP-007-4, R5.2.3

Change Rationale: (Part 5.5)

To provide clarification of expected actions in managing the passwords.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Modified two VSLs in R4.	Errata
5.1	11/22/13	FERC Order issued approving CIP-004-5.1. (Order becomes effective on 2/3/14.)	

5.1	5/7/14	Adopted by the NERC Board of Trustees to modify the VRF and VSLs for Requirement R4.	

Redline

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-5.1

3. Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-5.1:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-004-5.1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-004-5.1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-004-5.1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of

implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5.1 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-5.1 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-5.1 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5.1 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-5.1 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-5.1 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R4 – Access Management Program. [Violation Risk Factor: ~~Lower~~Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-5.1 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-5.1 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-5.1 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized	and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date, and did not identify, assess and correct the deficiencies. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted	correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	~~Lower~~Medium	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter, and did not identify, assess and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for ~~two~~ more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for ~~three~~ more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for	BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for ~~one~~ 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	Information is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its~~two~~ BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for ~~three~~ more than 10% but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for ~~four or more~~more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for ~~four or more~~more than 15% of its BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Information is correct and necessary within 15 calendar months of the previous verification but for ~~one~~ 5% or less of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)			Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted	physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4) OR The Responsible Entity has implemented	physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5.1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			circumstances, and did not identify, assess, and correct the deficiencies. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include

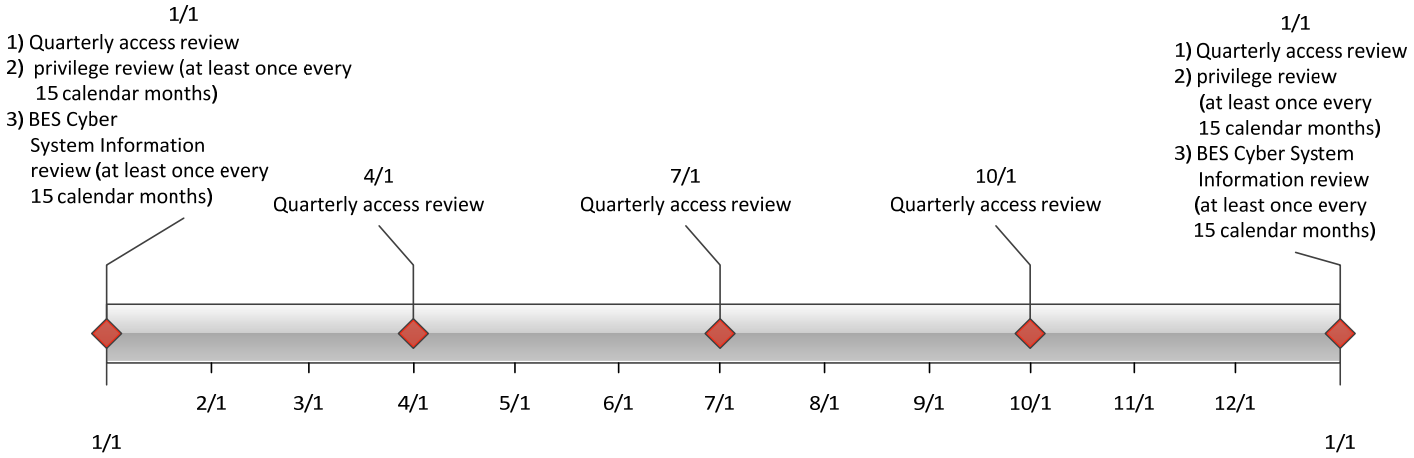
individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function



(i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.

Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

Reference to prior version: (Part 1.1) CIP-004-4, R1

Change Rationale: (Part 1.1)

Changed to remove the need to ensure or prove everyone with authorized electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that security awareness has been reinforced.*

Moved example mechanisms to guidance.

Rationale for R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:
    - The visitor control program
    - Electronic interconnectivity supporting the operation and control of BES Cyber Systems
    - Storage media as part of the handling of BES Cyber Systems information

2. Change references from Critical Cyber Assets to BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP004-4, R2.2.1

Change Rationale: (Part 2.1)

Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was

focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.

Reference to prior version: (Part 2.2) CIP004-4, R2.1

Change Rationale: (Part 2.2)

Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.

Reference to prior version: (Part 2.3) CIP004-4, R2.3

Change Rationale: (Part 2.3)

Updated to replace "annually" with "once every 15 calendar months."

Rationale for R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

Reference to prior version: (Part 3.1) CIP004-4, R3.1

Change Rationale: (Part 3.1)

Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.

Reference to prior version: (Part 3.2) CIP004-4, R3.1

Change Rationale: (Part 3.2)

Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added

additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.

Reference to prior version: (Part 3.3) New

Change Rationale: (Part 3.3)

There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.

Reference to prior version: (Part 3.4) CIP-004-4, R3.3

Change Rationale: (Part 3.4)

Separated into its own table item.

Reference to prior version: (Part 3.5) CIP-004-3, R3, R3.3

Change Rationale: (Part 3.5)

Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment. CIP-004-3, R3, R3.3

Rationale for R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. “Authorization” should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. “Provisioning” should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity’s policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account

databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

Reference to prior version: (Part 4.1) CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1

Change Rationale: (Part 4.1)

Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*

Reference to prior version: (Part 4.2) CIP 004-4, R4.1

Change Rationale: (Part 4.2)

Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

Reference to prior version: (Part 4.3) CIP 007-4, R5.1.3

Change Rationale: (Part 4.3)

Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.

Reference to prior version: (Part 4.4) CIP-003-4, R5.1.2

Change Rationale: (Part 4.4)

Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to

confirm access privileges are correct and the minimum necessary for performing assigned work functions.

Rationale for R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."

Reference to prior version: (Part 5.1) CIP 004-4, R4.2

Change Rationale: (Part 5.1)

The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards ***to require immediate revocation*** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*

Reference to prior version: (Part 5.2) CIP-004-4, R4.2

Change Rationale: (Part 5.2)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Reference to prior version: (Part 5.3) New

Change Rationale: (Part 5.3)

FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.

Reference to prior version: (Part 5.4) New

Change Rationale: (Part 5.4)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

Reference to prior version: (Part 5.5) CIP-007-4, R5.2.3

Change Rationale: (Part 5.5)

To provide clarification of expected actions in managing the passwords.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Modified two VSLs in R4.	Errata
5.1	11/22/13	FERC Order issued approving CIP-004-5.1. (Order becomes effective on 2/3/14.)	

CIP-006-5 Violation Risk Factor and Violation Severity Level Revisions

Clean and Redline

Clean

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-5

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The

documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management

Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR The Responsible Entity has a	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel and	The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5) OR The Responsible Entity	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access but did not identify,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified	identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the	assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has documented and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)		deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)	implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Perimeter. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Access Control Systems or to communicate such alerts within 15 minutes to identified personnel (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9)
R2	**Same-Day Operations**	**Medium**	N/A	The Responsible Entity included a visitor control program that requires logging of each	The Responsible Entity included a visitor control program that requires continuous	The Responsible Entity has failed to include or implement a visitor control program that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program to retain visitor logs for at	escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		
R3	**Long Term Planning**	**Medium**	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but	The Responsible Entity has not documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	did complete required testing within 26 calendar months. (3.1)	did complete required testing within 27 calendar months. (3.1)	has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. *Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.*

Summary of Changes: The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

Reference to prior version: (Part 1.1) *CIP-006-4c, R2.1 for Physical Access Control Systems New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*

Change Rationale: (Part 1.1)

To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.

Reference to prior version: (Part 1.2) CIP006-4c, R3 & R4
Change Rationale: (Part 1.2)

This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.3) CIP006-4c, R3 & R4

Change Rationale: (Part 1.3)

The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.

Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.
FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).

Reference to prior version: (Part 1.4) CIP006-4c, R5

Change Rationale: (Part 1.4)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.5) CIP006-4c, R5

Change Rationale: (Part 1.5)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.6) CIP006-4c, R5

Change Rationale: (Part 1.6)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.7) CIP006-4c, R5

Change Rationale: (Part 1.7)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.8) CIP-006-4c, R6

Change Rationale: (Part 1.8)

CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.

Examples of logging methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.9) CIP-006-4c, R7

Change Rationale: (Part 1.9)

No change.

Rationale for R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

Reference to prior version: (Part 2.1) CIP-006-4c, R1.6.2

Change Rationale: (Part 2.1)

Added the ability to not do this during CIP Exceptional Circumstances.

Reference to prior version: (Part 2.2) CIP-006-4c R1.6.1

Change Rationale: (Part 2.2)

Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.

Reference to prior version: (Part 2.3) CIP-006-4c, R7

Change Rationale: (Part 2.3)

No change

Rationale for R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

Reference to prior version: (Part 3.1) CIP-006-4c, R8.1 and R8.2

Change Rationale: (Part 3.1)

Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5	11/22/13	FERC Order issued approving CIP-006-5. (Order becomes effective on 2/3/14.)	
5	5/7/14	Adopted by the NERC Board of Trustees to modify the VRF for Requirement R3.	

Redline

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-5

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The

documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management

Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: ~~Lower~~Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR The Responsible Entity has a	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel and	The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5) OR The Responsible Entity	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access but did not identify,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified	identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the	assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has documented and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)		deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)	implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Perimeter. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Access Control Systems or to communicate such alerts within 15 minutes to identified personnel (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9)
R2	**Same-Day Operations**	**Medium**	N/A	The Responsible Entity included a visitor control program that requires logging of each	The Responsible Entity included a visitor control program that requires continuous	The Responsible Entity has failed to include or implement a visitor control program that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program to retain visitor logs for at	escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		
R3	**Long Term Planning**	~~Lower~~Medium	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but	The Responsible Entity has not documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	did complete required testing within 26 calendar months. (3.1)	did complete required testing within 27 calendar months. (3.1)	has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. *Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.*

Summary of Changes: The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

Reference to prior version: (Part 1.1) *CIP-006-4c, R2.1 for Physical Access Control Systems New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*

Change Rationale: (Part 1.1)

To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.

Reference to prior version: (Part 1.2) CIP006-4c, R3 & R4
Change Rationale: (Part 1.2)

This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.3) CIP006-4c, R3 & R4

Change Rationale: (Part 1.3)

The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.

Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.
FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).

Reference to prior version: (Part 1.4) CIP006-4c, R5

Change Rationale: (Part 1.4)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.5) CIP006-4c, R5

Change Rationale: (Part 1.5)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.6) CIP006-4c, R5

Change Rationale: (Part 1.6)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.7) CIP006-4c, R5

Change Rationale: (Part 1.7)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.8) CIP-006-4c, R6

Change Rationale: (Part 1.8)

CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.

Examples of logging methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.9) CIP-006-4c, R7

Change Rationale: (Part 1.9)

No change.

Rationale for R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

Reference to prior version: (Part 2.1) CIP-006-4c, R1.6.2

Change Rationale: (Part 2.1)

Added the ability to not do this during CIP Exceptional Circumstances.

Reference to prior version: (Part 2.2) CIP-006-4c R1.6.1

Change Rationale: (Part 2.2)

Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.

Reference to prior version: (Part 2.3) CIP-006-4c, R7

Change Rationale: (Part 2.3)

No change

Rationale for R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

Reference to prior version: (Part 3.1) CIP-006-4c, R8.1 and R8.2

Change Rationale: (Part 3.1)

Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5	11/22/13	FERC Order issued approving CIP-006-5. (Order becomes effective on 2/3/14.)	

CIP-008-5 Violation Risk Factor and Violation Severity Level Revisions

Clean and Redline

Clean

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident.*

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with	The Responsible Entity has not updated the	The Responsible Entity has neither	The Responsible Entity has neither

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR	documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the	documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response

activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

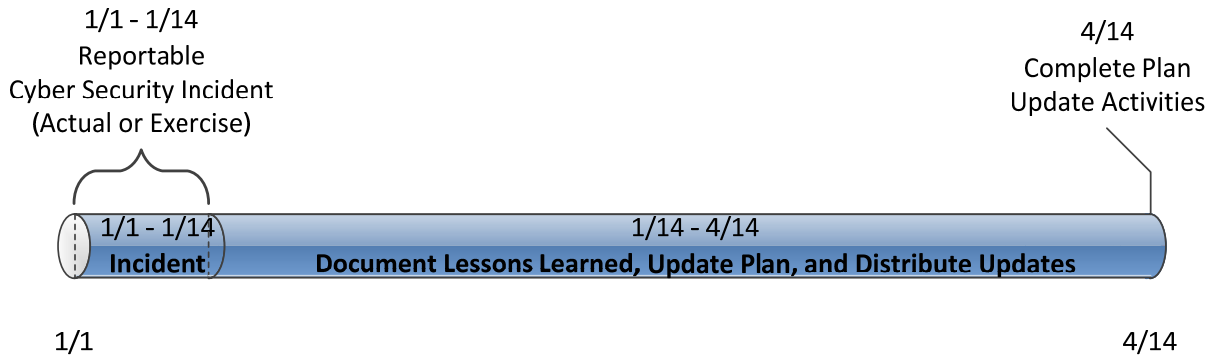


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

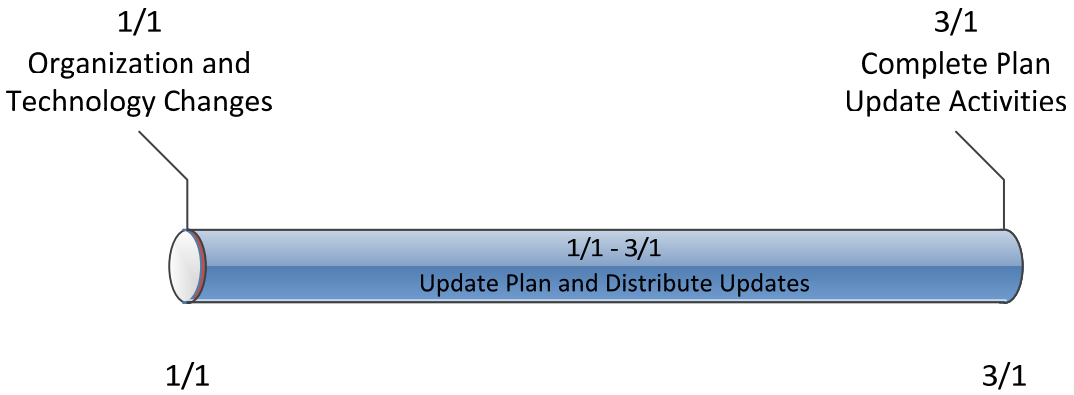


Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the

plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	

4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5. (Order becomes effective on 2/3/14.)	
5	5/7/14	Adopted by the NERC Board of Trustees to modify the VSL for Requirement R2.	

Redline

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident.*

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within ~~19~~ 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with	The Responsible Entity has not updated the	The Responsible Entity has neither	The Responsible Entity has neither

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR	documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the	documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response

activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

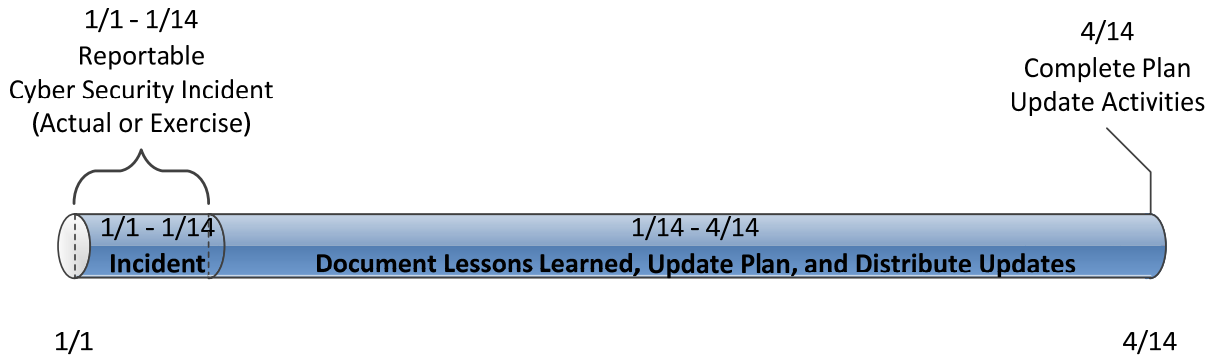


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

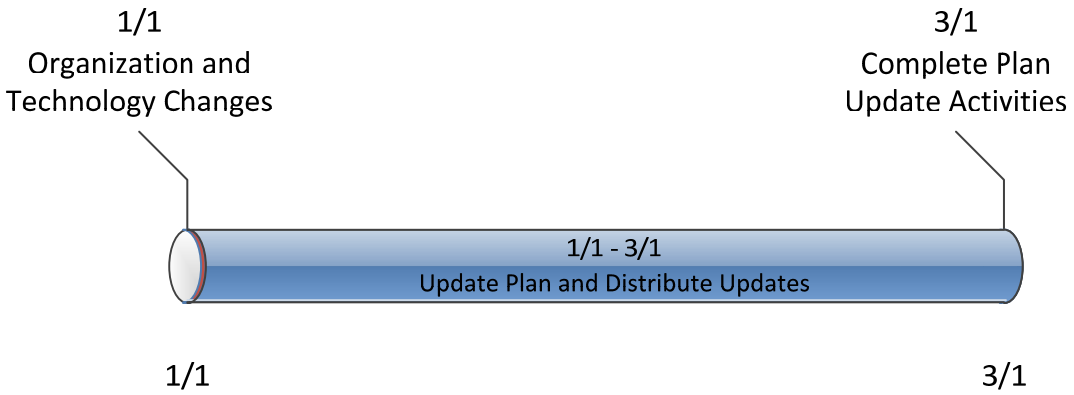


Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the

plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	

4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5. (Order becomes effective on 2/3/14.)	

CIP-009-5 Violation Risk Factor and Violation Severity Level Revisions

Clean and Redline

Clean

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-5

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The

documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, and	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Technology changes.	• Responders, or Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1~~Figure 1~~, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

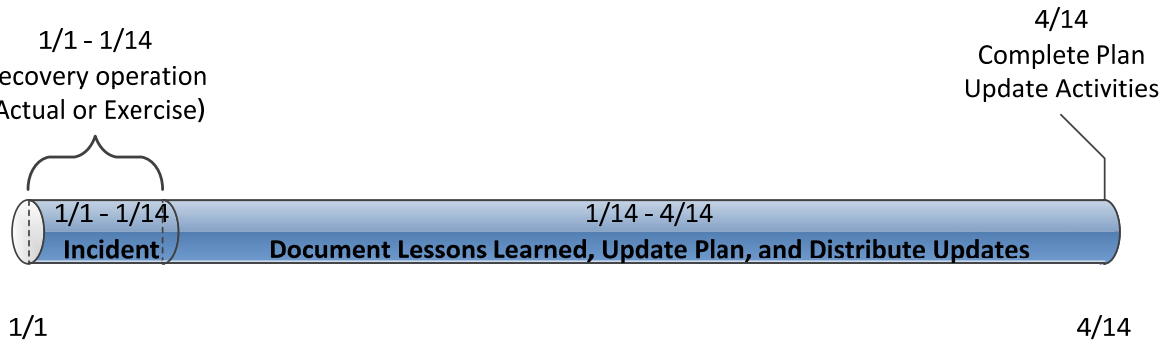


Figure 1: CIP-009-5 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2~~Figure 2~~, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

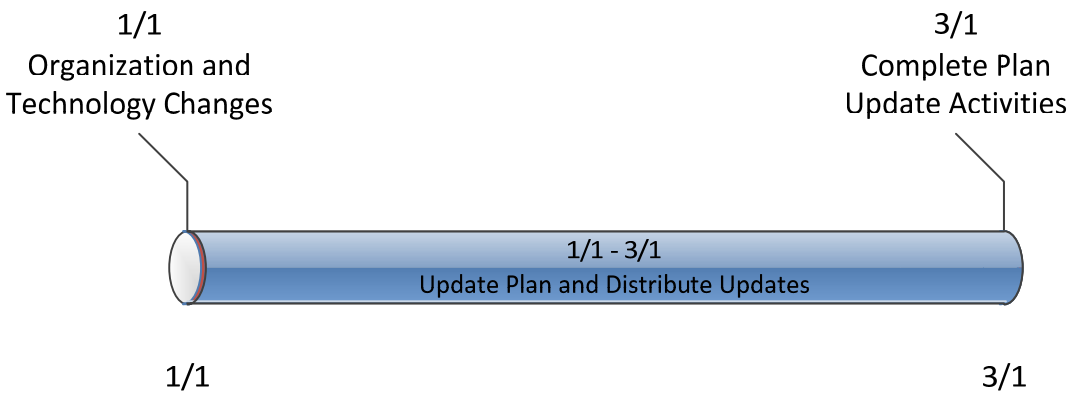


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

Reference to prior version: (Part 1.1) CIP-009, R1.1

Change Description and Justification: (Part 1.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.2) CIP-009, R1.2

Change Description and Justification: (Part 1.2)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.3) CIP-009, R4

Change Description and Justification: (Part 1.3)

Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.

Reference to prior version: (Part 1.4) New Requirement

Change Description and Justification: (Part 1.4)

Addresses FERC Order Section 739 and 748.

Reference to prior version: (Part 1.5) New Requirement

Change Description and Justification: (Part 1.5)

Added requirement to address FERC Order No. 706, Paragraph 706.

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP-009, R2

Change Description and Justification: (Part 2.1)

Minor wording change; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-009, R5

Change Description and Justification: (Part 2.2)

Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.

Reference to prior version: (Part 2.3) CIP-009, R2

Change Description and Justification: (Part 2.3)

Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.

Rationale for R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

Reference to prior version: (Part 3.1) CIP-009, R1 and R3

Change Description and Justification: (Part 3.1)

Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.

Reference to prior version: (Part 3.2) New Requirement

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5. (Order becomes effective on 2/3/14.)	
5	5/7/14	Adopted by the NERC Board of Trustees to modify VSLs for Requirement R3.	

Redline

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-5

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The

documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, and	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than ~~210~~ 120 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than ~~210~~ 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than ~~210~~ 120 calendar days of each recovery plan test or actual recovery. (3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within ~~210~~ 120 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Technology changes.	• Responders, or Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1~~Figure 1~~, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

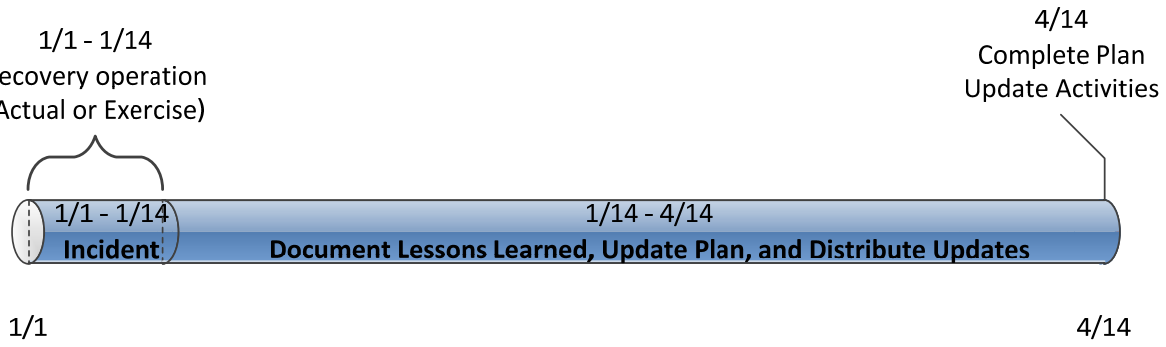


Figure 1: CIP-009-5 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2~~Figure 2~~, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

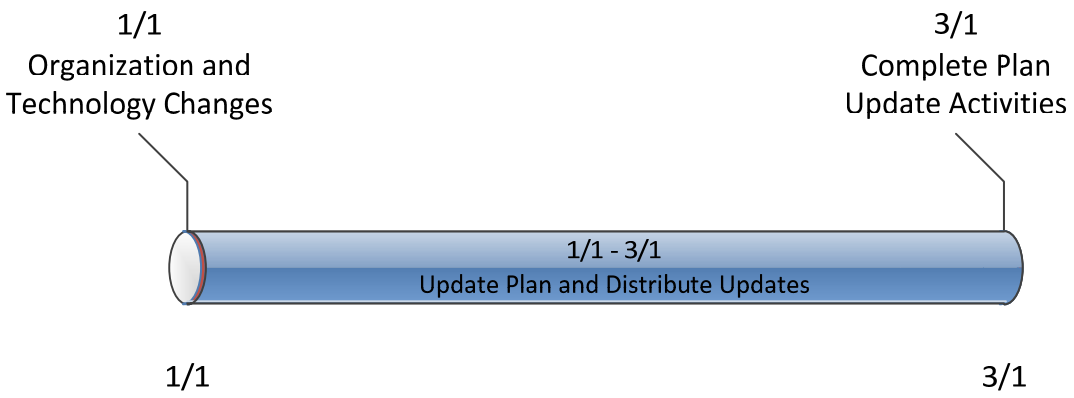


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

Reference to prior version: (Part 1.1) CIP-009, R1.1

Change Description and Justification: (Part 1.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.2) CIP-009, R1.2

Change Description and Justification: (Part 1.2)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.3) CIP-009, R4

Change Description and Justification: (Part 1.3)

Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.

Reference to prior version: (Part 1.4) New Requirement

Change Description and Justification: (Part 1.4)

Addresses FERC Order Section 739 and 748.

Reference to prior version: (Part 1.5) New Requirement

Change Description and Justification: (Part 1.5)

Added requirement to address FERC Order No. 706, Paragraph 706.

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP-009, R2

Change Description and Justification: (Part 2.1)

Minor wording change; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-009, R5

Change Description and Justification: (Part 2.2)

Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.

Reference to prior version: (Part 2.3) CIP-009, R2

Change Description and Justification: (Part 2.3)

Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.

Rationale for R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

Reference to prior version: (Part 3.1) CIP-009, R1 and R3

Change Description and Justification: (Part 3.1)

Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.

Reference to prior version: (Part 3.2) New Requirement

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5. (Order becomes effective on 2/3/14.)	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

June 4, 2014

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: Revisions to a Violation Severity Level Assigned to Protection System Maintenance Reliability Standards
Docket Nos. RM13-7-000 and RM14-8-000

Dear Secretary Bose:

In accordance with Order No. 793,[1] the North American Electric Reliability Corporation ("NERC") submits a proposed revision to a Violation Severity Level ("VSL") assigned to Requirement R1 in Protection System Maintenance ("PRC") Reliability Standard PRC-005-2 for Federal Energy Regulatory Commission ("Commission") approval. NERC has also made the same change to proposed Reliability Standard PRC-005-3, which has been adopted by the NERC Board of Trustees[2] and since filed for Commission approval.[3]

The proposed VSL revision to PRC-005-2, provided in Attachment A hereto, is consistent with the Commission's directive in Order No. 793. Attachment B includes a replacement "Exhibit A" to NERC's PRC-005-3 Petition that reflects the same VSL change in the proposed PRC-005-3 Reliability Standard (included as PRC-005-3.1 to reflect an errata change made).[4]

As background, on December 19, 2013, the Commission issued Order No. 793, approving Reliability Standard PRC-005-2 – Protection System Maintenance, stating that the "Reliability Standard contains overall improvements over the four existing Reliability Standards." However, the Commission

---

1 *Protection System Maintenance Reliability Standard*, Order No. 793, 145 FERC ¶ 61,253 (2013).

2 The agenda for the May 7, 2014 Board of Trustees meeting is available at http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/board_agenda_package_May_2014.pdf

3 On February 14, 2014, NERC submitted a petition for approval of proposed Reliability Standard PRC-005-3 (Protection System Maintenance). The Commission assigned the petition to Docket No. RM14-8-000. ("PRC-005-3 Petition")

4 This replacement exhibit is the same replacement exhibit included with an errata filing to NERC's Petition for approval of proposed Reliability Standard PRC-005-3, which has been separately filed in RM14-8-000.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

directed one change to the VSL assignment in Requirement R1 regarding the failure to include station batteries in a time-based maintenance program, noting that "the level of risk associated with the failure to test a given batter is not an appropriate consideration in the context of assigning violation severity levels, but rather, should be considered when assigning a violation risk factor." The Commission, therefore, directed NERC to submit a compliance filing changing the VSL for the failure to include station batteries in a time-based maintenance program to "severe."

NERC respectfully requests that the Commission approve the proposed VSL revision as just, reasonable, not unduly discriminatory or preferential, and in the public interest for PRC-005-2 and incorporate the replacement Exhibit A to the PRC-005-3 Petition in its rulemaking in RM14-8-000.

Respectfully submitted,

/s/ William H. Edwards
William H. Edwards
Counsel
North American Electric Reliability Corporation
1325 G St., NW, Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
william.edwards@nerc.net

cc: Official service lists in Docket Nos. RM13-7-000 and RM14-8-000.

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 4th day of June, 2014.

/s/ William H. Edwards

William H. Edwards
Counsel for North American
Electric Reliability Corporation

Exhibit A

PRC-005-2 Clean and Redline VSL Revisions

A. Introduction

1. Title: **Protection System Maintenance**

2. Number: PRC-005-2

3. Purpose: To document and implement programs for the maintenance of all Protection Systems affecting the reliability of the Bulk Electric System (BES) so that these Protection Systems are kept in working order.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner

4.1.2 Generator Owner

4.1.3 Distribution Provider

4.2. Facilities:

4.2.1 Protection Systems that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)

4.2.2 Protection Systems used for underfrequency load-shedding systems installed per ERO underfrequency load-shedding requirements.

4.2.3 Protection Systems used for undervoltage load-shedding systems installed to prevent system voltage collapse or voltage instability for BES reliability.

4.2.4 Protection Systems installed as a Special Protection System (SPS) for BES reliability.

4.2.5 Protection Systems for generator Facilities that are part of the BES, including:

4.2.5.1 Protection Systems that act to trip the generator either directly or via lockout or auxiliary tripping relays.

4.2.5.2 Protection Systems for generator step-up transformers for generators that are part of the BES.

4.2.5.3 Protection Systems for transformers connecting aggregated generation, where the aggregated generation is part of the BES (e.g., transformers connecting facilities such as wind-farms to the BES).

4.2.5.4 Protection Systems for station service or excitation transformers connected to the generator bus of generators which are part of the BES, that act to trip the generator either directly or via lockout or tripping auxiliary relays.

5. Effective Date: See Implementation Plan

6. Definitions Used in this Standard: The following terms are defined for use only within PRC-005-2, and should remain with the standard upon approval rather than being moved to the Glossary of Terms.

Unresolved Maintenance Issue – A deficiency identified during a maintenance activity that causes the component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up corrective action.

Segment – Protection Systems or components of a consistent design standard, or a particular model or type from a single manufacturer that typically share other common elements. Consistent performance is expected across the entire population of a Segment. A Segment must contain at least sixty (60) individual components.

Component Type - Any one of the five specific elements of the Protection System definition.

Component – A Component is any individual discrete piece of equipment included in a Protection System, including but not limited to a protective relay or current sensing device. The designation of what constitutes a control circuit Component is dependent upon how an entity performs and tracks the testing of the control circuitry. Some entities test their control circuits on a breaker basis whereas others test their circuitry on a local zone of protection basis. Thus, entities are allowed the latitude to designate their own definitions of control circuit Components. Another example of where the entity has some discretion on determining what constitutes a single Component is the voltage and current sensing devices, where the entity may choose either to designate a full three-phase set of such devices or a single device as a single Component.

Countable Event – A failure of a Component requiring repair or replacement, any condition discovered during the maintenance activities in Tables 1-1 through 1-5 and Table 3 which requires corrective action or a Misoperation attributed to hardware failure or calibration failure. Misoperations due to product design errors, software errors, relay settings different from specified settings, Protection System Component configuration errors, or Protection System application errors are not included in Countable Events.

B. Requirements

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a Protection System Maintenance Program (PSMP) for its Protection Systems identified in Section 4.2. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

The PSMP shall:

1.1. Identify which maintenance method (time-based, performance-based per PRC-005 Attachment A, or a combination) is used to address each Protection System Component Type. All batteries associated with the station dc supply Component Type of a Protection System shall be included in a time-based program as described in Table 1-4 and Table 3.

1.2. Include the applicable monitored Component attributes applied to each Protection System Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, and Table 3 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System Components.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals in its PSMP shall follow the procedure established in PRC-005 Attachment A to establish and maintain its performance-based intervals. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall maintain its Protection System Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall implement and follow its PSMP for its Protection System Components that are included within the performance-based program(s). *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R5. Each Transmission Owner, Generator Owner, and Distribution Provider shall demonstrate efforts to correct identified Unresolved Maintenance Issues. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

C. Measures

M1. Each Transmission Owner, Generator Owner and Distribution Provider shall have a documented Protection System Maintenance Program in accordance with Requirement R1.

For each Protection System Component Type, the documentation shall include the type of maintenance method applied (time-based, performance-based, or a combination of these maintenance methods), and shall include all batteries associated with the station dc supply Component Types in a time-based program as described in Table 1-4 and Table 3. (Part 1.1)

For Component Types that use monitoring to extend the maintenance intervals, the responsible entity(s) shall have evidence for each protection Component Type (such as manufacturer's specifications or engineering drawings) of the appropriate monitored Component attributes as specified in Tables 1-1 through 1-5, Table 2, and Table 3. (Part 1.2)

M2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals shall have evidence that its current performance-based maintenance program(s) is in accordance with Requirement R2, which may include but is not limited to Component lists, dated maintenance records, and dated analysis records and results.

M3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System Components included within its time-based program in accordance with Requirement R3. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance intervals in accordance with Requirement R2 shall have evidence that it has implemented the Protection System Maintenance Program for the Protection System Components included in its performance-based program in accordance with Requirement R4. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence that it has undertaken efforts to correct identified Unresolved Maintenance Issues in accordance with Requirement R5. The evidence may include but is not limited to work orders, replacement Component orders, invoices, project schedules with completed milestones, return material authorizations (RMAs) or purchase orders.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity

1.2. Compliance Monitoring and Enforcement Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.3. Evidence Retention

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

The Transmission Owner, Generator Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

For Requirement R1, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep its current dated Protection System Maintenance Program, as well as any superseded versions since the preceding compliance audit, including the documentation that specifies the type of maintenance program applied for each Protection System Component Type.

For Requirement R2, Requirement R3, Requirement R4, and Requirement R5, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the two most recent performances of each distinct maintenance activity for the Protection System Component, or all performances of each distinct maintenance activity for the Protection System Component since the previous scheduled audit date, whichever is longer.

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

1.4. Additional Compliance Information

None.

2. Violation Severity Levels

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The responsible entity's PSMP failed to specify whether one Component Type is being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1)	The responsible entity's PSMP failed to specify whether two Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1)	The responsible entity's PSMP failed to include the applicable monitoring attributes applied to each Protection System Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, and Table 3 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System Components. (Part 1.2).	The responsible entity failed to establish a PSMP. OR The responsible entity failed to specify whether three or more Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1). OR The responsible entity's PSMP failed to include applicable station batteries in a time-based program. (Part 1.1)
R2	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within three years.	NA	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within four years.	The responsible entity uses performance-based maintenance intervals in its PSMP but: 1) Failed to establish the technical justification described within Requirement R2 for the initial use of the performance-based PSMP OR 2) Failed to reduce Countable Events to no more than 4% within five years OR 3) Maintained a Segment with less than 60 Components OR

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
				4) Failed to: • Annually update the list of Components, OR • Annually perform maintenance on the greater of 5% of the segment population or 3 Components, OR • Annually analyze the program activities and results for each Segment.
R3	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain 5% or less of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain more than 15% of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.
R4	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain 5% or less of the annual scheduled maintenance for a specific Protection System Component Type in accordance with their performance-based PSMP.	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the annual scheduled maintenance for a specific Protection System Component Type in accordance	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the annual scheduled maintenance for a specific Protection System Component Type in accordance with their performance-based PSMP.	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 15% of the annual scheduled maintenance for a specific Protection System Component Type in accordance

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
		with their performance-based PSMP.		with their performance-based PSMP.
R5	The responsible entity failed to undertake efforts to correct 5 or fewer identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 5, but less than or equal to 10 identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 10, but less than or equal to 15 identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 15 identified Unresolved Maintenance Issues.

E. Regional Variances

None

F. Supplemental Reference Document

The following documents present a detailed discussion about determination of maintenance intervals and other useful information regarding establishment of a maintenance program.

1. PRC-005-2 Protection System Maintenance Supplementary Reference and FAQ — July 2012.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. 3. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/05
1a	February 17, 2011	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers	Project 2009-17 interpretation
1a	February 17, 2011	Adopted by Board of Trustees	
1a	September 26, 2011	FERC Order issued approving interpretation of R1 and R2 (FERC's Order is effective as of September 26, 2011)	
1.1a	February 1, 2012	Errata change: Clarified inclusion of generator interconnection Facility in Generator Owner's responsibility	Revision under Project 2010-07
1b	February 3, 2012	FERC Order issued approving interpretation of R1, R1.1, and R1.2 (FERC's Order dated March 14, 2012). Updated version from 1a to 1b.	Project 2009-10 Interpretation
1.1b	April 23, 2012	Updated standard version to 1.1b to reflect FERC approval of PRC-005-1b.	Revision under Project 2010-07

1.1b	May 9, 2012	PRC-005-1.1b was adopted by the Board of Trustees as part of Project 2010-07 (GOTO).	
2	November 7, 2012	Adopted by Board of Trustees	Complete revision, absorbing maintenance requirements from PRC-005-1b, PRC-008-0, PRC-011-0, PRC-017-0
2	October 17, 2013	Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase "or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;" to the second sentence under the "Retirement of Existing Standards" section.	
2	December 19, 2013	FERC Order issued approving PRC-005-2. (The enforcement date for PRC-005-2 will be April 1, 2015, which is the first date entities must be compliant with part of the standard. The implementation plan for PRC-005-2 includes specific compliance dates and timeframes for each of the Requirements. The regulatory approval date in the U.S. is February 24, 2014.	
2	May 7, 2014	Adopted by the NERC Board of Trustees to modify VSLs for Requirement R1.	

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[1]**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 calendar years	For all unmonitored relays: • Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (see Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. • Alarming for power supply failure (see Table 2).	12 calendar years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.

[1] For the tables in this standard, a calendar year starts on the first day of a new year (January 1) after a maintenance activity has been completed. For the tables in this standard, a calendar month starts on the first day of the first month after a maintenance activity has been completed.

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[1]**	**Maintenance Activities**
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2).	12 calendar years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 1-2 Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.	4 calendar months	Verify that the communications system is functional.
	6 calendar years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2).	12 calendar years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with all of the following: • Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation). (See Table 2) • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).	12 calendar years	Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the Protection System

Table 1-3 Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage and current sensing devices not having monitoring attributes of the category below.	12 calendar years	Verify that current and voltage signal values are provided to the protective relays.
Voltage and Current Sensing devices connected to microprocessor relays with AC measurements are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2).	No periodic maintenance specified	None.

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply using **Vented Lead-Acid (VLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack
	18 Calendar Months -or- 6 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **with Valve Regulated Lead-Acid (VRLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	6 Calendar Months	Inspect: • Condition of all individual units by measuring battery cell/unit internal ohmic values.
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Physical condition of battery rack
	6 Calendar Months -or- 3 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **Nickel-Cadmium (NiCad) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells. • Physical condition of battery rack
	6 Calendar Years	Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(d) Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System station dc supply not using a battery and not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	18 Calendar Months	Inspect: Condition of non-battery based dc supply
	6 Calendar Years	Verify that the dc supply can perform as manufactured when ac power is not present.

Table 1-4(e) Component Type – Protection System Station dc Supply for non-BES Interrupting Devices for SPS, non-distributed UFLS, and non-distributed UVLS systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a SPS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).	When control circuits are verified (See Table 1-5)	Verify Station dc supply voltage.

Table 1-4(f) Exclusions for Protection System Station dc Supply Monitoring Devices and Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2).	No periodic maintenance specified	No periodic verification of station dc supply voltage is required.
Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2).		No periodic inspection of the electrolyte level for each cell is required.
Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2).		No periodic inspection of unintentional dc grounds is required.
Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2).		No periodic verification of float voltage of battery charger is required.
Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2).		No periodic verification of the battery continuity is required.
Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2).		No periodic verification of the intercell and terminal connection resistance is required.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2).		No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2).		No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required.

Table 1-5 Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3) **Note:** Table requirements apply to all Control Circuitry Components of Protection Systems, and SPSs except as noted.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry).	6 calendar years	Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device.
Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 calendar years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with SPS.	12 calendar years	Verify all paths of the control circuits essential for proper operation of the SPS.
Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays.	12 calendar years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with protective functions and/or SPS whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

Table 2 – Alarming Paths and Monitoring In Tables 1-1 through 1-5 and Table 3, alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any alarm path through which alarms in Tables 1-1 through 1-5 and Table 3 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the "Alarm Path with monitoring" category below. Alarms are reported within 24 hours of detection to a location where corrective action can be initiated.	12 Calendar Years	Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated.
Alarm Path with monitoring: The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated.	No periodic maintenance specified	None.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 calendar years	Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self diagnosis and alarming (See Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. Alarming for power supply failure (See Table 2).	12 calendar years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2).	12 calendar years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Voltage and/or current sensing devices associated with UFLS or UVLS systems.	12 calendar years	Verify that current and/or voltage signal values are provided to the protective relays.
Protection System dc supply for tripping non-BES interrupting devices used only for a UFLS or UVLS system.	12 calendar years	Verify Protection System dc supply voltage.
Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-BES interrupting device trip coils).	12 calendar years	Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic).
Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-BES interrupting device trip coils).	12 calendar years	Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices.
Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-BES interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-BES interrupting devices (excludes non-BES interrupting device trip coils).	No periodic maintenance specified	None.
Trip coils of non-BES interrupting devices in UFLS or UVLS systems.	No periodic maintenance specified	None.

PRC-005 — Attachment A

Criteria for a Performance-Based Protection System Maintenance Program

Purpose: To establish a technical basis for initial and continued use of a performance-based Protection System Maintenance Program (PSMP).

To establish the technical justification for the initial use of a performance-based PSMP:

1. Develop a list with a description of Components included in each designated Segment of the Protection System Component population, with a minimum **Segment** population of 60 Components.
2. Maintain the Components in each Segment according to the time-based maximum allowable intervals established in Tables 1-1 through 1-5 and Table 3 until results of maintenance activities for the Segment are available for a minimum of 30 individual Components of the Segment.
3. Document the maintenance program activities and results for each Segment, including maintenance dates and Countable Events for each included Component.
4. Analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment and develop maintenance intervals.
5. Determine the maximum allowable maintenance interval for each Segment such that the Segment experiences **Countable Events** on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

To maintain the technical justification for the ongoing use of a performance-based PSMP:

1. At least annually, update the list of Protection System Components and Segments and/or description if any changes occur within the Segment.
2. Perform maintenance on the greater of 5% of the Components (addressed in the performance based PSMP) in each Segment or 3 individual Components within the Segment in each year.
3. For the prior year, analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment.
4. Using the prior year's data, determine the maximum allowable maintenance interval for each Segment such that the Segment experiences Countable Events on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.
5. If the Components in a Protection System Segment maintained through a performance-based PSMP experience 4% or more Countable Events, develop, document, and implement an action plan to reduce the Countable Events to less than 4% of the Segment population within 3 years.

A. Introduction

1. Title: **Protection System Maintenance**

2. Number: PRC-005-2

3. Purpose: To document and implement programs for the maintenance of all Protection Systems affecting the reliability of the Bulk Electric System (BES) so that these Protection Systems are kept in working order.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner

4.1.2 Generator Owner

4.1.3 Distribution Provider

4.2. Facilities:

4.2.1 Protection Systems that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)

4.2.2 Protection Systems used for underfrequency load-shedding systems installed per ERO underfrequency load-shedding requirements.

4.2.3 Protection Systems used for undervoltage load-shedding systems installed to prevent system voltage collapse or voltage instability for BES reliability.

4.2.4 Protection Systems installed as a Special Protection System (SPS) for BES reliability.

4.2.5 Protection Systems for generator Facilities that are part of the BES, including:

4.2.5.1 Protection Systems that act to trip the generator either directly or via lockout or auxiliary tripping relays.

4.2.5.2 Protection Systems for generator step-up transformers for generators that are part of the BES.

4.2.5.3 Protection Systems for transformers connecting aggregated generation, where the aggregated generation is part of the BES (e.g., transformers connecting facilities such as wind-farms to the BES).

4.2.5.4 Protection Systems for station service or excitation transformers connected to the generator bus of generators which are part of the BES, that act to trip the generator either directly or via lockout or tripping auxiliary relays.

5. Effective Date: See Implementation Plan

6. Definitions Used in this Standard: The following terms are defined for use only within PRC-005-2, and should remain with the standard upon approval rather than being moved to the Glossary of Terms.

Unresolved Maintenance Issue – A deficiency identified during a maintenance activity that causes the component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up corrective action.

Segment – Protection Systems or components of a consistent design standard, or a particular model or type from a single manufacturer that typically share other common elements. Consistent performance is expected across the entire population of a Segment. A Segment must contain at least sixty (60) individual components.

Component Type - Any one of the five specific elements of the Protection System definition.

Component – A Component is any individual discrete piece of equipment included in a Protection System, including but not limited to a protective relay or current sensing device. The designation of what constitutes a control circuit Component is dependent upon how an entity performs and tracks the testing of the control circuitry. Some entities test their control circuits on a breaker basis whereas others test their circuitry on a local zone of protection basis. Thus, entities are allowed the latitude to designate their own definitions of control circuit Components. Another example of where the entity has some discretion on determining what constitutes a single Component is the voltage and current sensing devices, where the entity may choose either to designate a full three-phase set of such devices or a single device as a single Component.

Countable Event – A failure of a Component requiring repair or replacement, any condition discovered during the maintenance activities in Tables 1-1 through 1-5 and Table 3 which requires corrective action or a Misoperation attributed to hardware failure or calibration failure. Misoperations due to product design errors, software errors, relay settings different from specified settings, Protection System Component configuration errors, or Protection System application errors are not included in Countable Events.

B. Requirements

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a Protection System Maintenance Program (PSMP) for its Protection Systems identified in Section 4.2. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

The PSMP shall:

1.1. Identify which maintenance method (time-based, performance-based per PRC-005 Attachment A, or a combination) is used to address each Protection System Component Type. All batteries associated with the station dc supply Component Type of a Protection System shall be included in a time-based program as described in Table 1-4 and Table 3.

1.2. Include the applicable monitored Component attributes applied to each Protection System Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, and Table 3 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System Components.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals in its PSMP shall follow the procedure established in PRC-005 Attachment A to establish and maintain its performance-based intervals. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall maintain its Protection System Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall implement and follow its PSMP for its Protection System Components that are included within the performance-based program(s). *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R5. Each Transmission Owner, Generator Owner, and Distribution Provider shall demonstrate efforts to correct identified Unresolved Maintenance Issues. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

C. Measures

M1. Each Transmission Owner, Generator Owner and Distribution Provider shall have a documented Protection System Maintenance Program in accordance with Requirement R1.

For each Protection System Component Type, the documentation shall include the type of maintenance method applied (time-based, performance-based, or a combination of these maintenance methods), and shall include all batteries associated with the station dc supply Component Types in a time-based program as described in Table 1-4 and Table 3. (Part 1.1)

For Component Types that use monitoring to extend the maintenance intervals, the responsible entity(s) shall have evidence for each protection Component Type (such as manufacturer's specifications or engineering drawings) of the appropriate monitored Component attributes as specified in Tables 1-1 through 1-5, Table 2, and Table 3. (Part 1.2)

M2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals shall have evidence that its current performance-based maintenance program(s) is in accordance with Requirement R2, which may include but is not limited to Component lists, dated maintenance records, and dated analysis records and results.

M3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System Components included within its time-based program in accordance with Requirement R3. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance intervals in accordance with Requirement R2 shall have evidence that it has implemented the Protection System Maintenance Program for the Protection System Components included in its performance-based program in accordance with Requirement R4. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence that it has undertaken efforts to correct identified Unresolved Maintenance Issues in accordance with Requirement R5. The evidence may include but is not limited to work orders, replacement Component orders, invoices, project schedules with completed milestones, return material authorizations (RMAs) or purchase orders.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity

1.2. Compliance Monitoring and Enforcement Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.3. Evidence Retention

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

The Transmission Owner, Generator Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

For Requirement R1, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep its current dated Protection System Maintenance Program, as well as any superseded versions since the preceding compliance audit, including the documentation that specifies the type of maintenance program applied for each Protection System Component Type.

For Requirement R2, Requirement R3, Requirement R4, and Requirement R5, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the two most recent performances of each distinct maintenance activity for the Protection System Component, or all performances of each distinct maintenance activity for the Protection System Component since the previous scheduled audit date, whichever is longer.

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

1.4. Additional Compliance Information

None.

2. Violation Severity Levels

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The responsible entity's PSMP failed to specify whether one Component Type is being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1) ~~OR~~ ~~The responsible entity's PSMP failed to include applicable station batteries in a time-based program. (Part 1.1)~~	The responsible entity's PSMP failed to specify whether two Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1)	The responsible entity's PSMP failed to include the applicable monitoring attributes applied to each Protection System Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, and Table 3 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System Components. (Part 1.2).	The responsible entity failed to establish a PSMP. OR The responsible entity failed to specify whether three or more Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1). OR The responsible entity's PSMP failed to include applicable station batteries in a time-based program. (Part 1.1)
R2	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within three years.	NA	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within four years.	The responsible entity uses performance-based maintenance intervals in its PSMP but: 1) Failed to establish the technical justification described within Requirement R2 for the initial use of the performance-based PSMP OR 2) Failed to reduce Countable Events to no more than 4% within five years OR 3) Maintained a Segment with less than 60 Components OR

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
				4) Failed to: • Annually update the list of Components, OR • Annually perform maintenance on the greater of 5% of the segment population or 3 Components, OR • Annually analyze the program activities and results for each Segment.
R3	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain 5% or less of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain more than 15% of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.
R4	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain 5% or less of the annual scheduled maintenance for a specific Protection System Component Type in accordance with their performance-based PSMP.	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the annual scheduled maintenance for a specific Protection System Component Type in accordance	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the annual scheduled maintenance for a specific Protection System Component Type in accordance with their performance-based PSMP.	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 15% of the annual scheduled maintenance for a specific Protection System Component Type in accordance

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
		with their performance-based PSMP.		with their performance-based PSMP.
R5	The responsible entity failed to undertake efforts to correct 5 or fewer identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 5, but less than or equal to 10 identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 10, but less than or equal to 15 identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 15 identified Unresolved Maintenance Issues.

E. Regional Variances

None

F. Supplemental Reference Document

The following documents present a detailed discussion about determination of maintenance intervals and other useful information regarding establishment of a maintenance program.

1. PRC-005-2 Protection System Maintenance Supplementary Reference and FAQ — July 2012.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. 3. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/05
1a	February 17, 2011	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers	Project 2009-17 interpretation
1a	February 17, 2011	Adopted by Board of Trustees	
1a	September 26, 2011	FERC Order issued approving interpretation of R1 and R2 (FERC's Order is effective as of September 26, 2011)	
1.1a	February 1, 2012	Errata change: Clarified inclusion of generator interconnection Facility in Generator Owner's responsibility	Revision under Project 2010-07
1b	February 3, 2012	FERC Order issued approving interpretation of R1, R1.1, and R1.2 (FERC's Order dated March 14, 2012). Updated version from 1a to 1b.	Project 2009-10 Interpretation
1.1b	April 23, 2012	Updated standard version to 1.1b to reflect FERC approval of PRC-005-1b.	Revision under Project 2010-07

1.1b	May 9, 2012	PRC-005-1.1b was adopted by the Board of Trustees as part of Project 2010-07 (GOTO).	
2	November 7, 2012	Adopted by Board of Trustees	Complete revision, absorbing maintenance requirements from PRC-005-1b, PRC-008-0, PRC-011-0, PRC-017-0
2	October 17, 2013	Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase "or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;" to the second sentence under the "Retirement of Existing Standards" section.	
2	December 19, 2013	FERC Order issued approving PRC-005-2. (The enforcement date for PRC-005-2 will be April 1, 2015, which is the first date entities must be compliant with part of the standard. The implementation plan for PRC-005-2 includes specific compliance dates and timeframes for each of the Requirements. The regulatory approval date in the U.S. is February 24, 2014.	
2	May 7, 2014	Adopted by the NERC Board of Trustees to modify VSLs for Requirement R1.	

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[1]**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 calendar years	For all unmonitored relays: • Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (see Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. • Alarming for power supply failure (see Table 2).	12 calendar years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.

[1] For the tables in this standard, a calendar year starts on the first day of a new year (January 1) after a maintenance activity has been completed. For the tables in this standard, a calendar month starts on the first day of the first month after a maintenance activity has been completed.

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[1]**	**Maintenance Activities**
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2).	12 calendar years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 1-2 Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.	4 calendar months	Verify that the communications system is functional.
	6 calendar years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2).	12 calendar years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with all of the following: • Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation). (See Table 2) • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).	12 calendar years	Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the Protection System

Table 1-3 Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage and current sensing devices not having monitoring attributes of the category below.	12 calendar years	Verify that current and voltage signal values are provided to the protective relays.
Voltage and Current Sensing devices connected to microprocessor relays with AC measurements are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2).	No periodic maintenance specified	None.

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply using **Vented Lead-Acid (VLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack
	18 Calendar Months -or- 6 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **with Valve Regulated Lead-Acid (VRLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	6 Calendar Months	Inspect: • Condition of all individual units by measuring battery cell/unit internal ohmic values.
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Physical condition of battery rack
	6 Calendar Months -or- 3 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **Nickel-Cadmium (NiCad) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells. • Physical condition of battery rack
	6 Calendar Years	Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(d) Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System station dc supply not using a battery and not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	18 Calendar Months	Inspect: Condition of non-battery based dc supply
	6 Calendar Years	Verify that the dc supply can perform as manufactured when ac power is not present.

Table 1-4(e) Component Type – Protection System Station dc Supply for non-BES Interrupting Devices for SPS, non-distributed UFLS, and non-distributed UVLS systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a SPS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).	When control circuits are verified (See Table 1-5)	Verify Station dc supply voltage.

Table 1-4(f) Exclusions for Protection System Station dc Supply Monitoring Devices and Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2).	No periodic maintenance specified	No periodic verification of station dc supply voltage is required.
Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2).		No periodic inspection of the electrolyte level for each cell is required.
Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2).		No periodic inspection of unintentional dc grounds is required.
Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2).		No periodic verification of float voltage of battery charger is required.
Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2).		No periodic verification of the battery continuity is required.
Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2).		No periodic verification of the intercell and terminal connection resistance is required.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2).		No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2).		No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required.

Table 1-5 Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3) **Note:** Table requirements apply to all Control Circuitry Components of Protection Systems, and SPSs except as noted.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry).	6 calendar years	Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device.
Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 calendar years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with SPS.	12 calendar years	Verify all paths of the control circuits essential for proper operation of the SPS.
Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays.	12 calendar years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with protective functions and/or SPS whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

Table 2 – Alarming Paths and Monitoring In Tables 1-1 through 1-5 and Table 3, alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any alarm path through which alarms in Tables 1-1 through 1-5 and Table 3 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the "Alarm Path with monitoring" category below. Alarms are reported within 24 hours of detection to a location where corrective action can be initiated.	12 Calendar Years	Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated.
Alarm Path with monitoring: The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated.	No periodic maintenance specified	None.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 calendar years	Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self diagnosis and alarming (See Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. Alarming for power supply failure (See Table 2).	12 calendar years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2).	12 calendar years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Voltage and/or current sensing devices associated with UFLS or UVLS systems.	12 calendar years	Verify that current and/or voltage signal values are provided to the protective relays.
Protection System dc supply for tripping non-BES interrupting devices used only for a UFLS or UVLS system.	12 calendar years	Verify Protection System dc supply voltage.
Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-BES interrupting device trip coils).	12 calendar years	Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic).
Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-BES interrupting device trip coils).	12 calendar years	Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices.
Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-BES interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-BES interrupting devices (excludes non-BES interrupting device trip coils).	No periodic maintenance specified	None.
Trip coils of non-BES interrupting devices in UFLS or UVLS systems.	No periodic maintenance specified	None.

PRC-005 — Attachment A

Criteria for a Performance-Based Protection System Maintenance Program

Purpose: To establish a technical basis for initial and continued use of a performance-based Protection System Maintenance Program (PSMP).

To establish the technical justification for the initial use of a performance-based PSMP:

1. Develop a list with a description of Components included in each designated Segment of the Protection System Component population, with a minimum **Segment** population of 60 Components.
2. Maintain the Components in each Segment according to the time-based maximum allowable intervals established in Tables 1-1 through 1-5 and Table 3 until results of maintenance activities for the Segment are available for a minimum of 30 individual Components of the Segment.
3. Document the maintenance program activities and results for each Segment, including maintenance dates and Countable Events for each included Component.
4. Analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment and develop maintenance intervals.
5. Determine the maximum allowable maintenance interval for each Segment such that the Segment experiences **Countable Events** on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

To maintain the technical justification for the ongoing use of a performance-based PSMP:

1. At least annually, update the list of Protection System Components and Segments and/or description if any changes occur within the Segment.
2. Perform maintenance on the greater of 5% of the Components (addressed in the performance based PSMP) in each Segment or 3 individual Components within the Segment in each year.
3. For the prior year, analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment.
4. Using the prior year's data, determine the maximum allowable maintenance interval for each Segment such that the Segment experiences Countable Events on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.
5. If the Components in a Protection System Segment maintained through a performance-based PSMP experience 4% or more Countable Events, develop, document, and implement an action plan to reduce the Countable Events to less than 4% of the Segment population within 3 years.

Exhibit B

PRC-005-3 Clean and Redline VSL Revisions

A. Introduction

1. Title: **Protection System and Automatic Reclosing Maintenance**

2. Number: PRC-005-3.1

3. Purpose: To document and implement programs for the maintenance of all Protection Systems and Automatic Reclosing affecting the reliability of the Bulk Electric System (BES) so that they are kept in working order.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner

4.1.2 Generator Owner

4.1.3 Distribution Provider

4.2. Facilities:

4.2.1 Protection Systems that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)

4.2.2 Protection Systems used for underfrequency load-shedding systems installed per ERO underfrequency load-shedding requirements.

4.2.3 Protection Systems used for undervoltage load-shedding systems installed to prevent system voltage collapse or voltage instability for BES reliability.

4.2.4 Protection Systems installed as a Special Protection System (SPS) for BES reliability.

4.2.5 Protection Systems for generator Facilities that are part of the BES, including:

4.2.5.1 Protection Systems that act to trip the generator either directly or via lockout or auxiliary tripping relays.

4.2.5.2 Protection Systems for generator step-up transformers for generators that are part of the BES.

4.2.5.3 Protection Systems for transformers connecting aggregated generation, where the aggregated generation is part of the BES (e.g., transformers connecting facilities such as wind-farms to the BES).

4.2.5.4 Protection Systems for station service or excitation transformers connected to the generator bus of generators which are part of the BES, that act to trip the generator either directly or via lockout or tripping auxiliary relays.

4.2.6 Automatic Reclosing[1], including:

4.2.6.1 Automatic Reclosing applied on the terminals of Elements connected to the BES bus located at generating plant substations where the total installed

[1] Automatic Reclosing addressed in Section 4.2.6.1 and 4.2.6.2 may be excluded if the equipment owner can demonstrate that a close-in three-phase fault present for twice the normal clearing time (capturing a minimum trip-close-trip time delay) does not result in a total loss of gross generation in the Interconnection exceeding the gross capacity of the largest BES generating unit within the Balancing Authority Area where the Automatic Reclosing is applied.

gross generating plant capacity is greater than the gross capacity of the largest BES generating unit within the Balancing Authority Area.

4.2.6.2 Automatic Reclosing applied on the terminals of all BES Elements at substations one bus away from generating plants specified in Section 4.2.6.1 when the substation is less than 10 circuit-miles from the generating plant substation.

4.2.6.3 Automatic Reclosing applied as an integral part of an SPS specified in Section 4.2.4.

5. Effective Date: See Implementation Plan

6. Definitions Used in this Standard: The following terms are defined for use only within PRC-005-3, and should remain with the standard upon approval rather than being moved to the Glossary of Terms.

Automatic Reclosing – Includes the following Components:

- Reclosing relay
- Control circuitry associated with the reclosing relay.

Unresolved Maintenance Issue – A deficiency identified during a maintenance activity that causes the Component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up corrective action.

Segment – Components of a consistent design standard, or a particular model or type from a single manufacturer that typically share other common elements. Consistent performance is expected across the entire population of a Segment. A Segment must contain at least sixty (60) individual Components.

Component Type – Either any one of the five specific elements of the Protection System definition or any one of the two specific elements of the Automatic Reclosing definition.

Component – A Component is any individual discrete piece of equipment included in a Protection System or in Automatic Reclosing, including but not limited to a protective relay, reclosing relay, or current sensing device. The designation of what constitutes a control circuit Component is dependent upon how an entity performs and tracks the testing of the control circuitry. Some entities test their control circuits on a breaker basis whereas others test their circuitry on a local zone of protection basis. Thus, entities are allowed the latitude to designate their own definitions of control circuit Components. Another example of where the entity has some discretion on determining what constitutes a single Component is the voltage and current sensing devices, where the entity may choose either to designate a full three-phase set of such devices or a single device as a single Component.

Countable Event – A failure of a Component requiring repair or replacement, any condition discovered during the maintenance activities in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 which requires corrective action or a Protection System Misoperation attributed to hardware failure or calibration failure. Misoperations due to product design errors, software errors, relay settings different from specified settings, Protection System Component or Automatic Reclosing configuration or application errors are not included in Countable Events.

B. Requirements

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a Protection System Maintenance Program (PSMP) for its Protection Systems and Automatic Reclosing identified in Facilities Section 4.2. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

The PSMP shall:

1.1. Identify which maintenance method (time-based, performance-based per PRC-005 Attachment A, or a combination) is used to address each Protection System and Automatic Reclosing Component Type. All batteries associated with the station dc supply Component Type of a Protection System shall be included in a time-based program as described in Table 1-4 and Table 3.

1.2. Include the applicable monitored Component attributes applied to each Protection System and Automatic Reclosing Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System and Automatic Reclosing Components.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals in its PSMP shall follow the procedure established in PRC-005 Attachment A to establish and maintain its performance-based intervals. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall maintain its Protection System and Automatic Reclosing Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall implement and follow its PSMP for its Protection System and Automatic Reclosing Components that are included within the performance-based program(s). *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R5. Each Transmission Owner, Generator Owner, and Distribution Provider shall demonstrate efforts to correct identified Unresolved Maintenance Issues. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

C. Measures

M1. Each Transmission Owner, Generator Owner and Distribution Provider shall have a documented Protection System Maintenance Program in accordance with Requirement R1.

For each Protection System and Automatic Reclosing Component Type, the documentation shall include the type of maintenance method applied (time-based, performance-based, or a combination of these maintenance methods), and shall include all batteries associated with the station dc supply Component Types in a time-based program as described in Table 1-4 and Table 3. (Part 1.1)

For Component Types that use monitoring to extend the maintenance intervals, the responsible entity(s) shall have evidence for each Protection System and Automatic Reclosing Component Type (such as manufacturer's specifications or engineering drawings) of the appropriate

monitored Component attributes as specified in Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2. (Part 1.2)

M2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals shall have evidence that its current performance-based maintenance program(s) is in accordance with Requirement R2, which may include but is not limited to Component lists, dated maintenance records, and dated analysis records and results.

M3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System and Automatic Reclosing Components included within its time-based program in accordance with Requirement R3. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance intervals in accordance with Requirement R2 shall have evidence that it has implemented the Protection System Maintenance Program for the Protection System and Automatic Reclosing Components included in its performance-based program in accordance with Requirement R4. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence that it has undertaken efforts to correct identified Unresolved Maintenance Issues in accordance with Requirement R5. The evidence may include but is not limited to work orders, replacement Component orders, invoices, project schedules with completed milestones, return material authorizations (RMAs) or purchase orders.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Compliance Monitoring and Enforcement Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.3. Evidence Retention

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

The Transmission Owner, Generator Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

For Requirement R1, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep its current dated Protection System Maintenance Program, as well as any superseded versions since the preceding compliance audit, including the documentation that specifies the type of maintenance program applied for each Protection System Component Type.

For Requirement R2, Requirement R3, Requirement R4, and Requirement R5, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the two most recent performances of each distinct maintenance activity for the Protection System or Automatic Reclosing Component, or all performances of each distinct maintenance activity for the Protection System or Automatic Reclosing Component since the previous scheduled audit date, whichever is longer.

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

1.4. Additional Compliance Information

None.

2. Violation Severity Levels

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The responsible entity's PSMP failed to specify whether one Component Type is being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1)	The responsible entity's PSMP failed to specify whether two Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1)	The responsible entity's PSMP failed to specify whether three Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1). OR The responsible entity's PSMP failed to include the applicable monitoring attributes applied to each Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Components. (Part 1.2).	The responsible entity failed to establish a PSMP. OR The responsible entity's PSMP failed to specify whether four or more Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1). OR The responsible entity's PSMP failed to include applicable station batteries in a time-based program. (Part 1.1)
R2	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within three years.	NA	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within four years.	The responsible entity uses performance-based maintenance intervals in its PSMP but: 1) Failed to establish the technical justification described within Requirement R2 for the initial use of the performance-based PSMP OR 2) Failed to reduce Countable Events to no more than 4% within five years OR

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
				3) Maintained a Segment with less than 60 Components OR 4) Failed to: • Annually update the list of Components, OR • Annually perform maintenance on the greater of 5% of the Segment population or 3 Components, OR • Annually analyze the program activities and results for each Segment.
R3	For Components included within a time-based maintenance program, the responsible entity failed to maintain 5% or less of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.	For Components included within a time-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.	For Components included within a time-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.	For Components included within a time-based maintenance program, the responsible entity failed to maintain more than 15% of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.
R4	For Components included within a performance-based maintenance program, the responsible entity failed to maintain 5% or less of the annual scheduled maintenance for a specific	For Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the annual scheduled maintenance for a specific	For Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the annual scheduled maintenance for a specific	For Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 15% of the annual scheduled maintenance for a specific

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Component Type in accordance with their performance-based PSMP.	Component Type in accordance with their performance-based PSMP.	Component Type in accordance with their performance-based PSMP.	Component Type in accordance with their performance-based PSMP.
R5	The responsible entity failed to undertake efforts to correct 5 or fewer identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 5, but less than or equal to 10 identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 10, but less than or equal to 15 identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 15 identified Unresolved Maintenance Issues.

E. Regional Variances

None

F. Supplemental Reference Document

The following documents present a detailed discussion about determination of maintenance intervals and other useful information regarding establishment of a maintenance program.

1. PRC-005-2 Protection System Maintenance Supplementary Reference and FAQ — March 2013.
2. Considerations for Maintenance and Testing of Autoreclosing Schemes — November 2012.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. 3. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/05
1a	February 17, 2011	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers	Project 2009-17 interpretation
1a	February 17, 2011	Adopted by Board of Trustees	
1a	September 26, 2011	FERC Order issued approving interpretation of R1 and R2 (FERC's Order is effective as of September 26, 2011)	
1.1a	February 1, 2012	Errata change: Clarified inclusion of generator interconnection Facility in Generator Owner's responsibility	Revision under Project 2010-07
1b	February 3, 2012	FERC Order issued approving interpretation of R1, R1.1, and R1.2 (FERC's Order dated March 14, 2012). Updated version from 1a to 1b.	Project 2009-10 Interpretation
1.1b	April 23, 2012	Updated standard version to 1.1b to reflect FERC approval of PRC-005-1b.	Revision under Project 2010-07

1.1b	May 9, 2012	PRC-005-1.1b was adopted by the Board of Trustees as part of Project 2010-07 (GOTO).	
2	November 7, 2012	Adopted by Board of Trustees	Project 2007-17 - Complete revision, absorbing maintenance requirements from PRC-005-1.1b, PRC-008-0, PRC-011-0, PRC-017-0
2	October 17, 2013	Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase “or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;” to the second sentence under the “Retirement of Existing	
2	May 7, 2014	Adopted by the NERC Board of Trustees to modify VSLs for Requirement R1.	
3	November 7, 2013	Adopted by the NERC Board of Trustees	Revised to address the FERC directive in Order No.758 to include Automatic Reclosing in maintenance programs.
3.1	February 12, 2014	Errata Change: The Standards Committee approved errata changes to correct capitalization of certain defined terms within the definitions of "Unresolved Maintenance Issue" and "Protection System Maintenance Program". The changes will be reflected in the definitions section of PRC-005-3 for "Unresolved Maintenance Issue" and in the NERC Glossary of Terms for "Protection System Maintenance Program".	

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[2]**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	For all unmonitored relays: • Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (see Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. • Alarming for power supply failure (see Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.

[2] For the tables in this standard, a calendar year starts on the first day of a new year (January 1) after a maintenance activity has been completed. For the tables in this standard, a calendar month starts on the first day of the first month after a maintenance activity has been completed.

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[2]**	**Maintenance Activities**
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 1-2 Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.	4 Calendar Months	Verify that the communications system is functional.
	6 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2).	12 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with all of the following: • Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation). (See Table 2) • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).	12 Calendar Years	Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the Protection System

Table 1-3 Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage and current sensing devices not having monitoring attributes of the category below.	12 Calendar Years	Verify that current and voltage signal values are provided to the protective relays.
Voltage and Current Sensing devices connected to microprocessor relays with AC measurements are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2).	No periodic maintenance specified	None.

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply using **Vented Lead-Acid (VLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	18 Calendar Months -or- 6 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **with Valve Regulated Lead-Acid (VRLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	6 Calendar Months	Inspect: • Condition of all individual units by measuring battery cell/unit internal ohmic values.
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Physical condition of battery rack

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	6 Calendar Months -or- 3 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **Nickel-Cadmium (NiCad) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells. • Physical condition of battery rack
	6 Calendar Years	Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(d) Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System station dc supply not using a battery and not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	18 Calendar Months	Inspect: Condition of non-battery based dc supply
	6 Calendar Years	Verify that the dc supply can perform as manufactured when ac power is not present.

Table 1-4(e) Component Type – Protection System Station dc Supply for non-BES Interrupting Devices for SPS, non-distributed UFLS, and non-distributed UVLS systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a SPS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).	When control circuits are verified (See Table 1-5)	Verify Station dc supply voltage.

Table 1-4(f) Exclusions for Protection System Station dc Supply Monitoring Devices and Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2).	No periodic maintenance specified	No periodic verification of station dc supply voltage is required.
Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2).		No periodic inspection of the electrolyte level for each cell is required.
Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2).		No periodic inspection of unintentional dc grounds is required.
Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2).		No periodic verification of float voltage of battery charger is required.
Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2).		No periodic verification of the battery continuity is required.
Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2).		No periodic verification of the intercell and terminal connection resistance is required.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2).		No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2).		No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required.

Table 1-5 Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3) Note: Table requirements apply to all Control Circuitry Components of Protection Systems, and SPSs except as noted.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device.
Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with SPS. (See Table 4-2(b) for SPS which include Automatic Reclosing.)	12 Calendar Years	Verify all paths of the control circuits essential for proper operation of the SPS.
Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays.	12 Calendar Years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with protective functions and/or SPSs whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

Table 2 – Alarming Paths and Monitoring In Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2, alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any alarm path through which alarms in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the "Alarm Path with monitoring" category below. Alarms are reported within 24 hours of detection to a location where corrective action can be initiated.	12 Calendar Years	Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated.
Alarm Path with monitoring: The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated.	No periodic maintenance specified	None.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate. For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self diagnosis and alarming (See Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Voltage and/or current sensing devices associated with UFLS or UVLS systems.	12 Calendar Years	Verify that current and/or voltage signal values are provided to the protective relays.
Protection System dc supply for tripping non-BES interrupting devices used only for a UFLS or UVLS system.	12 Calendar Years	Verify Protection System dc supply voltage.
Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic).
Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices.
Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-BES interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-BES interrupting devices (excludes non-BES interrupting device trip coils).	No periodic maintenance specified	None.
Trip coils of non-BES interrupting devices in UFLS or UVLS systems.	No periodic maintenance specified	None.

Table 4-1 Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Reclosing Relay		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored reclosing relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.
Monitored microprocessor reclosing relay with the following: • Internal self diagnosis and alarming (See Table 2). • Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.

Table 4-2(a) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing Relays that are NOT an Integral Part of an SPS		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Unmonitored Control circuitry associated with Automatic Reclosing that is not an integral part of an SPS.	12 Calendar Years	Verify that Automatic Reclosing, upon initiation, does not issue a premature closing command to the close circuitry.
Control circuitry associated with Automatic Reclosing that is not part of an SPS and is monitored and alarmed for conditions that would result in a premature closing command. (See Table 2)	No periodic maintenance specified	None.

Table 4-2(b) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing Relays that ARE an Integral Part of an SPS		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Close coils or actuators of circuit breakers or similar devices that are used in conjunction with Automatic Reclosing as part of an SPS (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each close coil or actuator is able to operate the circuit breaker or mitigating device.
Unmonitored close control circuitry associated with Automatic Reclosing used as an integral part of an SPS.	12 Calendar Years	Verify all paths of the control circuits associated with Automatic Reclosing that are essential for proper operation of the SPS.
Control circuitry associated with Automatic Reclosing that is an integral part of an SPS whose integrity is monitored and alarmed. (See Table 2)	No periodic maintenance specified	None.

PRC-005 — Attachment A

Criteria for a Performance-Based Protection System Maintenance Program

Purpose: To establish a technical basis for initial and continued use of a performance-based Protection System Maintenance Program (PSMP).

To establish the technical justification for the initial use of a performance-based PSMP:

1. Develop a list with a description of Components included in each designated Segment, with a minimum **Segment** population of 60 Components.
2. Maintain the Components in each Segment according to the time-based maximum allowable intervals established in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 until results of maintenance activities for the Segment are available for a minimum of 30 individual Components of the Segment.
3. Document the maintenance program activities and results for each Segment, including maintenance dates and Countable Events for each included Component.
4. Analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment and develop maintenance intervals.
5. Determine the maximum allowable maintenance interval for each Segment such that the Segment experiences **Countable Events** on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

To maintain the technical justification for the ongoing use of a performance-based PSMP:

1. At least annually, update the list of Components and Segments and/or description if any changes occur within the Segment.
2. Perform maintenance on the greater of 5% of the Components (addressed in the performance based PSMP) in each Segment or 3 individual Components within the Segment in each year.
3. For the prior year, analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment.
4. Using the prior year's data, determine the maximum allowable maintenance interval for each Segment such that the Segment experiences Countable Events on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.
5. If the Components in a Segment maintained through a performance-based PSMP experience 4% or more Countable Events, develop, document, and implement an action plan to reduce the Countable Events to less than 4% of the Segment population within 3 years.

A. Introduction

1. Title: **Protection System and Automatic Reclosing Maintenance**

2. Number: PRC-005-3.1

3. Purpose: To document and implement programs for the maintenance of all Protection Systems and Automatic Reclosing affecting the reliability of the Bulk Electric System (BES) so that they are kept in working order.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner

4.1.2 Generator Owner

4.1.3 Distribution Provider

4.2. Facilities:

4.2.1 Protection Systems that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)

4.2.2 Protection Systems used for underfrequency load-shedding systems installed per ERO underfrequency load-shedding requirements.

4.2.3 Protection Systems used for undervoltage load-shedding systems installed to prevent system voltage collapse or voltage instability for BES reliability.

4.2.4 Protection Systems installed as a Special Protection System (SPS) for BES reliability.

4.2.5 Protection Systems for generator Facilities that are part of the BES, including:

4.2.5.1 Protection Systems that act to trip the generator either directly or via lockout or auxiliary tripping relays.

4.2.5.2 Protection Systems for generator step-up transformers for generators that are part of the BES.

4.2.5.3 Protection Systems for transformers connecting aggregated generation, where the aggregated generation is part of the BES (e.g., transformers connecting facilities such as wind-farms to the BES).

4.2.5.4 Protection Systems for station service or excitation transformers connected to the generator bus of generators which are part of the BES, that act to trip the generator either directly or via lockout or tripping auxiliary relays.

4.2.6 Automatic Reclosing[1], including:

4.2.6.1 Automatic Reclosing applied on the terminals of Elements connected to the BES bus located at generating plant substations where the total installed

[1] Automatic Reclosing addressed in Section 4.2.6.1 and 4.2.6.2 may be excluded if the equipment owner can demonstrate that a close-in three-phase fault present for twice the normal clearing time (capturing a minimum trip-close-trip time delay) does not result in a total loss of gross generation in the Interconnection exceeding the gross capacity of the largest BES generating unit within the Balancing Authority Area where the Automatic Reclosing is applied.

gross generating plant capacity is greater than the gross capacity of the largest BES generating unit within the Balancing Authority Area.

4.2.6.2 Automatic Reclosing applied on the terminals of all BES Elements at substations one bus away from generating plants specified in Section 4.2.6.1 when the substation is less than 10 circuit-miles from the generating plant substation.

4.2.6.3 Automatic Reclosing applied as an integral part of an SPS specified in Section 4.2.4.

5. Effective Date: See Implementation Plan

6. Definitions Used in this Standard: The following terms are defined for use only within PRC-005-3, and should remain with the standard upon approval rather than being moved to the Glossary of Terms.

Automatic Reclosing – Includes the following Components:

- Reclosing relay
- Control circuitry associated with the reclosing relay.

Unresolved Maintenance Issue – A deficiency identified during a maintenance activity that causes the ~~component~~ Component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up corrective action.

Segment – Components of a consistent design standard, or a particular model or type from a single manufacturer that typically share other common elements. Consistent performance is expected across the entire population of a Segment. A Segment must contain at least sixty (60) individual Components.

Component Type – Either any one of the five specific elements of the Protection System definition or any one of the two specific elements of the Automatic Reclosing definition.

Component – A Component is any individual discrete piece of equipment included in a Protection System or in Automatic Reclosing, including but not limited to a protective relay, reclosing relay, or current sensing device. The designation of what constitutes a control circuit Component is dependent upon how an entity performs and tracks the testing of the control circuitry. Some entities test their control circuits on a breaker basis whereas others test their circuitry on a local zone of protection basis. Thus, entities are allowed the latitude to designate their own definitions of control circuit Components. Another example of where the entity has some discretion on determining what constitutes a single Component is the voltage and current sensing devices, where the entity may choose either to designate a full three-phase set of such devices or a single device as a single Component.

Countable Event – A failure of a Component requiring repair or replacement, any condition discovered during the maintenance activities in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 which requires corrective action or a Protection System Misoperation attributed to hardware failure or calibration failure. Misoperations due to product design errors, software errors, relay settings different from specified settings, Protection System Component or Automatic Reclosing configuration or application errors are not included in Countable Events.

B. Requirements

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a Protection System Maintenance Program (PSMP) for its Protection Systems and Automatic Reclosing identified in Facilities Section 4.2. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

The PSMP shall:

1.1. Identify which maintenance method (time-based, performance-based per PRC-005 Attachment A, or a combination) is used to address each Protection System and Automatic Reclosing Component Type. All batteries associated with the station dc supply Component Type of a Protection System shall be included in a time-based program as described in Table 1-4 and Table 3.

1.2. Include the applicable monitored Component attributes applied to each Protection System and Automatic Reclosing Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System and Automatic Reclosing Components.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals in its PSMP shall follow the procedure established in PRC-005 Attachment A to establish and maintain its performance-based intervals. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall maintain its Protection System and Automatic Reclosing Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall implement and follow its PSMP for its Protection System and Automatic Reclosing Components that are included within the performance-based program(s). *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R5. Each Transmission Owner, Generator Owner, and Distribution Provider shall demonstrate efforts to correct identified Unresolved Maintenance Issues. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

C. Measures

M1. Each Transmission Owner, Generator Owner and Distribution Provider shall have a documented Protection System Maintenance Program in accordance with Requirement R1.

For each Protection System and Automatic Reclosing Component Type, the documentation shall include the type of maintenance method applied (time-based, performance-based, or a combination of these maintenance methods), and shall include all batteries associated with the station dc supply Component Types in a time-based program as described in Table 1-4 and Table 3. (Part 1.1)

For Component Types that use monitoring to extend the maintenance intervals, the responsible entity(s) shall have evidence for each Protection System and Automatic Reclosing Component Type (such as manufacturer's specifications or engineering drawings) of the appropriate

monitored Component attributes as specified in Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2. (Part 1.2)

M2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals shall have evidence that its current performance-based maintenance program(s) is in accordance with Requirement R2, which may include but is not limited to Component lists, dated maintenance records, and dated analysis records and results.

M3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System and Automatic Reclosing Components included within its time-based program in accordance with Requirement R3. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance intervals in accordance with Requirement R2 shall have evidence that it has implemented the Protection System Maintenance Program for the Protection System and Automatic Reclosing Components included in its performance-based program in accordance with Requirement R4. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence that it has undertaken efforts to correct identified Unresolved Maintenance Issues in accordance with Requirement R5. The evidence may include but is not limited to work orders, replacement Component orders, invoices, project schedules with completed milestones, return material authorizations (RMAs) or purchase orders.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Compliance Monitoring and Enforcement Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.3. Evidence Retention

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

The Transmission Owner, Generator Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

For Requirement R1, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep its current dated Protection System Maintenance Program, as well as any superseded versions since the preceding compliance audit, including the documentation that specifies the type of maintenance program applied for each Protection System Component Type.

For Requirement R2, Requirement R3, Requirement R4, and Requirement R5, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the two most recent performances of each distinct maintenance activity for the Protection System or Automatic Reclosing Component, or all performances of each distinct maintenance activity for the Protection System or Automatic Reclosing Component since the previous scheduled audit date, whichever is longer.

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

1.4. Additional Compliance Information

None.

2. Violation Severity Levels

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The responsible entity's PSMP failed to specify whether one Component Type is being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1) ~~OR~~ ~~The responsible entity's PSMP failed to include applicable station batteries in a time-based program. (Part 1.1)~~	The responsible entity's PSMP failed to specify whether two Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1)	The responsible entity's PSMP failed to specify whether three Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1). OR The responsible entity's PSMP failed to include the applicable monitoring attributes applied to each Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Components. (Part 1.2).	The responsible entity failed to establish a PSMP. OR The responsible entity's PSMP failed to specify whether four or more Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1). OR The responsible entity's PSMP failed to include applicable station batteries in a time-based program. (Part 1.1)
R2	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within three years.	NA	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within four years.	The responsible entity uses performance-based maintenance intervals in its PSMP but: 1) Failed to establish the technical justification described within Requirement R2 for the initial use of the performance-based PSMP OR 2) Failed to reduce Countable Events to no more than 4% within five years OR

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
				3) Maintained a Segment with less than 60 Components OR 4) Failed to: • Annually update the list of Components, OR • Annually perform maintenance on the greater of 5% of the Segment population or 3 Components, OR • Annually analyze the program activities and results for each Segment.
R3	For Components included within a time-based maintenance program, the responsible entity failed to maintain 5% or less of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.	For Components included within a time-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.	For Components included within a time-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.	For Components included within a time-based maintenance program, the responsible entity failed to maintain more than 15% of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.
R4	For Components included within a performance-based maintenance program, the responsible entity failed to maintain 5% or less of the annual scheduled maintenance for a specific	For Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the annual scheduled maintenance for a specific	For Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the annual scheduled maintenance for a specific	For Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 15% of the annual scheduled maintenance for a specific

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Component Type in accordance with their performance-based PSMP.	Component Type in accordance with their performance-based PSMP.	Component Type in accordance with their performance-based PSMP.	Component Type in accordance with their performance-based PSMP.
R5	The responsible entity failed to undertake efforts to correct 5 or fewer identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 5, but less than or equal to 10 identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 10, but less than or equal to 15 identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 15 identified Unresolved Maintenance Issues.

E. Regional Variances

None

F. Supplemental Reference Document

The following documents present a detailed discussion about determination of maintenance intervals and other useful information regarding establishment of a maintenance program.

1. PRC-005-2 Protection System Maintenance Supplementary Reference and FAQ — March 2013.
2. Considerations for Maintenance and Testing of Autoreclosing Schemes — November 2012.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. 3. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/05
1a	February 17, 2011	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers	Project 2009-17 interpretation
1a	February 17, 2011	Adopted by Board of Trustees	
1a	September 26, 2011	FERC Order issued approving interpretation of R1 and R2 (FERC's Order is effective as of September 26, 2011)	
1.1a	February 1, 2012	Errata change: Clarified inclusion of generator interconnection Facility in Generator Owner's responsibility	Revision under Project 2010-07
1b	February 3, 2012	FERC Order issued approving interpretation of R1, R1.1, and R1.2 (FERC's Order dated March 14, 2012). Updated version from 1a to 1b.	Project 2009-10 Interpretation
1.1b	April 23, 2012	Updated standard version to 1.1b to reflect FERC approval of PRC-005-1b.	Revision under Project 2010-07

1.1b	May 9, 2012	PRC-005-1.1b was adopted by the Board of Trustees as part of Project 2010-07 (GOTO).	
2	November 7, 2012	Adopted by Board of Trustees	Project 2007-17 - Complete revision, absorbing maintenance requirements from PRC-005-1.1b, PRC-008-0, PRC-011-0, PRC-017-0
2	October 17, 2013	Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase “or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;” to the second sentence under the “Retirement of Existing	
2	May 7, 2014	Adopted by the NERC Board of Trustees to modify VSLs for Requirement R1.	
3	November 7, 2013	Adopted by the NERC Board of Trustees	Revised to address the FERC directive in Order No.758 to include Automatic Reclosing in maintenance programs.
3.1	February 12, 2014	Errata Change: The Standards Committee approved errata changes to correct capitalization of certain defined terms within the definitions of "Unresolved Maintenance Issue" and "Protection System Maintenance Program". The changes will be reflected in the definitions section of PRC-005-3 for "Unresolved Maintenance Issue" and in the NERC Glossary of Terms for "Protection System Maintenance Program".	

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[2]**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	For all unmonitored relays: • Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (see Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. • Alarming for power supply failure (see Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.

[2] For the tables in this standard, a calendar year starts on the first day of a new year (January 1) after a maintenance activity has been completed. For the tables in this standard, a calendar month starts on the first day of the first month after a maintenance activity has been completed.

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[2]**	**Maintenance Activities**
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 1-2 Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.	4 Calendar Months	Verify that the communications system is functional.
	6 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2).	12 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with all of the following: • Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation). (See Table 2) • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).	12 Calendar Years	Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the Protection System

Table 1-3 Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage and current sensing devices not having monitoring attributes of the category below.	12 Calendar Years	Verify that current and voltage signal values are provided to the protective relays.
Voltage and Current Sensing devices connected to microprocessor relays with AC measurements are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2).	No periodic maintenance specified	None.

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply using **Vented Lead-Acid (VLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	18 Calendar Months -or- 6 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **with Valve Regulated Lead-Acid (VRLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	6 Calendar Months	Inspect: • Condition of all individual units by measuring battery cell/unit internal ohmic values.
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Physical condition of battery rack

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	6 Calendar Months -or- 3 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **Nickel-Cadmium (NiCad) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells. • Physical condition of battery rack
	6 Calendar Years	Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(d) Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System station dc supply not using a battery and not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	18 Calendar Months	Inspect: Condition of non-battery based dc supply
	6 Calendar Years	Verify that the dc supply can perform as manufactured when ac power is not present.

Table 1-4(e) Component Type – Protection System Station dc Supply for non-BES Interrupting Devices for SPS, non-distributed UFLS, and non-distributed UVLS systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a SPS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).	When control circuits are verified (See Table 1-5)	Verify Station dc supply voltage.

Table 1-4(f) Exclusions for Protection System Station dc Supply Monitoring Devices and Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2).	No periodic maintenance specified	No periodic verification of station dc supply voltage is required.
Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2).		No periodic inspection of the electrolyte level for each cell is required.
Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2).		No periodic inspection of unintentional dc grounds is required.
Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2).		No periodic verification of float voltage of battery charger is required.
Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2).		No periodic verification of the battery continuity is required.
Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2).		No periodic verification of the intercell and terminal connection resistance is required.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2).		No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2).		No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required.

Table 1-5 Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3) Note: Table requirements apply to all Control Circuitry Components of Protection Systems, and SPSs except as noted.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device.
Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with SPS. (See Table 4-2(b) for SPS which include Automatic Reclosing.)	12 Calendar Years	Verify all paths of the control circuits essential for proper operation of the SPS.
Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays.	12 Calendar Years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with protective functions and/or SPSs whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

Table 2 – Alarming Paths and Monitoring In Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2, alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any alarm path through which alarms in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the "Alarm Path with monitoring" category below. Alarms are reported within 24 hours of detection to a location where corrective action can be initiated.	12 Calendar Years	Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated.
Alarm Path with monitoring: The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated.	No periodic maintenance specified	None.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate. For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self diagnosis and alarming (See Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Voltage and/or current sensing devices associated with UFLS or UVLS systems.	12 Calendar Years	Verify that current and/or voltage signal values are provided to the protective relays.
Protection System dc supply for tripping non-BES interrupting devices used only for a UFLS or UVLS system.	12 Calendar Years	Verify Protection System dc supply voltage.
Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic).
Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices.
Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-BES interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-BES interrupting devices (excludes non-BES interrupting device trip coils).	No periodic maintenance specified	None.
Trip coils of non-BES interrupting devices in UFLS or UVLS systems.	No periodic maintenance specified	None.

Table 4-1 Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Reclosing Relay		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored reclosing relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.
Monitored microprocessor reclosing relay with the following: • Internal self diagnosis and alarming (See Table 2). • Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.

Table 4-2(a) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing Relays that are NOT an Integral Part of an SPS		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Unmonitored Control circuitry associated with Automatic Reclosing that is not an integral part of an SPS.	12 Calendar Years	Verify that Automatic Reclosing, upon initiation, does not issue a premature closing command to the close circuitry.
Control circuitry associated with Automatic Reclosing that is not part of an SPS and is monitored and alarmed for conditions that would result in a premature closing command. (See Table 2)	No periodic maintenance specified	None.

Table 4-2(b) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing Relays that ARE an Integral Part of an SPS		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Close coils or actuators of circuit breakers or similar devices that are used in conjunction with Automatic Reclosing as part of an SPS (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each close coil or actuator is able to operate the circuit breaker or mitigating device.
Unmonitored close control circuitry associated with Automatic Reclosing used as an integral part of an SPS.	12 Calendar Years	Verify all paths of the control circuits associated with Automatic Reclosing that are essential for proper operation of the SPS.
Control circuitry associated with Automatic Reclosing that is an integral part of an SPS whose integrity is monitored and alarmed. (See Table 2)	No periodic maintenance specified	None.

PRC-005 — Attachment A

Criteria for a Performance-Based Protection System Maintenance Program

Purpose: To establish a technical basis for initial and continued use of a performance-based Protection System Maintenance Program (PSMP).

To establish the technical justification for the initial use of a performance-based PSMP:

1. Develop a list with a description of Components included in each designated Segment, with a minimum **Segment** population of 60 Components.
2. Maintain the Components in each Segment according to the time-based maximum allowable intervals established in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 until results of maintenance activities for the Segment are available for a minimum of 30 individual Components of the Segment.
3. Document the maintenance program activities and results for each Segment, including maintenance dates and Countable Events for each included Component.
4. Analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment and develop maintenance intervals.
5. Determine the maximum allowable maintenance interval for each Segment such that the Segment experiences **Countable Events** on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

To maintain the technical justification for the ongoing use of a performance-based PSMP:

1. At least annually, update the list of Components and Segments and/or description if any changes occur within the Segment.
2. Perform maintenance on the greater of 5% of the Components (addressed in the performance based PSMP) in each Segment or 3 individual Components within the Segment in each year.
3. For the prior year, analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment.
4. Using the prior year's data, determine the maximum allowable maintenance interval for each Segment such that the Segment experiences Countable Events on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.
5. If the Components in a Segment maintained through a performance-based PSMP experience 4% or more Countable Events, develop, document, and implement an action plan to reduce the Countable Events to less than 4% of the Segment population within 3 years.

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)**	**Docket No. RD14-___-000**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARDS VAR-001-4 AND VAR-002-3 AND THE RETIREMENT OF RELIABILITY STANDARDS VAR-001-3 AND VAR-002-2b

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

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Shamai Elstein
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, DC 20005
(202) 400-3000
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

June 9, 2014

TABLE OF CONTENTS

Page

I. EXECUTIVE SUMMARY 3
II. NOTICES AND COMMUNICATIONS 8
III. BACKGROUND 8
A. Regulatory Framework 8
B. NERC Reliability Standards Development Procedure 9
C. The Existing VAR Reliability Standards 10
1. Reliability Standard VAR-001-3 10
2. Reliability Standard VAR-002-2b 12
D. Procedural History of Project 2013-04 – Voltage and Reactive Control (VAR) 13
IV. JUSTIFICATION FOR APPROVAL 15
A. Basis and Purpose of the Proposed Reliability Standards 15
B. Requirements in the Proposed Reliability Standards 17
1. Reliability Standard VAR-001-4 17
2. Reliability Standard VAR-002-3 27
C. Proposed VAR-001-4 and VAR-002-3 Satisfy Outstanding Commission Directives 32
D. Enforceability of the Proposed Reliability Standards 40
V. EFFECTIVE DATE 41
VI. CONCLUSION 42

Exhibit A Proposed Reliability Standards
Exhibit A-1 Proposed Reliability Standard VAR-001-4
Exhibit A-2 Proposed Reliability Standard VAR-002-3
Exhibit B Implementation Plan
Exhibit C Order No. 672 Criteria
Exhibit D Mapping Document
Exhibit D-1 Mapping Document for Proposed Reliability Standard VAR-001-4
Exhibit D-2 Mapping Document for Proposed Reliability Standard VAR-002-3
Exhibit E Analysis of Violation Risk Factors and Violation Severity Levels
Exhibit F Summary of Development History and Record of Development
Exhibit G Standard Drafting Team Roster

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. RD14-___-000**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARDS VAR-001-4 AND VAR-002-3 AND THE RETIREMENT OF RELIABILITY STANDARDS VAR-001-3 AND VAR-002-2b

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA")[1] and Section 39.5 of the Commission's Regulations,[2] the North American Electric Reliability Corporation ("NERC")[3] hereby submits proposed Reliability Standards VAR-001-4 (Voltage and Reactive Control) and VAR-002-3 (Generator Operation for Maintaining Network Voltage Schedules) for Commission approval.[4] NERC requests that the Commission approve proposed Reliability Standards VAR-001-4 and VAR-002-3 as just, reasonable, not unduly discriminatory or preferential, and in the public interest.[5] NERC also requests approval of (i) the associated Implementation Plan, (ii) the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs"), and (iii) the retirement of currently effective Reliability Standards VAR-001-3 and VAR-002-2b, as detailed in this Petition.

---

1 16 U.S.C. § 824o(d)(1) (2012).

2 18 C.F.R. § 39.5 (2013).

3 The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009) ("ERO Certification Order").

4 The NERC Board of Trustees approved proposed Reliability Standards VAR-001-4 on February 6, 2014 and VAR-002-3 on May 7, 2014.

5 Unless otherwise designated, all capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary"), *available at* http://www.nerc.com/files/Glossary_of_Terms.pdf.

As required by Section 39.5(a)[6] of the Commission's Regulations, this Petition presents the technical basis and purpose of proposed Reliability Standards VAR-001-4 and VAR-002-3, a summary of the development history, and a demonstration that the proposed Reliability Standards meet the criteria identified by the Commission in Order No. 672.[7] This Petition is organized as follows: First, the Petition presents an executive summary of the proposed Reliability Standards. Next, the Petition provides background on the regulatory structure governing the Reliability Standards approval process, as well as information on the existing Reliability Standards that proposed VAR-001-4 and VAR-002-3 Reliability Standards will replace. The Petition then discusses the proposed Reliability Standards in detail, including how they satisfy the governing statutory criteria and the Commission's directives associated with these Reliability Standards. Finally, we provide the requested effective date for the proposed Reliability Standards.

The following documents are attached as exhibits to this Petition: (a) the proposed Reliability Standards (Exhibit A, with VAR-001-4 as Exhibit A-1 and VAR-002-3 as Exhibit A-2), (b) the proposed Implementation Plan for the proposed Reliability Standards (Exhibit B), (c) a discussion of how the proposed Reliability Standards satisfy the Order No. 672 criteria (Exhibit C), (d) mapping documents showing how the proposed Reliability Standards compare to the corresponding existing Reliability Standards (Exhibit D, with VAR-001-4 compared against VAR-001-3 as Exhibit D-1 and VAR-002-3 compared against VAR-002-2b as Exhibit D-2), (e) an analysis of the VRFs and VSLs for the proposed Reliability Standards (Exhibit E), (f) a

[6] 18 C.F.R. § 39.5(a) (2013).

[7] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, at PP 262, 321–37, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

summary of the development history and record of development for the proposed Reliability Standards (Exhibit F), and (g) the standard drafting team roster (Exhibit G).

I. EXECUTIVE SUMMARY

The Voltage and Reactive ("VAR") group of Reliability Standards, which consists of two continent-wide Reliability Standards, VAR-001-3 and VAR-002-2b,[8] is designed to maintain voltage stability on the Bulk-Power System, protect transmission, generation, distribution, and customer equipment, and support the reliable operation of the Bulk-Power System. Voltage stability is the ability of a power system to maintain acceptable voltage levels throughout the system under normal operating conditions and following a disturbance. Failure to maintain acceptable voltage levels (*i.e.*, voltage levels become too high or too low) may cause violations of System Operating Limits ("SOLs") and Interconnection Reliability Operating Limits ("IROLs"), result in damage to Bulk-Power System equipment, and thereby threaten the reliable operation of the Bulk-Power System. The primary factor in maintaining voltage stability is having the appropriate amount of Reactive Power on the system.[9] Proposed Reliability Standards VAR-001-4 and VAR-002-3 are intended to replace and improve upon Reliability Standards VAR-001-3 and VAR-002-2b, respectively, to ensure that the Bulk-Power System operates at acceptable voltage levels and that sufficient Reactive Power is available to maintain voltage stability.

[8] The VAR group of Reliability Standards also includes two regional Reliability Standards, VAR-002-WECC-1 and VAR-501-WECC-1. NERC is not proposing any modifications to these regional Reliability Standards. Additionally, VAR-001-3 includes a regional variance developed by the Western Electricity Coordinating Council ("WECC") applicable to Generator Operators located in the WECC region. NERC has not substantively modified the WECC regional variance and it will be carried forward as part of VAR-001-4. Accordingly, this Petition does not discuss the two regional Reliability Standards or the regional variance.

[9] Reactive Power is the portion of electricity that establishes and sustains the electric and magnetic fields of Bulk-Power System equipment and supports voltage stability.

In general, proposed Reliability Standard VAR-001-4 sets forth the requirements applicable to Transmission Operators for scheduling, monitoring, and controlling Reactive Power resources in the Real-time Operations, Same-day Operations, and Operational Planning time horizons to regulate voltage and Reactive Power flows for the reliable operation of the Bulk-Power System. Proposed Reliability Standard VAR-002-3 sets forth the requirements applicable to Generator Operators and Generator Owners for providing the necessary reactive support and voltage control necessary to maintain reliable operations. Generators are the largest and most reliable Reactive Power resource and play an integral role in maintaining voltage stability on the Bulk-Power System. Collectively, the proposed Reliability Standards are designed to prevent voltage instability and voltage collapse on the Bulk-Power System.

As described further below, proposed Reliability Standard VAR-001-4 requires each Transmission Operator to:

- Specify a system-wide voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within SOLs and IROLs, and to provide the voltage schedule to its Reliability Coordinator and adjacent Transmission Operators upon request (Requirement R1);
- Schedule sufficient reactive resources to regulate voltage levels (Requirement R2);
- Operate or direct the operation of devices to regulate transmission voltage and reactive flows (Requirement R3);
- Develop a set of criteria to exempt generators from certain requirements under Reliability Standard VAR-002-3 related to voltage or Reactive Power schedules, automatic voltage regulations, and notification (Requirement R4);
- Specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) for generators at either the high or low voltage side of the generator step-up transformer, provide the schedule to the associated Generator Operator, direct the Generator Operator to comply with that schedule in automatic voltage control mode, provide the Generator Operator the notification requirements for deviating from the schedule, and, if requested, provide the Generator Operator the criteria used to develop the schedule (Requirement R5); and

- Communicate step-up transformer tap changes, the time frame for completion, and the justification for these changes to Generator Owners (Requirement R6).

Proposed Reliability Standard VAR-002-3 requires each Generator Operator to:

- Operate each of its generators connected to the interconnected transmission system in automatic voltage control mode or in a different control mode as instructed by the Transmission Operator, unless the Generator Operator (1) is exempted pursuant to the criteria developed under VAR-001-4, Requirement R4, or (2) makes certain notifications to the Transmission Operator specifying the reasons it cannot so operate (Requirement R1);

- Maintain the Transmission Operator's generator voltage or Reactive Power schedule, unless the Generator Operator (1) is exempted pursuant to the criteria developed under VAR-001-4, Requirement R4, or (2) complies with the notification requirements for deviations as established by the Transmission Owner pursuant to VAR-001-4, Requirement R5 (Requirement R2);[10]

- Notify the Transmission Operator of a change in status of its voltage controlling device within 30 minutes, unless the status is restored within that time period (Requirement R3); and

- Notify the Transmission Operator of a change in reactive capability due to factors other than those described in VAR-002-3, Requirement R3 within 30 minutes unless the capability has been restored during that time period (Requirement R4).

Proposed Reliability Standard VAR-002-3 also requires each Generator Owner to:

- Provide information on its step-up transformers and auxiliary transformers within 30 days of a request from the Transmission Operator or Transmission Planner (Requirement R5); and

- Comply with the Transmission Operator's step-up transformer tap change directives unless compliance would violate safety, an equipment rating, or applicable laws, rules or regulations (Requirement R6).

[10] VAR-002-3, Requirement R2 also provides that: (1) when a generator's AVR is out of service or the generator does not have AVR, the Generator Operator shall use an alternative method to control the generator's Reactive Power output to meet the schedule; (2) when instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met; and (3) if the Generator Operator does not monitor voltage at the location specified in its voltage schedule, it shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

The proposed Reliability Standards were developed to address outstanding Commission directives from Order Nos. 693[11] and 724[12] and build upon the previous versions of the Reliability Standards to improve their quality and content.[13] In addition to addressing certain Commission directives, the proposed Reliability Standards streamline language for increased clarity, omit requirements duplicative with or otherwise unnecessary when compared to existing Reliability Standards, and remove requirements that provide little to no reliability benefit. As discussed further below, Reliability Standard VAR-001-4 improves upon the prior version of the standard as follows:

- Requirements that are duplicative of other currently enforceable and pending Reliability Standards are removed.

- Requirement R1 improves reliability by requiring Transmission Operators to (1) define system voltage schedules, which may be a range or a target value with an associated tolerance band, to help ensure the Bulk-Power System operates within operating limits, and (2) coordinate with adjacent Transmission Operators and Reliability Coordinators regarding those system voltage schedules.

- Requirement R2 consolidates Requirements R2 and R9 of VAR-001-3 to clarify the Transmission Operator's responsibility to schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions.[14]

- Requirement R3 consolidates Requirements R7 and R8 of VAR-001-3 to clarify the Transmission Operator's responsibility to provide the necessary voltage support (*i.e.*, "operate or direct the Real-time operation of devices"[15]) to help maintain voltage stability.

- Requirement R4 continues to provide Transmission Operators the flexibility to exempt generators from certain compliance obligations, but clarifies the obligations from which

---

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

[12] *Electric Reliability Organization Interpretations of Specific Requirements of Frequency Response and Bias and Voltage and Reactive Control Reliability Standards*, Order No. 724, 127 FERC ¶ 61,158 (2009).

[13] Exhibits D-1 and D-2 to this Petition provide mapping documents comparing the existing VAR-001-3 and VAR-002-2b Reliability Standards to the proposed VAR-001-4 and VAR-002-3 Reliability Standards.

[14] A Contingency is defined in the NERC Glossary as "the unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch or other electrical element."

[15] VAR-001-4, Requirement R3.

generators may be exempt. Requirement R4 also eliminates the need for Transmission Operators to maintain a list of all generators that have been granted an exemption as such a requirement provides little to no reliability benefit.

- Requirement R5 creates a more transparent information-sharing process between Transmission Operators and Generator Operators about voltage or Reactive Power schedules and notification requirements for deviating from such schedules.

- Requirement R5 also addresses the Commission's Order No. 693 directive to consider a time frame associated with an "incident" of non-compliance with VAR-002,[16] as well as the Order No. 724 directive to develop and implement technically sound voltage schedules.

Further, in proposed Reliability Standard VAR-002-3:

- Requirements R1 and R2 carry forward the obligations that Generator Operators operate in automatic voltage control mode and follow the voltage or Reactive Power schedule provided by the Transmission Operator but provide Generator Operators increased flexibility to deviate from voltage or Reactive Power schedules and operational modes where system-specific circumstances or events may require these deviations to protect reliability and prevent equipment damage.

- Requirements R3 and R4 remove unnecessary and overly burdensome communication requirements that provide little to no reliability benefit. Eliminating these notification requirements will enable Transmission Operators to focus resources on improving system monitoring and responding to voltage issues as they may arise in Real-time.

- Requirements R5 and R6 improve clarity by removing extraneous language (Requirement R5) and adopting consistent language throughout the requirement (Requirement R6), which will help responsible entities understand and more effectively apply these requirements.

For the reasons discussed herein, NERC respectfully requests that the Commission approve proposed Reliability Standards VAR-001-4 and VAR-002-3 as just, reasonable, not unduly discriminatory or preferential, and in the public interest.

[16] As further discussed in Section IV.C, this Commission directive was issued in reference to Reliability Standard VAR-002. However, the standard drafting team determined that this directive is more appropriately addressed in VAR-001-4, Requirement R5.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing should be addressed to the following:[17]

Charles A. Berardesco*
Senior Vice President and General Counsel
Holly A. Hawkins*
Assistant General Counsel
Shamai Elstein*
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, DC 20005
(202) 400-3000
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Valerie Agnew*
Director of Standards Development
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
valerie.agnew@nerc.net

III. BACKGROUND

A. Regulatory Framework

In FPA section 215,[18] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the nation's Bulk-Power System, and certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval.[19] All users, owners, and operators of the Bulk-Power System in the United States are subject to Commission-approved Reliability Standards.[20] The ERO must obtain Commission approval of each Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, as well as modifications to the Reliability

---

[17] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's Regulations, 18 C.F.R. § 385.203, to allow the inclusion of more than two persons on the service list in this proceeding.

[18] 16 U.S.C. § 824o.

[19] The Commission certified NERC as the ERO. *See* Order No. 672, *order on reh'g*, Order No. 672-A; ERO Certification Order, *supra* note 3.

[20] 16 U.S.C. § 824o(b)(1).

Standards,[21] and the Commission may order the ERO to submit new or modified Reliability Standards.[22]

The Commission has the regulatory responsibility to approve Reliability Standards that protect the reliability of the Bulk-Power System and to ensure that they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The Commission gives due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard.[23]

B. NERC Reliability Standards Development Procedure

NERC develops Reliability Standards in accordance with Section 300 of the NERC Rules of Procedure and the NERC Standard Processes Manual.[24] The Commission has found that the NERC Rules of Procedure provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards, and thus satisfy certain of the criteria for approving Reliability Standards.[25] The development process is open to any person or entity with a legitimate interest in the reliability of the Bulk-Power System. NERC considers all stakeholder comments and requires a vote by stakeholders as well as the NERC Board of Trustees to approve a Reliability Standard before NERC will submit the

---

21 18 C.F.R. § 39.5(a).

22 16 U.S.C. § 824o(d)(5).

23 16 U.S.C. § 824o(d)(2); 18 C.F.R. § 39.5(c)(1).

24 Rules of Procedure of the North American Electric Reliability Corporation, § 300 ("NERC Rules of Procedure"), *available at* http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx; Standard Processes Manual, v.3 (June 26, 2013), *available at* http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

25 ERO Certification Order at P 250.

Reliability Standard for Commission approval. NERC developed proposed Reliability Standards VAR-001-4 and VAR-002-3 in an open and fair manner and in accordance with this process.[26]

C. The Existing VAR Reliability Standards

1. Reliability Standard VAR-001-3

Currently enforceable Reliability Standard VAR-001-3 requires Transmission Operators to monitor, control and maintain voltage levels, reactive flows and reactive resources within certain limits in Real-time to protect equipment and the reliable operation of the Interconnection.[27] Under the existing requirements, [28] each Transmission Operator is required to:

- Individually and jointly with other Transmission Operators ensure that formal policies and procedures are developed, maintained and implemented for monitoring and controlling voltage levels and MVar flows within their individual areas and the areas of neighboring Transmission Operators (Requirement R1);
- Acquire sufficient reactive resources within its areas to protect voltage levels under normal and Contingency conditions (Requirement R2);
- Specify criteria to exempt generators from compliance with the voltage or Reactive Power schedule developed by the Transmission Operator in accordance with VAR-001-3, maintain a list of exempted generators, and notify Generator Owners of any exempted generators (Requirement R3);
- Specify a voltage or Reactive Power schedule at the interconnection between the generator facilities and Transmission Owner's facilities, provide the schedule to the associated Generator Operator, and direct it to comply with the schedule in automatic voltage control mode (Requirement R4);

[26] Order No. 672 at P 334.

[27] As noted above, VAR-001-3 also includes a regional variance applicable to Generator Operators in the Western Interconnection. Because NERC is not proposing any substantive changes to that regional variance, it is not discussed herein.

[28] The Commission approved retirement of Requirement R5 effective January 21, 2014. *See Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards*, Order No. 788, 145 FERC ¶ 61,147, at P 17 (2013).

- Know the status of all transmission Reactive Power resources and, when notified of the loss of an automatic voltage regulator ("AVR") control, direct the Generator Operator to maintain or change its voltage or Reactive Power schedule (Requirement R6);

- Operate or direct operations of devices to regulate transmission voltage and reactive flow (Requirement R7);

- Operate or direct operations of capacitive and inductive reactive resources within its area to maintain system and Interconnection voltages within established limits (Requirement R8);

- Maintain reactive resources to support its voltage under first Contingency conditions and disperse and locate these resources to allow for effective and quick application when Contingencies occur (Requirement R9);

- Correct and report SOL and IROL violations resulting from reactive resource deficiencies (Requirement R10);

- Consult with and provide documentation to Generator Owners about required tap changes, timeframes for completion, and technical justification for these changes (Requirement R11); and

- Direct corrective action necessary to prevent voltage collapse when reactive resources are insufficient.

Currently enforceable Reliability Standard VAR-001-3, however, does not address the following outstanding Commission directives from Order Nos. 693 and 724:

- Include Reliability Coordinators as responsible entities;[29]

- Address the power factor range at the interface between Load Serving Entities ("LSEs") and the Bulk-Power System;[30]

- Consider acceptable ranges of net power factors where LSEs receive service from the Bulk-Power System;[31]

- Specify and define requirements on "established limits" and "sufficient reactive resources" and identify voltage and Reactive Power margins to prevent voltage instability;[32]

---

29 Order No. 693 at P 1855.

30 *Id.* at P 1861.

31 *Id.* at PP 1860, 1862.

32 *Id.* at P 1868.

- Require the performance of periodic voltage stability analysis using online and offline techniques to assist Real-time operations;[33] and

- Ensure voltage schedules reflect sound engineering and operating judgment and experience.[34]

As discussed below, proposed Reliability Standard VAR-001-4 or other existing or pending Reliability Standards address these outstanding Commission directives.

2. Reliability Standard VAR-002-2b

Currently enforceable Reliability Standard VAR-002-2b requires that generators provide reactive and voltage control necessary to maintain voltage levels, reactive flows and reactive resources within applicable facility ratings to protect equipment and the reliable operation of the Interconnection. Under the existing requirements, each Generator Operator is required to:

- Operate in automatic voltage control mode unless it is exempted or the Generator Operator notifies its Transmission Operator that it is (1) operating the generator in start-up or shutdown mode pursuant to a Real-time communication or a procedure previously provided to the Transmission Operator, or (2) not operating the generator in automatic voltage control mode for a reason other than start-up or shutdown (Requirement R1);

- Maintain the voltage or Reactive Power schedule, unless otherwise exempted by the Transmission Operator, use an alternative method for controlling the generator voltage and Reactive Power output when a generator's AVR is out of service, and, when directed to modify voltage, provide an explanation to the Transmission Operator if it cannot meet the schedule (Requirement R2); and

- Notify its Transmission Operator as soon as practical, but within 30 minutes, of a status or capability change on any Reactive Power resource (generator or other), including the status of each AVR and power system stabilizer, and the expected duration of the identified change (Requirement R3).

Reliability Standard VAR-002-2b also requires each Generator Owner to:

- Provide tap-related information on step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage within 30

[33] *Id.* at P 1875.

[34] Order No. 724 at P 49.

calendar days of a request from the Transmission Operator and Transmission Planner (Requirement R4); and

- Ensure that transformer tap positions are changed according to the Transmission Operator's specifications, unless this action would violate safety, an equipment rating, or a regulatory or statutory requirement, in which case the Generator Owner must notify the Transmission Operator and justify why the Generator Owner is unable to comply (Requirement R5).

Currently enforceable Reliability Standard VAR-002-2b does not address the Commission's directive to consider an additional time frame associated with an "incident" of non-compliance with VAR-002.[35] As discussed below, this directive is addressed in proposed Reliability Standard VAR-001-4.

D. Procedural History of Project 2013-04 – Voltage and Reactive Control (VAR)

In February 2013, NERC initiated an informal development process to revive efforts to modify the existing VAR Reliability Standards to address the outstanding Commission directives from Order Nos. 693 and 724 related to those standards.[36] Participants in this informal process were industry subject matter experts, NERC staff, and FERC staff from the Office of Electric Reliability. The informal development group met numerous times between February 2013 and July 2013 to discuss the outstanding Commission directives and ways to improve the existing VAR Reliability Standards. The informal group also conducted industry outreach to obtain feedback on the existing standards.

After evaluating the VAR Reliability Standards and the Commission's directives, the informal group concluded that certain of the existing requirements and outstanding directives overlapped with or were duplicative of requirements in other Reliability Standards to maintain and operate within SOLs and IROLs or were otherwise unnecessary from a reliability

[35] Order No. 693 at PP 1883, 1885.

[36] In 2008, NERC initiated Project 2008-01 to address the directives from Order No. 693 related to the VAR Reliability Standards. That project was not completed due to project reprioritization.

perspective. To that end, the informal participants developed revised drafts of the VAR Reliability Standards to address Commission directives, eliminate duplicative or unnecessary requirements, and improve the quality and content of those existing requirements that are necessary to help maintain voltage stability on the Bulk-Power System.

As discussed further in Exhibit F, Project 2013-04 formally commenced on July 19, 2013 with the posting of a Standard Authorization Request ("SAR") along with the initial drafts of the proposed Reliability Standards developed by the informal participants for a 45-day comment period and ballot. A formal standard drafting team was formed following the posting of the SAR and the initial drafts of the proposed Reliability Standards.[37]

Following the close of the initial ballot, the standard drafting team addressed industry comments and posted second drafts of the proposed Reliability Standards on October 11, 2013 for an additional 45-day comment period and ballot. Proposed Reliability Standard VAR-001-4 received the requisite approval during the second ballot and was subsequently posted for a final ballot. The final ballot concluded on December 23, 2013 and received an approval rating of 75.35%. The NERC Board of Trustees approved proposed Reliability Standard VAR-001-4 on February 6, 2014.

The standard drafting team addressed additional industry comments on the second draft of proposed Reliability Standard VAR-002-3 and, on February 27, 2014, posted a third draft of the standard for a 45-day comment period and ballot. Proposed Reliability Standard VAR-002-3 received the requisite approval in the third ballot and was subsequently posted for a final ballot. The final ballot concluded on May 5, 2014 and received an approval rating of 88.26%. The NERC Board of Trustees approved proposed Reliability Standard VAR-002-3 on May 7, 2014.

[37] Exhibit G provides the standard drafting team roster.

IV. JUSTIFICATION FOR APPROVAL

As discussed below and in Exhibit C, proposed Reliability Standards VAR-001-4 and VAR-002-3 satisfy the Commission's criteria in Order No. 672 and are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The following sections provide: (1) the basis and purpose of the proposed Reliability Standards; (2) a discussion of the requirements in the proposed Reliability Standards; (3) an explanation of how the proposed Reliability Standards satisfy outstanding Commission directives from Order Nos. 693 and 724; and (4) a discussion of the enforceability of the proposed Reliability Standards.

A. Basis and Purpose of the Proposed Reliability Standards

Proposed Reliability Standards VAR-001-4 and VAR-002-3 replace and improve upon the prior versions of the standards (VAR-001-3 and VAR-002-2b) by addressing outstanding Commission directives from Order Nos. 693 and 724, improving reliability, clarifying language in certain requirements, and eliminating redundant or unnecessary requirements. As is further discussed in Section IV.C below, the outstanding Commission directives are addressed by proposed Reliability Standards VAR-001-4 and VAR-002-3, or already have been addressed in other currently enforceable or pending Reliability Standards. So as to avoid unnecessary redundancies or duplicative requirements, NERC does not propose to address in VAR-001-4 and VAR-002-3 those directives already addressed by other existing or pending Reliability Standards.

The standard drafting team sought to modify the currently enforceable Reliability Standards VAR-001-3 and VAR-002-2b to improve the clarity, quality, and content of the standards. These efforts include, but are not limited to, the following:

- VAR-001-4, Requirement R1 removes voltage level controls and monitoring obligations duplicative with other currently enforceable Reliability Standards and improves reliability by requiring Transmission Operators to (1) specify system voltage schedules,

which may be either a range or a target value with associated tolerance bands, and (2) coordinate with adjacent Transmission Operators and Reliability Coordinators regarding those system voltage schedules.

- VAR-001-4, Requirements R2 and R3 simplify and consolidate several existing requirements while ensuring sufficient reactive resources are scheduled (Requirement R2) and voltage support is provided (Requirement R3).

- VAR-001-4, Requirement R4 removes unnecessary compliance complexities and offers Transmission Operators the flexibility to tailor exemption criteria to area-specific needs.

- VAR-001-4, Requirement R5 improves transparency of Transmission Operator voltage or Reactive Power schedules for generators and provides the Transmission Operator the flexibility to develop notification requirements for deviations from those schedules based on the unique characteristics and needs of its system.

- VAR-001-4, Requirement R6 maintains and improves upon the existing tap setting requirements to avoid an adverse reliability impact caused by an improper tap setting that in turn may affect the Reactive Power output of a generator.

- VAR-002-3, Requirement R1 improves upon the prior version of the Reliability Standard by providing an option for certain Generator Operators to operate in modes other than automatic voltage control mode, as may be instructed by the Transmission Operator. Further, in addition to start-up or shutdown, Requirement R1 adds testing as a time when a generator need not operate in automatic voltage control mode or a different mode instructed by the Transmission Operator.

- VAR-002-3, Requirement R2 carries forward the requirement that Generator Operators maintain the generator voltage or Reactive Power schedule provided by the Transmission Operator pursuant to VAR-001-4, Requirement R5 but allows the Generator Operator to deviate from that schedule if it is exempted or satisfies the notification requirements established by the Transmission Operator under VAR-001-4, Requirement R5, Part 5.2. VAR-002-3, Requirement R2 also clarifies that Generator Operators that do not monitor voltage at the location specified in their voltage schedule provided by the Transmission Operator may convert the schedule to the voltage point monitored by the Generator Operator using a documented conversion methodology.

- VAR-002-3, Requirements R3 and R4 limit status change notification requirements to those changes lasting longer than 30 minutes because notification of changes resolved within a 30-minute window provides minimal, if any, reliability benefit.

- VAR-002-3, Requirements R5 and R6 include clarifying edits to remove an unnecessary sub-part (Requirement R5) and uniformly reference the applicable entity (Requirement R6).

B. Requirements in the Proposed Reliability Standards

1. Reliability Standard VAR-001-4

Proposed Reliability Standard VAR-001-4 consists of six requirements and is applicable to Transmission Operators and, for the WECC regional variance maintained and carried forward from Reliability Standard VAR-001-3, Generator Operators within the Western Interconnection. An explanation of the six requirements and the omission of certain VAR-001-3 requirements are provided below.[38]

VAR-001-4, Requirement R1

> **R1.** Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.
>
> **1.1.** Each Transmission Operator shall provide a copy of the voltage schedules (which is either a range or a target value with an associated tolerance band) to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.

Requirement R1 is intended to replace and simplify the currently-effective VAR-001-3, Requirement R1, which requires Transmission Operators, individually and jointly, to develop formal policies and procedures for controlling and monitoring voltage levels and MVar flows. In evaluating VAR-001-3, Requirement R1, the standard drafting team concluded that because controlling and monitoring voltage levels and MVar flows is already required by the Transmission Operations ("TOP") group of Reliability Standards, it should not be duplicated in proposed Reliability Standard VAR-001-4. Specifically, currently effective Reliability Standard TOP-004-2, Requirement R6 also requires "Transmission Operators, individually and jointly

[38] The WECC regional variance is not reproduced herein as it has not been substantively modified from the currently enforceable VAR-001-3 regional variance. Only non-material changes have been made to reference the replacement of VAR-001-4, Requirements R4 and R5, rather than VAR-001-3, Requirements R3 and R5.

with other Transmission Operators, [to] develop, maintain, and implement formal policies and procedures to provide for transmission reliability." That requirement specifies that the "policies and procedures shall address the execution and coordination of activities that impact inter- and intra-Regional reliability, including," among other things, "monitoring and controlling voltage levels and real and reactive power flows."

Additionally, currently effective TOP Reliability Standards require that Transmission Operators plan to meet SOLs and IROLs (TOP-002-2.1b, Requirement R10) and operate within SOLs and IROLs (TOP-004-2, Requirement R1).[39] As stated in the NERC Glossary, a SOL is defined as:

> the value (such as MW, MVar, Amperes, Frequency or Volts) that satisfies the most limiting of the prescribed operating criteria for a specified system configuration to ensure operation within acceptable reliability criteria. [SOLs] are based upon certain operating criteria. These include, but are not limited to: [1] Facility Ratings (Applicable pre- and post-Contingency equipment or facility ratings); [2] Transient Stability Ratings (Applicable pre- and post-Contingency Stability Limits); [3] Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability); and [4] System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits).[40]

Accordingly, to meet the obligations under Reliability Standards TOP-002-2.1b, Requirement R10 and TOP-004-2, Requirement R1 to plan to meet and operate within SOLs and IROLs, a Transmission Operator is required to monitor and control voltage levels and MVar flows. Failure to do so could lead to a violation of these requirements.

Similarly, monitoring and controlling voltage and MVar flows is fundamental to complying with TOP-004-2, Requirements R2 and R3, which require a Transmission Operator to

---

[39] Reliability Standard FAC-014-2, Requirement R2 requires a Transmission Operator to establish SOLs (as directed by its Reliability Coordinator) for its portion of the Reliability Coordinator Area that are consistent with its Reliability Coordinator's SOL Methodology.

[40] An IROL is defined in the NERC Glossary as "[a] SOL that, if violated, could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Bulk Electric System" (footnote omitted).

operate to protect against instability, uncontrolled separation, or cascading outages from (1) the most severe single contingency (Requirement R2), and (2) multiple outages, as specified by its Reliability Coordinator (Requirement R3). Failure to monitor and control voltage and MVar flows could result in a violation of these requirements.

Certain of the TOP Reliability Standards are currently being modified as part of a standards development project at NERC. While certain language and obligations from the existing TOP Reliability Standards may change, the obligation to monitor and control voltage levels and reactive flows will remain. Specifically, as proposed, draft Reliability Standards TOP-001-3 and TOP-002-4 would collectively require Transmission Operators to plan to meet and operate within SOLs and IROLs.[41] In addition, those draft Reliability Standards would require each Transmission Operator to (1) monitor facilities within its area and neighboring areas to maintain reliability in its area, and (2) perform a Real-time Assessment at least once every 30 minutes. To comply with these obligations, Transmission Operators must monitor and control voltage, as discussed above.

Because controlling and monitoring voltage and MVar flows is covered elsewhere, the standard drafting team modified VAR-001-4, Requirement R1 to only require that Transmission Operators (1) specify a system voltage schedule as part of its plan to operate with SOLs and IROLs, and (2) provide such schedules to adjacent Transmission Operators and applicable Reliability Coordinators, upon request. The requirement to specify a system voltage schedule as a range or a target value with an associated tolerance band will help ensure that the system maintains an appropriate voltage level in Real-time. The reactive behavior of any particular system depends on a myriad of local conditions which change over time. The intent of

[41] As of the date of this Petition, proposed Reliability Standards TOP-001-3 and TOP-002-4 have been posted for an initial comment period and ballot, which is scheduled to close on July 2, 2014.

Requirement R1 is not to mandate that Transmission Operators set and maintain a static voltage level; rather it is to require Transmission Operators to identify the acceptable voltage limits (either by identifying a range or a target value with an associated tolerance band) that supports reliable operations in Real-time.

The requirement to share the voltage schedule with neighboring Transmission Operators and Reliability Coordinators will allow for increased and improved coordination between neighboring areas. Given the interconnected nature of the Bulk-Electric System, voltage coordination is necessary to help ensure that sufficient Reactive Power is available to support both Real-time and day-ahead operations.

VAR-001-4, Requirement R2

> **R2.** Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load.

Requirement R2 modifies and consolidates the obligations in currently-effective VAR-001-3, Requirements R2 and R9 to require the scheduling of sufficient reactive resources. As noted above, the primary factor in maintaining voltage stability is having the appropriate amount of Reactive Power on the system. Proposed Requirement R2 helps ensure that sufficient reactive resources are online and scheduled in Real-time.

VAR-001-3, Requirements R2 and R9 require each Transmission Operator to (1) "acquire sufficient reactive resources . . . within its area to protect the voltage levels under normal and Contingency conditions" and (2) "maintain reactive resources . . . to support its voltage under first Contingency conditions," respectively. The standard drafting team concluded that these requirements should be combined into a single requirement that more directly states

the desired performance for ensuring that sufficient Reactive Power is on the system in Real-time to maintain voltage stability (*i.e.*, to "schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions").[42]

Requirement R2 also clarifies the language with respect to the manner in which Transmission Operators may schedule sufficient reactive resources (*e.g.*, through reactive generation scheduling, transmission line and reactive resource switching, and using controllable load). Consistent with the Commission's directive in Order No. 693,[43] Requirement R2 includes the use of controllable load in the non-exhaustive list of ways to provide sufficient reactive resources. As the Commission stated, "in many cases, load response and demand-side investment can reduce the need for reactive power capability in the system."[44]

VAR-001-4, Requirement R3

> **R3.** Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary.

Whereas Requirement R2 obligates the Transmission Operator to ensure that there are sufficient reactive resources online and scheduled, Requirement R3 requires that a Transmission Operator actually provide sufficient voltage support in Real-time by operating its own devices or directing others to do so.

Requirement R3 carries forward the obligation from VAR-001-3, Requirement R7. However, by deleting the phrase "be able to" Requirement R3 creates an affirmative obligation to operate or direct the operation of devices to regulate transmission voltage and reactive flow

---

42 VAR-001-4, Requirement R2.

43 Order No. 693 at P 1879.

44 *Id*.

when necessary.[45] Additionally, the standard drafting team concluded that there was no need to separately carry forward VAR-001-3, Requirement R8 because it was subsumed in proposed VAR-001-4, Requirement R3.

VAR-001-4, Requirement R4

> **R4.** The Transmission Operator shall specify the criteria that will exempt generators from: 1) following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any associated notifications.
>
> **4.1** If a Transmission Operator determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.

As discussed below, proposed Reliability Standard VAR-002-3 imposes requirements on the Generator Operator for providing reactive support, including: (1) following the voltage or Reactive Power schedule provided by the Transmission Operator; (2) operating its generator(s) in automatic voltage control mode; and (3) notifying the Transmission Operator of any deviations from the schedule or changes to the status of its voltage control mode. In certain circumstances, however, it may not be necessary or desired for a Generator Operator to comply with such requirements. For instance, a Generator Operator may need to be exempt from performance for the following system events, among others: (1) maintenance during shoulder months; (2) scenarios where two generators are located within close proximity and cannot both operate in voltage control mode; and (3) system voltage swings where it would harm reliability if all Generator Operators provided deviation notifications to their respective Transmission Operators at one time.

[45] VAR-001-3, Requirement R7 states as follows: "The Transmission Operator shall ***be able to*** operate or direct the operation of devices necessary to regulate transmission voltage and reactive flow" (emphasis added).

Requirement R4 carries forward the authority in currently enforceable Reliability Standard VAR-001-3, Requirement R3 for a Transmission Operator to exempt a Generator Operator from having to comply with all or some of its Reactive Power obligations. Proposed Requirement R4 clarifies that a Transmission Operator may exempt a Generator Operator from the following requirements: (1) complying with a voltage or Reactive Power schedule; (2) operating in automatic voltage control mode; and (3) certain notification requirements. Requirement R4 also allows each Transmission Operator to tailor its criteria for exemptions to its area's specific needs.

Further, Requirement R4 simplifies Reliability Standard VAR-001-3, Requirement R3 by removing the need for Transmission Operators to maintain a list of generators in its area that are exempt from following a voltage or Reactive Power schedule. Removal of this list requirement alleviates unnecessary compliance burdens and complexities related to how often to update and maintain these lists. Instead, proposed Requirement R4 focuses on whether the exemption criteria are transparent and whether the Transmission Owner notified the Generator Operator that it is exempt.

VAR-001-4, Requirement R5

> **R5.** Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the generator step-up transformer at the Transmission Operator's discretion.
>
> **5.1.** The Transmission Operator shall provide the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).
>
> **5.2.** The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage

or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).

5.3. The Transmission Operator shall provide the criteria used to develop voltage schedules [or] Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the Generator Operator within 30 days of receiving a request.

Requirement R5 carries forward the obligation from currently-effective Reliability Standard VAR-001-3, Requirement R4 that Transmission Operators must provide a voltage or Reactive Power schedule for each generator and direct the associated Generator Operator to comply with that schedule in automatic voltage control mode unless otherwise instructed or exempted. Proposed Requirement R5 modifies that requirement to clarify that a Transmission Operator may provide the voltage or Reactive Power schedule at either the high or low voltage side of the generator step-up transformer.[46] Specifying the location of the voltage or Reactive Power schedule provides a mechanism for the Generator Operator to convert the scheduled voltage to the voltage point it monitors. As discussed below, VAR-002-3, Requirement R2, Part 2.2 clarifies that if the Generator Operator does not monitor voltage at the location specified in the schedule provided by the Transmission Operator, the Generator Operator may use a conversion methodology for converting the scheduled voltage to the voltage point monitored by the Generator Operator.

As with the system level voltage schedule, the voltage or Reactive Power schedule provided to Generator Operators must be a range or a target value with an associated tolerance band. Specifying the voltage schedule as a range or as a target value with an associated tolerance

[46] VAR-003-1, Requirement R4 simply states that the Transmission Operator must "specify a voltage or Reactive Power schedule at the interconnection between the generator facility and the Transmission Operator's facilities" (footnote omitted).

band provides information that Generator Operators can use to set their control devices to appropriate settings to maintain operation within the specified tolerances.

Further, Part 5.2 requires Transmission Operators to provide Generator Operators the notification requirements for deviations from the voltage or Reactive Power schedule. Part 5.2 ensures that Generator Operators are aware of the notification requirements for deviating from the required schedule while also providing Transmission Operators the flexibility to develop notification requirements that best suit their needs.

Lastly, Requirement R5 provides for increased transparency of the Transmission Operator's development of voltage and Reactive Power schedules. Part 5.3 requires Transmission Operators to provide Generator Operators the criteria for developing the voltage or Reactive Power schedule, if requested. Part 5.3 will help ensure that the Transmission Operator has a technical basis for setting the required voltage and Reactive Power schedule that takes into account system needs and any limitations of the specific generator. Providing such criteria may alleviate some operational disputes between Transmission Operators and Generator Operators regarding the technical justifications for the voltage and Reactive Power schedules.

VAR-001-4, Requirement R6

> **R6.** After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.

Requirement R6 updates currently-effective VAR-001-3, Requirement R11 to allow for scheduling consultation. Because an improper tap setting may affect the amount of VARs produced by a generator, the standard drafting team concluded that this requirement needed to be included in proposed Reliability Standard VAR-001-4.

Omitted VAR-001-3 Requirements

Several currently enforceable requirements from Reliability Standard VAR-001-3 have been omitted from proposed Reliability Standard VAR-001-4 because they have been retired (Requirement R5)[47] or are duplicative with other currently enforceable and pending Reliability Standards (existing Requirements R6, R10 and R12). On this last category of omitted requirements:

- VAR-001-3, Requirement R6 is duplicative of currently enforceable TOP-006-2, Requirement R1, which requires that Transmission Operators know the status of all generating and transmission resources, including Reactive Power resources, available for use. In addition, TOP-006-2, Requirement R2 requires, among other things, each Reliability Coordinator, Transmission Operator, and Balancing Authority to monitor applicable real and reactive power flows, voltage, and the status of rotating and static reactive resources, which requires monitoring of power system stabilizers ("PSS") in areas that rely on PSS equipment. The TOP Reliability Standards currently in development would require each Transmission Owner to monitor Facilities, sub-100 kV facilities, and the status of Special Protection Systems within its area and neighboring areas, as needed to maintain reliability within its Transmission Operator Area.[48] This monitoring activity requires Transmission Operators to know the status of Reactive Power resources.

- VAR-001-3, Requirement R10 is duplicative of currently enforceable TOP-004-2, Requirement R1, which provides that Transmission Operators shall operate within SOLs and IROLs. This would include taking action to correct SOL and IROL violations resulting from reactive resource deficiencies. Additionally, TOP-004-2, Requirement R4 requires Transmission Operators that enter an unknown operating state (*i.e.*, any state for which valid operating limits have not been determined) to restore operations to respect proven reliable power system limits within 30 minutes. The TOP Reliability Standard currently in development will continue to require Transmission Operators to operate within SOLs and IROLs and take action to correct and report such violations.[49]

---

[47] The Commission approved the retirement of Requirement R5 of VAR-001-2. *See* Order No. 788 at P 17 (accepting retirement of VAR-001-2, Requirement R5, effective January 21, 2014, because it is redundant with the *pro forma* Open Access Transmission Tariff and any resulting reliability gap is addressed by currently enforceable VAR-001-3, Requirement R2). (Currently effective VAR-001-3, Requirement R5 also notes that Requirement R5 will be retired effective January 21, 2014.) Proposed VAR-001-4, Requirement R2 will also achieve the reliability objective envisioned by retired Requirement R5.

[48] *See* draft Reliability Standard TOP-001-3, Requirement R10, *available at* http://www.nerc.com/pa/Stand/Pages/Project-2014-03-Revisions-to-TOP-and-IRO-Standards.aspx.

[49] *See* draft Reliability Standard TOP-001-3, Requirements R12–R15.

- VAR-001-3, Requirement R12 is also duplicative with requirements in TOP-004-2 to take corrective action, including load-shedding, to operate within SOLs and IROLs and prevent voltage collapse. The TOP Reliability Standard currently in development will continue to require Transmission Operators to take action to prevent voltage collapse.[50] Additionally, Reliability Standard EOP-003-2 covers plans for load shedding to prevent voltage collapse.

2. Reliability Standard VAR-002-3

Proposed Reliability Standard VAR-002-3 consists of six requirements and is applicable to Generator Operators and Generator Owners. An explanation of each of the six requirements is provided below.

VAR-002-3, Requirement R1

> **R1.** The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode as instructed by the Transmission Operator unless: 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following:
>
> - That the generator is being operated in start-up,[FN1] shutdown,[FN2] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
>
> - That the generator is not being operated in automatic voltage control mode or in the control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing.
>
> [FN1: Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.]
>
> [FN2: Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.]

Requirement R1 carries forward the obligation in currently effective VAR-002-2b, Requirement R1 for Generator Operators to operate generators in automatic voltage control

[50] *See id.*

mode, but modifies the requirement to allow a Generator Operator to operate in a different control mode if instructed by the Transmission Operator. From a reliability perspective, it is beneficial for generators to operate in automatic voltage control mode. Once set in "voltage controlling" mode, the AVR should automatically adjust to voltage swings within its pre-defined voltage band. A different control mode, however, may be appropriate in certain circumstance. For instance, where two large generators are located within close proximity, if both generators operate in voltage control mode it may result in undesirable effects, such as voltage swings due to the units competing to control voltage. In such instances, to improve voltage regulation and stability, it may be beneficial to allow one of the units to be in automatic voltage control mode while directing the other unit to operate in an alternative mode. Proposed Reliability Standard VAR-002-3 therefore provides for a default mode of operation (*i.e.*, automatic voltage control mode) while also providing flexibility for Transmission Operators and Generator Operators to coordinate if a different control mode would be more effective.

Additionally, Requirement R1 modifies currently effective VAR-002-2b, Requirement R1 to add testing as a time when a generator need not operate in automatic voltage control mode or a different mode instructed by the Transmission Operator.

VAR-002-3, Requirement R2

> **R2.** Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[FN3] (within each generating Facility's capabilities[FN4]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator.
>
> > **2.1.** When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

2.2. When instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

[FN3: The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.]

[FN4: Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a generator is operating in manual control, reactive power capability may change based on stability considerations.]

Requirement R2 carries forward the affirmative obligation from VAR-003-1, Requirement R2 that the Generator Operator maintain the voltage or Reactive Power schedule provided by the Transmission Operator, unless the Transmission Operator exempts the Generator Operator from doing so. Proposed Requirement R2 adds that the Generator Operator need not comply with the schedule if it satisfies the notification requirements for deviations established by the Transmission Operator under Reliability Standard VAR-001-4, Requirement R5, Part 5.2. By removing prescriptive notification requirements for the entire continent and providing additional flexibility, proposed Requirement R2, together with VAR-001-4, Requirement R5, Part 5.2, allows each Transmission Operator to determine the notification requirements for each of its respective Generator Operators based on system requirements and generator needs.

Additionally, proposed Requirement R2 includes a new Part 2.3 to allow Generator Operators that do not monitor voltage at the location specified in their voltage schedule provided by the Transmission Operator to convert the schedule to the voltage point monitored by the Generator Operator. As noted above, proposed Reliability Standard VAR-001-4, Requirement

R5 clarifies that the Transmission Operator may specify the schedule at either the high or low voltage side of the generator step-up transformer. Part 2.3 of proposed VAR-002-3 was included to allow a generator to continue monitoring voltage based on existing equipment, provided it has a methodology for conversion. There are many ways to convert the voltage schedule, including the development of voltage regulation curves for the transformers or the use of straight ratio conversion. This standard provides Generator Operators with the ability to meet a voltage schedule based on metering equipment while providing the necessary voltage support.

VAR-002-3, Requirements R3 and R4

> **R3.** Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within 30 minutes of such change, then the Generator Operator is not required to notify the Transmission Operator of the status change.
>
> **R4.** Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within 30 minutes of the Generator Operator becoming aware of such change, then the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability.

Proposed Requirements R3 and R4 separate the notification requirements in currently-effective VAR-002-2b, Requirement R3 into two requirements: (1) for AVR/PSS status changes (proposed Requirement R3), and (2) for reactive capability changes (proposed Requirement R4). Each of the proposed requirements provides for a 30-minute window to allow a Generator Operator time to resolve an issue before having to notify the Transmission Operator of a change. For example, proposed Requirement R3 limits the notifications required when an AVR goes out of service and quickly comes back in service (*i.e.*, within 30 minutes) because notification of this type of status change provides little to no benefit to reliability. For the same reason, proposed

Requirement R3 also removes existing Part 3.1, which requires that the Generator Operator provide an estimate for the expected duration of the status change.

Proposed Requirement R4 also limits the notifications required when a reactive capability change occurs and is quickly restored (*i.e.*, within 30 minutes) because notification of this type of status change provides little to no benefit to reliability. Proposed Requirement R4 improves VAR-002-2b, Requirement R3, which requires notification as soon as the reactive capability change occurs, to allow Generator Operators to report reactive capability changes after they become aware of the change. Proposed Requirement R4 also removes existing Part 3.2, which requires that the Generator Operator provide an estimate for the expected duration of the status change.

VAR-002-3, Requirement R5

R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request.

5.1. For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

5.1.1. Tap settings.

5.1.2. Available fixed tap ranges.

5.1.3. Impedance data.

Requirement R5 maintains most of currently-effective VAR-002-2b, Requirement R4 because of the importance of accurate tap settings. That is, if the tap setting is not properly set, then the VARs available from a particular generator may be affected. Proposed Requirement R5 removes existing Sub-part 4.1.4, which requires that a Generator Owner provide "[t]he +/- voltage range with step-change in % for load-tap changing transformers." This percentage

information is extraneous because tap settings, available fixed tap ranges and impedance data already are required[51] and can be used to calculate the step-change percentage, if needed.

VAR-002-3, Requirement R6

> **R6.** After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement.
>
> > **6.1.** If the Generator Owner cannot comply with the Transmission Operator's specifications, the Generator Owner shall notify the Transmission Operator and shall provide the technical justification.

Requirement R6 maintains most of currently-effective VAR-002-2b, Requirement R5 due to the importance of accurate tap settings, as explained above. However, Requirement R6 updates VAR-002-2b, Requirement R5 to clarify that the requirement and corresponding part apply to the same functional entity (Generator Owners).[52]

C. Proposed VAR-001-4 and VAR-002-3 Satisfy Outstanding Commission Directives

Project 2013-04 was initiated to address outstanding Commission directives from Order Nos. 693 and 724. The following is a discussion of each outstanding directive and the manner in which proposed Reliability Standards VAR-001-4 and VAR-002-3 address them.[53]

Applicability to Reliability Coordinators: In Order No. 693, the Commission directed NERC to modify Reliability Standard VAR-001 to "include reliability coordinators as applicable

---

[51] VAR-002-2b, Requirement R4, Sub-parts 4.1.1–4.1.3; VAR-002-3, Requirement R5, Sub-parts 5.1.1–5.1.3.

[52] Existing Requirement R5 references "Generator Owner" in Requirement R5 and "Generator Operator" in Part 5.1. Proposed Requirement R6 modifies the reference to "Generator Operator" in Part 5.1 to reference "Generator Owner" in what is now Part 6.1.

[53] Since the issuance of Order No. 693, the Commission withdrew its directives from paragraphs 1863 and 1869 of Order No. 693 related to the VAR Reliability Standards. *Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards*, 145 FERC ¶ 61,147 at PP 25–26, Att. A (2013).

entities and include a new requirement(s) that identifies the reliability coordinator's monitoring responsibilities."[54] The Commission reasoned that because "a reliability coordinator is the highest level of authority overseeing the reliability of the Bulk-Power System it is important to include the reliability coordinator as an applicable entity to assure that adequate voltage and reactive resources are being maintained."[55] Because the Interconnection Reliability Operations and Coordination ("IRO") group of Reliability Standards address Reliability Coordinator monitoring functions, the standard drafting team concluded that any additional requirements on the Reliability Coordinator monitoring function regarding voltage should be addressed in the IRO Reliability Standards. There is currently a NERC standards development project, Project 2014-03 – Revisions to TOP and IRO Standards, which is modifying the IRO Reliability Standards. The standard drafting team for that project is considering whether any revisions are necessary to address this directive.[56] Therefore, NERC does not propose to apply VAR-001-4 to Reliability Coordinators or develop any additional VAR-001-4 requirements applicable to Reliability Coordinators at this time.

Reactive Power requirements for LSEs: As directed by the Commission,[57] NERC addressed Reactive Power requirements for LSEs on a comparable basis with purchasing-selling

---

[54] Order No. 693 at P 1855.

[55] *Id*.

[56] Specifically, the drafting team for Project 2014-03 has proposed a new IRO-002-4, Requirement R4, which provides:

> Each Reliability Coordinator shall monitor Facilities within its Reliability Coordinator Area and neighboring Reliability Coordinator Areas to determine any potential [SOL and IROL] exceedances within its Reliability Coordinator Area, including sub-100 kV facilities needed to make this determination and the status of Special Protection Systems in its Reliability Coordinator Area.

[57] Order No. 692 at P 1858.

entities in Reliability Standard VAR-001-2, Requirement R5.[58] Subsequently, the Commission approved retirement of the requirement addressing this directive because the directive is effectively addressed in Schedule 2 (Reactive Supply and Voltage Control from Generation or Other Sources Service) of the Commission's *pro forma* Open Access Transmission Tariff.[59] As such, NERC does not propose to address this directive in the proposed Reliability Standards.

Power factor range at the interface between LSEs and the Bulk-Power System: The Commission directed NERC to develop a modification to the VAR Reliability Standards "to address the power factor range at the interface between LSEs and the Bulk-Power System."[60] The Commission was concerned that during high loads, if the power factor at the interface between many LSEs and the Bulk-Power System is so low as to result in low voltages at key busses on the Bulk-Power System, then there is risk for voltage collapse. Since the issuance of this directive, however, other Reliability Standards approved by the Commission address this issue. Specifically, Reliability Standard TPL-001-4, which has been approved by the Commission and subject to future enforcement, requires that system models include Real and reactive Load forecasts.[61] These system model inputs provide the appropriate power factors to be maintained. Additionally, Reliability Standard FAC-001-1 requires that each Transmission Owner and applicable Generator Owner provide a written summary of its plan to achieve the required system performance for "Voltage, Reactive Power, and ***power factor control***."[62] Because currently enforceable Reliability Standards TPL-001-4 and FAC-001-1 address the

---

[58] *NERC Petition for Approval of Proposed Modifications to Reliability Standards BAL-002-1; EOP-002-3; FAC-002-1; MOD-021-2; PRC-004-2; and VAR-001-2*, 134 FERC ¶ 61,015 (2011).

[59] Order No. 788 at P 17.

[60] Order No. 693 at P 1861.

[61] TPL-001-4, Requirement R1, Part 1.1.4, *available at* http://www.nerc.com/files/TPL-001-4.pdf.

[62] *See* FAC-001-1, Requirement R3, Part 3.1.9, *available at* http://www.nerc.com/files/FAC-001-1.pdf (emphasis added).

appropriate power factors to be maintained, the VAR standard drafting team determined it would be duplicative and unnecessary for reliability purposes to add the same or similar requirements to proposed Reliability Standards VAR-001-4 and VAR-002-3.

Consideration of acceptable ranges of net power factor range: The Commission directed NERC to consider the difficulty of reaching "an agreement on acceptable ranges of net power factors at the interfaces where LSEs receive service from the Bulk-Power System because the acceptable range of power factors at any particular point on the electrical system varies based on many location-specific factors."[63] The standard drafting team considered this directive carefully and determined that it has been addressed by the interconnection process and related agreements, as well as by currently enforceable Reliability Standards TPL-001-4 and FAC-001-1, as discussed above. Therefore, the standard drafting team did not include any additional language to proposed Reliability Standards VAR-001-4 and VAR-002-3 to address this directive.

Detailed and definitive requirement on established limits and sufficient reactive resources: The Commission directed NERC to "include more detailed and definitive requirements on 'established limits' and 'sufficient reactive resources' and identify acceptable margins (*i.e.*, voltage and/or reactive power margins) above voltage instability points to prevent voltage instability and to ensure reliable operation."[64] The Commission, in part, was addressing concerns that the Transmission Operator should be required to have a technical basis for setting the required voltage schedule that takes into account system needs and any limitations of the specific generator.[65] Proposed Reliability Standard VAR-001-4 addresses this concern by requiring Transmission Operators to (1) share their system voltage schedules with their

63 Order No. 693 at PP 1860, 1862.

64 *Id*. at P 1868.

65 *See id*. at P 1864.

Reliability Coordinators and adjacent Transmission Operators (Requirement R1, Part 1.1), and (2) provide Generator Operators the criteria used to develop generator-specific voltage and Reactive Power schedules (Requirement R5, Part 5.3). This increased transparency will help ensure that Transmission Operators have a technical basis for setting system-wide and generator specific voltage and Reactive Power schedules that takes into account system needs and any limitations of the specific generator.

Additionally, the Commission stated that "the Reliability Standard would benefit from having more defined requirements that clearly define what voltage limits are used and how much reactive resources are needed to ensure voltage instability will not occur under normal and emergency conditions."[66] Currently enforceable FAC and TOP Reliability Standards approved by the Commission following the issuance of Order No. 693, however, address this directive by requiring entities to develop methodologies for establishing SOLs and IROLs that include detailed and definitive requirements for voltage limits and margins. Specifically, Reliability Standard FAC-011-2, Requirement R1 requires the Reliability Coordinator to have a documented methodology for use in developing SOLs (the "SOL Methodology") within its Reliability Coordinator Area for use in the operations horizon.[67] Among other things, the SOL Methodology must include a requirement that SOLs provide BES performance consistent with maintaining voltage stability.[68]

---

[66] *Id*. at P 1870.

[67] Reliability Standard FAC-010-2.1 requires the Reliability Coordinator to have a documented SOL Methodology for use in the planning horizon.

[68] Specifically, FAC-011-2, Requirement R2 provides that:

> [t]he Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following:

continued . . .

Reliability Standard FAC-014-2 then requires (1) each Reliability Coordinator to ensure that SOLs, including IROLs, for its Reliability Coordinator Area are established and consistent with its SOL Methodology, and (2) each Transmission Operator to establish SOLs (as directed by its Reliability Coordinator) for its portion of the Reliability Coordinator Area that are consistent with its Reliability Coordinator's SOL Methodology.

These FAC Reliability Standards operate in tandem with the TOP Reliability Standards, which, as discussed above, require that each Transmission Operator plan to meet and operate within SOLs and IROLs. The standard drafting team determined that these currently enforceable FAC and TOP Reliability Standards collectively provide sufficient detail on "established limits" and margins, and it was unnecessary to include any additional definitive and detailed requirements in VAR-001-4 or VAR-002-3 to address voltage instability and ensure reliable operations. The standard drafting team determined, however, that because acceptable voltage limits and the level of sufficient Reactive Power necessary to maintain voltage depends on the unique characteristics of each system, the proposed Reliability Standards cannot dictate a specific, "one-size-fits-all" approach to determining what constitutes a sufficient level of Reactive Power. Rather, the SOL Methodologies developed by Reliability Coordinators under FAC-011-2 will provide the necessary detail tailored to the needs of the system in question.

Periodic voltage stability analysis: The Commission directed NERC to include a requirement to "perform voltage stability analysis periodically, using online techniques where

---

> R2.1. In the pre-contingency state, the BES shall demonstrate transient, dynamic and ***voltage stability***; all Facilities shall be within their Facility Ratings and within their thermal, voltage and ***stability limits***. . . .
>
> R2.2. [T]he system shall demonstrate transient, dynamic and ***voltage stability***; all Facilities shall be operating within their Facility Ratings and within their thermal, ***voltage and stability limits***; and Cascading or uncontrolled separation shall not occur.

(Emphasis added.)

commercially-available, and offline simulation tools where online tools are not available, to assist real-time operations."[69] The Commission stated that "[t]he ERO should consider the available technologies and software as it develops this modification to VAR-001-1 and identify a process to assure that the Reliability Standard is not limiting the application of validated software or other tools."[70] The standard drafting team concluded that requiring periodic voltage stability analysis in proposed VAR-001-4 was duplicative of requirements in the TOP group of Reliability Standards. Specifically, period voltage stability analysis is already required to comply with Reliability Standards TOP-002-2.1b, Requirements R10[71] and R11,[72] TOP-004-2, Requirement R6,[73] and TOP-006-2, Requirement R2.[74] Each of these existing Reliability Standards requires active planning and monitoring to operate within SOLs. Because periodic voltage stability analysis is an inherent component of these monitoring requirements, particularly TOP-002-2.1b, Requirement R11, the standard drafting team did not propose to duplicate these requirements in proposed Reliability Standards VAR-001-4 and VAR-002-3. As noted above, the TOP Reliability Standards currently in development propose to carry forward the obligation

---

69 Order No. 693 at P 1875.

70 *Id*.

71 Reliability Standard TOP-002-2.1b, Requirement R10 provides that "[e]ach Balancing Authority and Transmission Operator shall plan to meet all [SOLs] and [IROLs]."

72 Reliability Standard TOP-002-2.1b, Requirement R11 provides that the "Transmission Operator shall perform seasonal, next-day, and current-day Bulk Electric System studies to determine SOLs." The requirement also specifies that the "Transmission Operator shall update these Bulk Electric System studies as necessary to reflect current system conditions; and shall make the results of Bulk Electric System studies available to the Transmission Operators, Balancing Authorities (subject to confidentiality requirements), and to its Reliability Coordinator."

73 TOP-004-2, Requirement R6 provides that "Transmission Operators, individually and jointly with other Transmission Operators, shall develop, maintain, and implement formal policies and procedures to provide for transmission reliability. These policies and procedures shall address the execution and coordination of activities that impact inter- and intra-Regional reliability, including . . . [m]onitoring and controlling voltage levels and real and reactive power flows.

74 TOP-006-2, Requirement R2 requires that "[e]ach Reliability Coordinator, Transmission Operator, and Balancing Authority shall monitor applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, and status of rotating and static reactive resources."

to plan to meet and operate within SOLs and IROLs. Further, draft Reliability Standard TOP-002-4, Requirement R1 would require Transmission Operators to perform an Operational Planning Analysis that will allow it to assess whether its planned operations for the next day within its Transmission Operator Area will exceed any of its SOLs.[75] An Operational Planning Analyses would include a voltage stability analysis to assist Real-time operations.

NERC is not proposing to modify its Reliability Standards to require that entities perform periodic voltage stability analyses using online techniques where commercially-available or offline simulation tools where online tools are not available. From a Reliability Standards perspective, the goal is to ensure that relevant entities perform periodic voltage stability analyses in a manner that helps maintain reliable operation in Real-time, not to limit or dictate the techniques or tools used to perform the analysis. An entity may perform the analysis using online techniques or offline simulation tools based on their availability and effectiveness. To comply with the TOP Reliability Standards, however, the entity must show that it performed a voltage stability analysis using techniques and/or tools designed to assess voltage stability effectively.

Controllable load: The Commission directed NERC to include controllable load as a reactive resource.[76] As noted above, proposed Reliability Standard VAR-001-4, Requirement R2 addresses this directive as controllable load is included as a "sufficient reactive resource."

---

[75] The term "Operational Planning Analysis" is proposed to be modified as follows:

> An evaluation of projected system conditions to assess anticipated (pre-Contingency) and potential (post-Contingency) conditions for next-day operations. The evaluation shall reflect inputs including, but not limited to, load forecasts; generation output levels; Interchange; known Protection System and Special Protection System status or degradation; Transmission outages; generator outages; Facility Ratings; and identified phase angle and equipment limitations.

[76] Order No. 693 at P 1879.

VAR-002 non-compliance window: The Commission directed NERC to consider modifying VAR-002 to add a time frame associated with an "incident" of non-compliance with VAR-002.[77] The standard drafting team considered modifications to VAR-002, but could not reach consensus on establishing, or developing guidelines for defining, a continent-wide time frame that would apply to all generators under VAR-002. Rather, the directive was addressed in an equally effective and efficient manner in proposed Reliability Standard VAR-001-4, Requirement R5, which requires that each Transmission Operator provide its Generator Operators with applicable voltage or Reactive Power schedules and notification requirements for deviations from those schedules. This approach provides the necessary flexibility to each Transmission Operator to define time frames based on its unique system assessments and tailor deviation notifications to the voltage constraints experienced in a particular area.

Technically sound voltage schedules: In Order No. 724, the Commission remanded to NERC an interpretation of VAR-001-1, Requirement R4 to ensure voltage schedules "reflect sound engineering, as well as operating judgment and experience."[78] To address this directive, Requirement R5, Part 5.3 requires a Transmission Operator, upon request, to provide the Generator Operator the technical support for how a voltage schedule and an associated tolerance band was established. This increased transparency will help ensure that the schedules reflect sound engineering and operating judgment.

D. Enforceability of the Proposed Reliability Standards

Proposed Reliability Standards VAR-001-4 and VAR-002-3 include VRFs and VSLs. The VRFs and VSLs guide how NERC will enforce the requirements of the proposed Reliability

---

[77] *Id*. at PP 1883, 1885.

[78] Order No. 724 at P 49.

Standards and comport with NERC and Commission guidelines related to their assignment. Exhibit E provides a detailed review of the VRFs and VSLs, as well as analysis on how the VRFs and VSLs were determined using the NERC and Commission guidelines.

The proposed Reliability Standards also include measures that support each requirement promulgated thereunder by clearly identifying what is required for compliance and how the requirement will be enforced. These measures help ensure that the requirements will be enforced in a clear, consistent and non-preferential manner and without prejudice to any party.[79]

V. EFFECTIVE DATE

As described in the Implementation Plan attached hereto as Exhibit B, NERC respectfully requests that the Commission approve proposed Reliability Standards VAR-001-4 and VAR-002-3 and the retirement of VAR-001-3 and VAR-002-2b, effective on the first day of the first calendar quarter after Commission approval. The proposed implementation period will provide sufficient time for responsible entities to develop or modify their processes to transition from compliance with existing Reliability Standards VAR-001-3 and VAR-002-2b to proposed Reliability Standards VAR-001-4 and VAR-002-3.

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

VI. CONCLUSION

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

- Proposed Reliability Standards VAR-001-4 and VAR-002-3 and the associated elements included in Exhibit A, effective as proposed herein;
- The proposed Implementation Plan included in Exhibit B; and
- The retirement of the currently effective Reliability Standards VAR-001-3 and VAR-002-2b, effective as proposed herein.

Respectfully submitted,

/s/ Shamai Elstein

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Shamai Elstein
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, DC 20005
(202) 400-3000
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: June 9, 2014

Exhibit A-1

Proposed Reliability Standard VAR-001-4

A. Introduction

1. **Title:** Voltage and Reactive Control

2. **Number:** VAR-001-4

3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in Real-time to protect equipment and the reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators

   4.2. Generator Operators within the Western Interconnection (for the WECC Variance)

5. **Effective Date:**

   5.1. The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits. *[Violation Risk Factor: High] [Time Horizon: Operational Planning]*

1.1. Each Transmission Operator shall provide a copy of the voltage schedules (which is either a range or a target value with an associated tolerance band) to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.

M1. The Transmission Operator shall have evidence that it specified system voltage schedules using either a range or a target value with an associated tolerance band.

For part 1.1, the Transmission Operator shall have evidence that the voltage schedules (which is either a range or a target value with an associated tolerance band) were provided to its Reliability Coordinator and adjacent Transmission Operators within 30 days of a request. Evidence may include, but is not limited to, emails, website postings, and meeting minutes.

R2. Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operational Planning]*

M2. Each Transmission Operator shall have evidence of scheduling sufficient reactive resources based on their assessments of the system. For the operational planning time horizon, Transmission Operators shall have evidence of assessments used as the basis for how resources were scheduled.

R3. Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operational Planning]*

M3. Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as necessary in Real-time. This may include instructions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments.

R4. The Transmission Operator shall specify the criteria that will exempt generators from: 1) following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any associated notifications. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

4.1 If a Transmission Operator determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.

M4. Each Transmission Operator shall have evidence of the documented criteria for generator exemptions.

For part 4.1, the Transmission Operator shall also have evidence to show that, for each generator in its area that is exempt from: 1) following a voltage or Reactive Power schedule, 2) from having its

automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any notifications, the associated Generator Operator was notified of this exemption.

R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the generator step-up transformer at the Transmission Operator's discretion. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

5.1. The Transmission Operator shall provide the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).

5.2. The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).

5.3. The Transmission Operator shall provide the criteria used to develop voltage schedules Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the Generator Operator within 30 days of receiving a request.

M5. The Transmission Operator shall have evidence of a documented voltage or Reactive Power Schedule (which is either a range or a target value with an associated tolerance band).

For part 5.1, the Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the applicable Generator Operators, and that the Generator Operator was directed to comply with the schedule in automatic voltage control mode, unless exempted.

For part 5.2, the Transmission Operator shall have evidence it provided notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band). For part 5.3, the Transmission Operator shall have evidence it provided the criteria used to develop voltage schedules or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) within 30 days of receiving a request by a Generator Operator.

R6. After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with the requirement and that it consulted with the Generator Owner.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Transmission Operator shall retain evidence for Measures 1 through 6 for 12 months. The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operational Planning**	**High**	N/A	N/A	N/A	The Transmission Operator does not specify a system voltage schedule (which is either a range or a target value with an associated tolerance band).
R2	**Real-time Operations, Same-day Operations, and Operational Planning**	**High**	N/A	N/A	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an SOL.	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an IROL.
R3	**Real-time Operations, Same-day Operations, and Operational Planning**	**High**	N/A	N/A	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an SOL.	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an IROL.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Operations Planning**	**Lower**	N/A	N/A	The Transmission Operator has exemption criteria and notified the Generator Operator, but the Transmission Operator does not have evidence of the notification to the Generator Operator.	The Transmission Operator does not have exemption criteria.
R5	**Operations Planning**	**Medium**	N/A	The Transmission Operator does not provide the criteria for voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) after 30 days of a request.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) to all Generator Operators.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) to any Generator Operators. Or The Transmission Operator does not provide the Generator Operator with the notification requirements for deviations from the

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).
R6	**Operations Planning**	**Lower**	The Transmission Operator does not provide either the technical justification or timeframe for changing generator step-up tap settings.	N/A	N/A	The Transmission Operator does not provide the technical justification and the timeframe for changing generator step-up tap settings.

D. Regional Variances

The following Interconnection-wide variance shall be applicable in the Western Electricity Coordinating Council (WECC) and replaces, in their entirety, Requirements R4 and R5. Please note that Requirement R4 is deleted and R5 is replaced with the following requirements.

Requirements

E.A.13 Each Transmission Operator shall issue any one of the following types of voltage schedules to the Generator Operators for each of their generation resources that are on-line and part of the Bulk Electric System within the Transmission Operator Area: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- A voltage set point with a voltage tolerance band and a specified period.
- An initial volt-ampere reactive output or initial power factor output with a voltage tolerance band for a specified period that the Generator Operator uses to establish a generator bus voltage set point.
- A voltage band for a specified period.

E.A.14 Each Transmission Operator shall provide one of the following voltage schedule reference points for each generation resource in its Area to the Generator Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- The generator terminals.
- The high side of the generator step-up transformer.
- The point of interconnection.
- A location designated by mutual agreement between the Transmission Operator and Generator Operator.

E.A.15 Each Generator Operator shall convert each voltage schedule specified in Requirement E.A.13 into the voltage set point for the generator excitation system. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

E.A.16 Each Generator Operator shall provide its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals within 30 calendar days of request by its Transmission Operator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

E.A.17 Each Transmission Operator shall provide to the Generator Operator, within 30 calendar days of a request for data by the Generator Operator, its transmission equipment data and operating data that supports development of the voltage set point conversion methodology. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

E.A.18 Each Generator Operator shall meet the following control loop specifications if the Generator Operator uses control loops external to the Automatic Voltage Regulators (AVR) to manage MVar loading: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

E.A.18.1. Each control loop's design incorporates the AVR's automatic voltage controlled response to voltage deviations during System Disturbances.

E.A.18.2. Each control loop is only used by mutual agreement between the Generator Operator and the Transmission Operator affected by the control loop.

Measures[1]

M.E.A.13 Each Transmission Operator shall have and provide upon request, evidence that it provided the voltage schedules to the Generator Operator. Dated spreadsheets, reports, voice recordings, or other documentation containing the voltage schedule including set points, tolerance bands, and specified periods as required in Requirement E.A.13 are acceptable as evidence.

M.E.A.14 The Transmission Operator shall have and provide upon request, evidence that it provided one of the voltage schedule reference points in Requirement E.A.14 for each generation resource in its Area to the Generator Operator. Dated letters, e-mail, or other documentation that contains notification to the Generator Operator of the voltage schedule reference point for each generation resource are acceptable as evidence.

M.E.A.15 Each Generator Operator shall have and provide upon request, evidence that it converted a voltage schedule as described in Requirement E.A.13 into a voltage set point for the AVR. Dated spreadsheets, logs, reports, or other documentation are acceptable as evidence.

M.E.A.16 The Generator Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Transmission Operator it provided its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.E.A.17 The Transmission Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Generator Operator it provided data to support development of the voltage set point conversion methodology. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.E.A.18 If the Generator Operator uses outside control loops to manage MVar loading, the Generator Operator shall have and provide upon request, evidence that it met the control loop specifications in sub-parts E.A.18.1 through E.A.18.2. Design specifications with identified agreed-upon control loops, system reports, or other dated documentation are acceptable as evidence.

[1] The number for each measure corresponds with the number for each requirement, i.e. M.E.A.13 means the measure for Requirement E.A.13.

Violation Severity Levels

E #	Lower VSL	Moderate VSL	High VSL	Severe VSL
E.A.13	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to at least one generation resource but less than or equal to 5% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 5% but less than or equal to 10% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 10% but less than or equal to 15% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 15% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.
E.A.14	The Transmission Operator did not provide a voltage schedule reference point for at least one but less than or equal to 5% of the generation resources in the Transmission Operator area.	The Transmission Operator did not provide a voltage schedule reference point for more than 5% but less than or equal to 10% of the generation resources in the Transmission Operator Area.	The Transmission Operator did not a voltage schedule reference point for more than 10% but less than or equal to 15% of the generation resources in the Transmission Operator Area.	The Transmission Operator did not provide a voltage schedule reference point for more than 15% of the generation resources in the Transmission Operator Area.
E.A.15	The Generator Operator failed to convert at least one voltage schedule in Requirement E.A.13 into the voltage set point for the AVR for less	The Generator Operator failed to convert the voltage schedules in Requirement E.A.13 into the voltage set point for the AVR for 25% or more but	The Generator Operator failed to convert the voltage schedules in Requirement E.A.13 into the voltage set point for the AVR for 50% or more but less than 75% of	The Generator Operator failed to convert the voltage schedules in Requirement E.A.13 into the voltage set point for the AVR for 75% or more of the voltage schedules.

E #	Lower VSL	Moderate VSL	High VSL	Severe VSL
	than 25% of the voltage schedules.	less than 50% of the voltage schedules.	the voltage schedules.	
E.A.16	The Generator Operator provided its voltage set point conversion methodology greater than 30 days but less than or equal to 60 days of a request by the Transmission Operator.	The Generator Operator provided its voltage set point conversion methodology greater than 60 days but less than or equal to 90 days of a request by the Transmission Operator.	The Generator Operator provided its voltage set point conversion methodology greater than 90 days but less than or equal to 120 days of a request by the Transmission Operator.	The Generator Operator did not provide its voltage set point conversion methodology within 120 days of a request by the Transmission Operator.
E.A.17	The Transmission Operator provided its data to support development of the voltage set point conversion methodology than 30 days but less than or equal to 60 days of a request by the Generator Operator.	The Transmission Operator provided its data to support development of the voltage set point conversion methodology greater than 60 days but less than or equal to 90 days of a request by the Generator. Operator.	The Transmission Operator provided its data to support development of the voltage set point conversion methodology greater than 90 days but less than or equal to 120 days of a request by the Generator. Operator.	The Transmission Operator did not provide its data to support development of the voltage set point conversion methodology within 120 days of a request by the Generator Operator.

E #	Lower VSL	Moderate VSL	High VSL	Severe VSL
E.A.18	N/A	The Generator Operator did not meet the control loop specifications in EA18.2 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.	The Generator Operator did not meet the control loop specifications in EA18.1 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.	The Generator Operator did not meet the control loop specifications in EA18.1 through EA18.2 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

Rationale:

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

Rationale for R1:

Paragraph 1868 of Order No. 693 requires NERC to add more "detailed and definitive requirements on “established limits” and “sufficient reactive resources”, and identify acceptable margins (i.e. voltage and/or reactive power margins)." Since Order No. 693 was issued, however, several FAC and TOP standards have become enforceable to add more requirements around voltage limits. More specifically, FAC-011 and FAC-014 require that System Operating Limits (SOLs) and reliability margins are established. The NERC Glossary definition of SOLs includes both: 1) Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) and 2*)* System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits). Therefore, for reliability reasons Requirement R1 now requires a Transmission Operator (TOP) to set voltage or Reactive Power schedules with associated tolerance bands. Further, since neighboring areas can affect each other greatly, each TOP must also provide a copy of these schedules to its Reliability Coordinator (RC) and adjacent TOP upon request.

Rationale for R2:

Paragraph 1875 from Order No. 693 directed NERC to include requirements to run voltage stability analysis periodically, using online techniques where commercially available and offline tools when online tools are not available. This standard does not explicitly require the periodic voltage stability analysis because such analysis would be performed pursuant to the SOL methodology developed under the FAC standards. TOP standards also require the TOP to operate within SOLs and Interconnection Reliability Operating Limits (IROL). The VAR standard drafting team (SDT) and industry participants also concluded that the best models and tools are the ones that have been proven and the standard should not add a requirement for a responsible entity to purchase new online simulations tools. Thus, the VAR SDT simplified the requirements to ensuring sufficient reactive resources are online or scheduled. Controllable load is specifically included to answer FERC's directive in Order No. 693 at Paragraph 1879.

Rationale for R3:

Similar to Requirement R2, the VAR SDT determined that for reliability purposes, the TOP must ensure sufficient voltage support is provided in Real-time in order to operate within an SOL.

Rationale for R4:

The VAR SDT received significant feedback on instances when a TOP would need the flexibility for defining exemptions for generators. These exemptions can be tailored as the TOP deems necessary for the specific area's needs. The goal of this requirement is to provide a TOP the ability to exempt a Generator Operator (GOP) from: 1) a voltage or Reactive Power schedule, 2) a setting on the AVR, or 3) any VAR-002 notifications based on the TOP's criteria. Feedback from the industry detailed many system events that would require these types of exemptions which included, but are not limited to: 1) maintenance during shoulder months, 2) scenarios where two units are located within close proximity and both cannot be in voltage control mode, and 3) large system voltage swings where it would harm reliability if all GOP were to notify their respective TOP of deviations at one time. Also, in an effort to improve the requirement, the sub-requirements containing an exemption list were removed from the currently enforceable standard because this created more compliance issues with regard to how often the list would be updated and maintained.

Rationale for R5:

The new requirement provides transparency regarding the criteria used by the TOP to establish the voltage schedule. This requirement also provides a vehicle for the TOP to use appropriate granularity when setting notification requirements for deviation from the voltage or Reactive Power schedule. Additionally, this requirement provides clarity regarding a "tolerance band" as specified in the voltage schedule and the control dead-band in the generator's excitation system.

Voltage Schedule tolerances are the bandwidth that accompanies the voltage target in a voltage schedule, should reflect the anticipated fluctuation in voltage at the Generation Operator's facility during normal operations, and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a Generation Operator's automatic voltage regulator's control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

Rationale for R6:

Although tap settings are first established prior to interconnection, this requirement could not be deleted because no other standard addresses when a tap setting must be adjusted. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	August 2, 2006	BOT Adoption	Revised
1	June 18, 2007	FERC approved Version 1 of the standard.	Revised
1	July 3, 2007	Added “Generator Owners” and “Generator Operators” to Applicability section.	Errata
1	August 23, 2007	Removed “Generator Owners” and “Generator Operators” to Applicability section.	Errata
2	August 5, 2010	Adopted by NERC Board of Trustees; Modified to address Order No. 693 Directives contained in paragraphs 1858 and 1879.	Revised
2	January, 10 2011	FERC issued letter order approving the addition of LSEs and Controllable Load to the standard.	Revised
3	May 9, 2012	Adopted by NERC Board of Trustees; Modified to add a WECC region variance	Revised
3	June 20, 2013	FERC issued order approving VAR-001-3	Revised
3	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	Revised
4	February 6, 2014	Adopted by NERC Board of Trustees	Revised

A. Introduction

1. **Title:** Voltage and Reactive Control

2. **Number:** VAR-001-34

3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real-time to protect equipment and the reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators.

   4.2. Purchasing-Selling Entities.

   4.3. Load Serving Entities.

   4.4.2. Generator Operators within the Western Interconnection. (for the WECC Variance)

5. **(Proposed) Effective Date:**

   5.1. The standard shall become effective on the first day of the first calendar quarter six months after the date that the standard is approved by an applicable regulatory governmental authority or as otherwise provided for in a jurisdiction where approval; or in those jurisdictions where no regulatory approval by an applicable governmental authority is required, for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter six months after the date the standard is adopted by the NERC Board of Trustees' adoption Trustees or as otherwise provided for in that jurisdiction.

B. Requirements

Each Transmission Operator, individually and jointly Measures

R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with other an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits. *[Violation Risk Factor: High] [Time Horizon: Operational Planning]*

1.1. Each Transmission Operator shall provide a copy of the voltage schedules (which is either a range or a target value with an associated tolerance band) to its Reliability Coordinator and adjacent Transmission Operators, shall ensure that formal policies and procedures are developed, maintained, and implemented for monitoring within 30 calendar days of a request.

M1. The Transmission Operator shall have evidence that it specified system voltage schedules using either a range or a target value with an associated tolerance band.

1.1. For part 1.1, the Transmission Operator shall have evidence that the voltage schedules (which is either a range or a target value with an associated tolerance band) were provided to its Reliability Coordinator and controlling voltage levels and Mvar flows within their individual areas and with the areas of neighboringadjacent Transmission Operators.

Each Transmission Operator shall acquire sufficient reactive resources — which within 30 days of a request. Evidence may include, but is not limited to, emails, website postings, and meeting minutes.

R2. Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling;, transmission line and reactive resource switching;,, and using controllable load — within its area to protect the voltage levels under normal. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and* Contingency conditions. This includes the *Operational Planning]*

M2. Each Transmission Operator's shareOperator shall have evidence of the scheduling sufficient reactive requirementsresources based on their assessments of interconnectingthe system. For the operational planning time horizon, Transmission Operators shall have evidence of assessments used as the basis for how resources were scheduled.

R2.R3. Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission circuits.voltage and reactive flow as necessary. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operational Planning]*

M3. Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as necessary in Real-time. This may include instructions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments.

1.3. The Transmission Operator shall specify the criteria that exemptswill exempt generators from compliance with the requirements defined in Requirement 4, and Requirement 6.1.

R3.1.R4. Each Transmission Operator shall maintain a list of generators in its area that are exempt from : 1) following a voltage or Reactive Power schedule. , 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any associated notifications. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

R3.2.4.1 For eachIf a Transmission Operator determines that a generator that is on thishas satisfied the exemption list, the Transmission Operatorcriteria, it shall notify the associated Generator Owner. Operator.

M4. Each Transmission Operator shall have evidence of the documented criteria for generator exemptions.

For part 4.1, the Transmission Operator shall also have evidence to show that, for each generator in its area that is exempt from: 1) following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any notifications, the associated Generator Operator was notified of this exemption.

R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule [1](which is either a range or a target value with an associated tolerance band) at either the interconnection betweenhigh voltage side or low voltage side of the generator facility andstep-up transformer at the Transmission Owner's facilities to be maintained by each generator. Operator's discretion. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R4.5.1. The Transmission Operator shall provide the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).

1.7. Each Purchasing-Selling Entity and Load-Serving Entity shall arrange for (self-provide or purchase) reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching;, and controllable load – to satisfy its reactive requirements identified by its Transmission Service Provider. (Retirement approved by FERC effective January 21, 2014.)

1.8. The Transmission Operator shall know the status of all transmission provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power resources, including the status of voltage regulators and power system stabilizers.

R6.1.5.2. When notified of the loss of an automatic voltage regulator control, the Transmission Operator shall direct the Generator Operator to maintain or change either its voltage schedule or its Reactive Power schedule.(which is either a range or a target value with an associated tolerance band).

1.10. The Transmission Operator shall be able to operate or directprovide the operation of devices necessary to regulate transmissioncriteria used to develop voltage and reactive flow.

R8.5.3. Each Transmissionschedules Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the Generator Operator shall operate or

[1] The voltage schedule is a target voltage to be maintained within a tolerance band during a specified period.

~~direct the operation of capacitive and inductive reactive resources within its area – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; controllable load; and, if necessary, load shedding – to maintain system and Interconnection voltages within established limits~~within 30 days of receiving a request.

~~**1.0.** Each Transmission Operator shall maintain reactive resources – which may include, but is not limited to, reactive generation scheduling; transmission line and reactive resource switching; and controllable load – to support its voltage under first Contingency conditions.~~

~~**2.0.** Each Transmission Operator shall disperse and locate the reactive resources so that the resources can be applied effectively and quickly when Contingencies occur.~~

~~**3.0.** Each Transmission Operator shall correct IROL or SOL violations resulting from reactive resource deficiencies (IROL violations must be corrected within 30 minutes) and complete the required IROL or SOL violation reporting.~~

M5. The Transmission Operator shall have evidence of a documented voltage or Reactive Power Schedule (which is either a range or a target value with an associated tolerance band).

For part 5.1, the Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the applicable Generator Operators, and that the Generator Operator was directed to comply with the schedule in automatic voltage control mode, unless exempted.

For part 5.2, the Transmission Operator shall have evidence it provided notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band). For part 5.3, the Transmission Operator shall have evidence it provided the criteria used to develop voltage schedules or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) within 30 days of receiving a request by a Generator Operator.

~~**R11.**~~**R6.** After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~**1.0.** The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.~~

~~B. Measures~~

~~**M3.** The Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule as specified in Requirement 4 to each Generator Operator it requires to follow such a schedule.~~

~~**M4.** The Transmission Operator shall have evidence to show that, for each generating unit in its area that is exempt from following a voltage or Reactive Power schedule, the associated Generator Owner was notified of this exemption in accordance with Requirement 3.2.~~

~~**M5.** The Transmission Operator shall have evidence to show that it issued directives as specified in Requirement 6.1 when notified by a Generator Operator of the loss of an automatic voltage regulator control.~~

~~M4.~~M6. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with ~~Requirement 11~~the requirement and that it consulted with the Generator Owner.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

Regional Entity.

Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.2. Compliance Monitoring and Enforcement Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

DataAs defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.4.1.2. Evidence Retention:

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

The Transmission Operator shall retain evidence for Measures 1 through 46 for 12 months.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.5.1.4. Additional Compliance Information:

The Transmission Operator shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

1. Violation Severity Levels (no changes)

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operational Planning	High	N/A	N/A	N/A	The Transmission Operator does not specify a system voltage schedule (which is either a range or a target value with an associated tolerance band).
R2	Real-time Operations, Same-day Operations, and Operational Planning	High	N/A	N/A	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an SOL.	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an IROL.
R3	Real-time Operations, Same-day Operations, and Operational Planning	High	N/A	N/A	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an SOL.	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an IROL.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	Operations Planning	Lower	N/A	N/A	The Transmission Operator has exemption criteria and notified the Generator Operator, but the Transmission Operator does not have evidence of the notification to the Generator Operator.	The Transmission Operator does not have exemption criteria.
R5	Operations Planning	Medium	N/A	The Transmission Operator does not provide the criteria for voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) after 30 days of a request.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) to all Generator Operators.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) to any Generator Operators. Or The Transmission Operator does not provide the Generator Operator with the notification requirements for deviations from the

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).
R6	**Operations Planning**	**Lower**	The Transmission Operator does not provide either the technical justification or timeframe for changing generator step-up tap settings.	N/A	N/A	The Transmission Operator does not provide the technical justification and the timeframe for changing generator step-up tap settings.

~~D.~~ D. Regional Variances

~~Regional Variance for the Western Electricity Coordinating Council~~

The following Interconnection-wide variance shall be applicable in the Western Electricity Coordinating Council (WECC) and replaces, in their entirety, Requirements ~~R3~~R4 and ~~R4.~~ R5. Please note that Requirement ~~R3~~R4 is deleted and ~~R4~~R5 is replaced with the following requirements.

Requirements

~~E.A.13.~~**E.A.13** Each Transmission Operator shall issue any one of the following types of voltage schedules to the Generator Operators for each of their generation resources that are on-line and part of the Bulk Electric System within the Transmission Operator Area: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- A voltage set point with a voltage tolerance band and a specified period.
- An initial volt-ampere reactive output or initial power factor output with a voltage tolerance band for a specified period that the Generator Operator uses to establish a generator bus voltage set point.
- A voltage band for a specified period.

~~E.A.15.~~**E.A.14** Each Transmission Operator shall provide one of the following voltage schedule reference points for each generation resource in its Area to the Generator Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations~~]~~:]*

- The generator terminals.
- The high side of the generator step-up transformer.
- The point of interconnection.
- A location designated by mutual agreement between the Transmission Operator and Generator Operator.

~~E.A.16.~~**E.A.15** Each Generator Operator shall convert each voltage schedule specified in Requirement E.A.13 into the voltage set point for the generator excitation system. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

~~E.A.18.~~**E.A.16** Each Generator Operator shall provide its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals within

30 calendar days of request by its Transmission Operator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~E.A.20.~~**E.A.17** Each Transmission Operator shall provide to the Generator Operator, within 30 calendar days of a request for data by the Generator Operator, its transmission equipment data and operating data that supports development of the voltage set point conversion methodology. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~E.A.22.~~**E.A.18** Each Generator Operator shall meet the following control loop specifications if the Generator Operator uses control loops external to the Automatic Voltage Regulators (AVR) to manage MVar loading: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

~~E.A.18.2.~~**E.A.18.1.** Each control loop's design incorporates the AVR's automatic voltage controlled response to voltage deviations during System Disturbances.

~~E.A.18.3.~~**E.A.18.2.** Each control loop is only used by mutual agreement between the Generator Operator and the Transmission Operator affected by the control loop.

Measures2

~~M.E.A.13.~~ **M.E.A.13** Each Transmission Operator shall have and provide upon request, evidence that it provided the voltage schedules to the Generator Operator. Dated spreadsheets, reports, voice recordings, or other documentation containing the voltage schedule including set points, tolerance bands, and specified periods as required in Requirement E.A.13 are acceptable as evidence.

~~M.E.A.14.~~ **M.E.A.14** The Transmission Operator shall have and provide upon request, evidence that it provided one of the voltage schedule reference points in Requirement E.A.14 for each generation resource in its Area to the Generator Operator. Dated letters, e-mail, or other documentation that contains notification to the Generator Operator of the voltage schedule reference point for each generation resource are acceptable as evidence.

~~M.E.A.15.~~ **M.E.A.15** Each Generator Operator shall have and provide upon request, evidence that it converted a voltage schedule as described in Requirement E.A.13 into a

[2] The number for each measure corresponds with the number for each requirement, i.e. M.E.A.13 means the measure for Requirement E.A.13.

voltage set point for the AVR. Dated spreadsheets, logs, reports, or other documentation are acceptable as evidence.

~~M.E.A.16.~~ **M.E.A.16** The Generator Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Transmission Operator it provided its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

~~M.E.A.17.~~ **M.E.A.17** The Transmission Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Generator Operator it provided data to support development of the voltage set point conversion methodology. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

~~M.E.A.18.~~ **M.E.A.18** If the Generator Operator uses outside control loops to manage MVar loading, the Generator Operator shall have and provide upon request, evidence that it met the control loop specifications in sub-parts E.A.18.1 through E.A.18.2. Design specifications with identified agreed-upon control loops, system reports, or other dated documentation are acceptable as evidence.

Violation Severity Levels

E #	Lower VSL	Moderate VSL	High VSL	Severe VSL
E.A.13	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to at least one generation resource but less than or equal to 5% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 5% but less than or equal to 10% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 10% but less than or equal to 15% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.	For the specified period, the Transmission Operator did not issue one of the voltage schedules listed in E.A.13 to more than 15% of the generation resources that are on-line and part of the BES in the Transmission Operator Area.

E #	Lower VSL	Moderate VSL	High VSL	S evere VSL
E.A .14	The Transmission Operator did not provide a voltage schedule reference point for at least one but less than or equal to 5% of the generation resources in the Transmission Operator area.	he Transmission Operator did not provide a voltage schedule reference point for more than 5% but less than or equal to 10% of the generation resources in the Transmission Operator Area.	he Transmission Operator did not a voltage schedule reference point for more than 10% but less than or equal to 15% of the generation resources in the Transmission Operator Area.	T he Transmission Operator did not provide a voltage schedule reference point for more than 15% of the generation resources in the Transmission Operator Area.
E.A .15	The Generator Operator failed to convert at least one voltage schedule in Requirement E.A.13 into the voltage set point for the AVR for less than 25% of the voltage schedules.	The Generator Operator failed to convert the voltage schedules in Requirement E.A.13 into the voltage set point for the AVR for 25% or more but less than 50% of the voltage schedules.	he Generator Operator failed to convert the voltage schedules in Requirement E.A.13 into the voltage set point for the AVR for 50% or more but less than 75% of the voltage schedules.	The Generator Operator failed to convert the voltage schedules in Requirement E.A.13 into the voltage set point for the AVR for 75% or more of the voltage schedules.
E.A.1	The Generator Operator provided its voltage set point conversion methodology greater than 30 days but less than or equal to 60 days of a request by the Transmission Operator.	The Generator Operator provided its voltage set point conversion methodology greater than 60 days but less than or equal to 90 days of a request by the Transmission Operator.	he Generator Operator provided its voltage set point conversion methodology greater than 90 days but less than or equal to 120 days of a request by the	T he Generator Operator did not provide its voltage set point conversion methodology within 120 days of a request by the Transmission Operator.

E #	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Transmission Operator.	
E.A .17	The Transmission Operator provided its data to support development of the voltage set point conversion methodology than 30 days but less than or equal to 60 days of a request by the Generator Operator.	The Transmission Operator provided its data to support development of the voltage set point conversion methodology greater than 60 days but less than or equal to 90 days of a request by the Generator. Operator.	he Transmission Operator provided its data to support development of the voltage set point conversion methodology greater than 90 days but less than or equal to 120 days of a request by the Generator. Operator.	The Transmission Operator did not provide its data to support development of the voltage set point conversion methodology within 120 days of a request by the Generator Operator.
E.A .18	/A	The Generator Operator did not meet the control loop specifications in EA18.2 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.	he Generator Operator did not meet the control loop specifications in EA18.1 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.	The Generator Operator did not meet the control loop specifications in EA18.1 through EA18.2 when the Generator Operator uses control loop external to the AVR to manage Mvar loading.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

Rationale:

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

Rationale for R1:

Paragraph 1868 of Order No. 693 requires NERC to add more "detailed and definitive requirements on “established limits” and “sufficient reactive resources”, and identify acceptable margins (i.e. voltage and/or reactive power margins)." Since Order No. 693 was issued, however, several FAC and TOP standards have become enforceable to add more requirements around voltage limits. More specifically, FAC-011 and FAC-014 require that System Operating Limits (SOLs) and reliability margins are established. The NERC Glossary definition of SOLs includes both: 1) Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) and 2) System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits). Therefore, for reliability reasons Requirement R1 now requires a Transmission Operator (TOP) to set voltage or Reactive Power schedules with associated tolerance bands. Further, since neighboring areas can affect each other greatly, each TOP must also provide a copy of these schedules to its Reliability Coordinator (RC) and adjacent TOP upon request.

Rationale for R2:

Paragraph 1875 from Order No. 693 directed NERC to include requirements to run voltage stability analysis periodically, using online techniques where commercially available and offline tools when online tools are not available. This standard does not explicitly require the periodic voltage stability analysis because such analysis would be performed pursuant to the SOL methodology developed under the FAC standards. TOP standards also require the TOP to operate within SOLs and Interconnection Reliability Operating Limits (IROL). The VAR standard drafting team (SDT) and industry participants also concluded that the best models and tools are the ones that have been proven and the standard should not add a requirement for a responsible entity to purchase new online simulations tools. Thus, the VAR SDT simplified the requirements to ensuring sufficient reactive resources are online or scheduled. Controllable load is specifically included to answer FERC's directive in Order No. 693 at Paragraph 1879.

Rationale for R3:

Similar to Requirement R2, the VAR SDT determined that for reliability purposes, the TOP must ensure sufficient voltage support is provided in Real-time in order to operate within an SOL.

Rationale for R4:

The VAR SDT received significant feedback on instances when a TOP would need the flexibility for defining exemptions for generators. These exemptions can be tailored as the TOP deems necessary for the specific area's needs. The goal of this requirement is to provide a TOP the ability to exempt a Generator Operator (GOP) from: 1) a voltage or Reactive Power schedule, 2) a setting on the AVR, or 3) any VAR-002 notifications based on the TOP's criteria. Feedback from the industry detailed many system events that would require these types of exemptions which included, but are not limited to: 1) maintenance during shoulder months, 2) scenarios where two units are located within close proximity and both cannot be in voltage control mode, and 3) large system voltage swings where it would harm reliability if all GOP were to notify their respective TOP of deviations at one time. Also, in an effort to improve the requirement, the sub-requirements containing an exemption list were removed from the currently enforceable standard because this created more compliance issues with regard to how often the list would be updated and maintained.

Rationale for R5:

The new requirement provides transparency regarding the criteria used by the TOP to establish the voltage schedule. This requirement also provides a vehicle for the TOP to use appropriate granularity when setting notification requirements for deviation from the voltage or Reactive Power schedule. Additionally, this requirement provides clarity regarding a "tolerance band" as specified in the voltage schedule and the control dead-band in the generator's excitation system.

Voltage Schedule tolerances are the bandwidth that accompanies the voltage target in a voltage schedule, should reflect the anticipated fluctuation in voltage at the Generation Operator's facility during normal operations, and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a Generation Operator's automatic voltage regulator's control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

Rationale for R6:

Although tap settings are first established prior to interconnection, this requirement could not be deleted because no other standard addresses when a tap setting must be adjusted. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	August 2, 2006	BOT Adoption	Revised
1	June 18, 2007	FERC approved Version 1 of the standard.	Revised
1	July 3, 2007	Added "Generator Owners" and "Generator Operators" to Applicability section.	Errata
1	August 23, 2007	Removed "Generator Owners" and "Generator Operators" to Applicability section.	Errata
2	August 5, 2010	Adopted by NERC Board of Trustees; Modified to address Order No. 693 Directives contained in paragraphs 1858 and 1879.	Revised.
2	January, 10 2011	FERC issued letter order approving the addition of LSEs and Controllable Load to the standard.	Revised
3	May 9, 2012	Adopted by NERC Board of Trustees; Modified to add a WECC region variance	Revised
3	June 20, 2013	FERC issued order approving VAR-001-3	Revised
3	November 21, 2013	R5 and associated elements approved by FERC for retirement as part of the Paragraph 81 project (Project 2013-02)	Revised
4	February 6, 2014	Adopted by NERC Board of Trustees	Revised

Exhibit A-2

Proposed Reliability Standard VAR-002-3

A. Introduction

1. **Title:** **Generator Operation for Maintaining Network Voltage Schedules**

2. **Number:** VAR-002-3

3. **Purpose:** To ensure generators provide reactive support and voltage control, within generating Facility capabilities, in order to protect equipment and maintain reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Generator Operator

   4.2. Generator Owner

5. **Effective Dates**

   The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode as instructed by the Transmission Operator unless: 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- That the generator is being operated in start-up,[1] shutdown,[2] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in automatic voltage control mode or in the control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or in a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If a generator is exempted, the Generator Operator shall also have evidence that the generator is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within each generating Facility's capabilities[4]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.

[2] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

[3] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.

[4] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a generator is operating in manual control, reactive power capability may change based on stability considerations.

output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

2.2. When instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage or Reactive Power schedule.

For Part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

For Part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's instructions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the instruction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For Part 2.3, for Generator Operators that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall demonstrate the methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within 30 minutes of such change, then the Generator Operator is not required to notify the Transmission Operator of the status change *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any status change identified in Requirement R3. If the status has been restored within the first 30 minutes, no notification is necessary.

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within 30 minutes of the

Generator Operator becoming aware of such change, then the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability in accordance with Requirement R4. If the capability has been restored within the first 30 minutes, no notification is necessary.

R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

5.1. For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

5.1.1. Tap settings.

5.1.2. Available fixed tap ranges.

5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirement R5, Part 5.1.1 through Part 5.1.3 within 30 calendar days.

R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

6.1. If the Generator Owner cannot comply with the Transmission Operator's specifications, the Generator Owner shall notify the Transmission Operator and shall provide the technical justification.

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation in accordance with Requirement R6. The Generator Owner shall have evidence that it notified its associated Transmission Operator when it could not comply with the Transmission Operator's step-up transformer tap specifications in accordance with Requirement R6, Part 6.1.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. The Generator Operator shall maintain all other evidence for the current and previous calendar year.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Real-time Operations**	**Medium**	N/A	N/A	N/A	Unless exempted, the Generator Operator did not operate each generator connected to the interconnected transmission system in the automatic voltage control mode or in a different control mode as instructed by the Transmission Operator, and failed to provide the required notifications to Transmission Operator as identified in Requirement R1.
R2	**Real-time Operations**	**Medium**	N/A	N/A	The Generator Operator did not have a conversion methodology when it monitors voltage at a location different from the schedule provided by the Transmission Operator.	The Generator Operator did not maintain the voltage or Reactive Power schedule as instructed by the Transmission Operator and did not make the necessary notifications required by the Transmission Operator. OR The Generator Operator did not have an operating AVR, and the responsible entity did not use an alternative method for controlling voltage. OR The Generator Operator did not modify voltage when directed, and the responsible entity did not provide any

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						explanation.
R3	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of the status change.
R4	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of becoming aware of the capability change.
R5	**Real-time Operations**	**Lower**	N/A	N/A	The Generator Owner failed to provide its associated Transmission Operator and Transmission Planner one of the types of data specified in Requirement R5 Parts 5.1.1, 5.1.2, and 5.1.3.	The Generator Owner failed to provide to its associated Transmission Operator and Transmission Planner two or more of the types of data specified in Requirement R5 Parts 5.1.1, 5.1.2, and 5.1.3.
R6	**Real-time Operations**	**Lower**	N/A	N/A	N/A	The Generator Owner did not ensure the tap changes were made according the Transmission Operator's specifications. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Generator Owner failed to perform the tap changes, and the Generator Owner did not provide technical justification for why it could not comply with the Transmission Operator specifications.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	5/1/2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and 2.4.3.	July 5, 2006
1a	12/19/2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	1/16/2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	Errata
1.1a	10/29/2008	BOT adopted errata changes; updated version number to "1.1a"	Errata
1.1b	3/3/2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	Revised
2b	8/16/2012	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4. FERC Order issued approving VAR-002-2b. Adopted by Board of Trustees.	Revised
2b	4/16/2013	FERC Order issued approving VAR-002-2b	
3	5/7/2014	Adopted by the NERC Board of Trustees	

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

Rationale:

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

Rationale for R1:

This requirement has been maintained due to the importance of running a unit with its automatic voltage regulator (AVR) in service and in either voltage controlling mode or the mode instructed by the TOP. However, the requirement has been modified to allow for testing, and the measure has been updated to include some of the evidence that can be used for compliance purposes.

Rationale for R2:

Requirement R2 details how a Generator Operator (GOP) operates its generator(s) to provide voltage support and when the GOP is expected to notify the Transmission Operator (TOP). In an effort to remove prescriptive notification requirements for the entire continent, the VAR-002-3 standard drafting team (SDT) opted to allow each TOP to determine the notification requirements for each of its respective GOPs based on system requirements. Additionally, a new Part 2.3 has been added to detail that each GOP may monitor voltage by using its existing facility equipment.

Conversion Methodology: There are many ways to convert the voltage schedule from one voltage level to another. Some entities may choose to develop voltage regulation curves for their transformers; others may choose to do a straight ratio conversion; others may choose an entirely different methodology. All of these methods have technical challenges, but the studies performed by the TOP, which consider N-1 and credible N-2 contingencies, should compensate for the error introduced by these methodologies, and the TOP possesses the authority to direct the GOP to modify its output if its performance is not satisfactory. During a significant system event, such as a voltage collapse, even a generation unit in automatic voltage control that controls based on the low-side of the generator step-up transformer should see the event on the low-side of the generator step-up transformer and respond accordingly.

Voltage Schedule Tolerances: The bandwidth that accompanies the voltage target in a voltage schedule should reflect the anticipated fluctuation in voltage at the GOP's Facility during normal operations and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a GOP's AVR control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

Rationale for R3:

This requirement has been modified to limit the notifications required when an AVR goes out of service and quickly comes back in service. Notifications of this type of status change provide little to no benefit to reliability. Thirty (30) minutes have been built into the requirement to allow a GOP time to resolve an issue before having to notify the TOP of a status change. The requirement has also been amended to remove the sub-requirement to provide an estimate for the expected duration of the status change.

Rationale for R4:

This requirement has been bifurcated from the prior version VAR-002-2b Requirement R3. This requirement allows GOPs to report reactive capability changes after they are made aware of the change. The current standard requires notification as soon as the change occurs, but many GOPs are not aware of a reactive capability change until it has taken place.

Rationale for R5:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected. The prior version of VAR-002-2b, Requirement R4.1.4 (the +/- voltage range with step-change in % for load-tap changing transformers) has been removed. The percentage information was not needed because the tap settings, ranges and impedance are required. Those inputs can be used to calculate the step-change percentage if needed.

Rationale for R6:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected.

A. Introduction

1. **Title:** **Generator Operation for Maintaining Network Voltage Schedules**~~—~~

2. **Number:** VAR-002-~~2b~~3

3. **Purpose:** ~~—~~ To ensure generators provide reactive support and voltage control ~~necessary to ensure voltage levels, reactive flows, and reactive resources are maintained,~~ within ~~applicable~~generating Facility ~~Ratings~~capabilities, in order to protect equipment and ~~the~~maintain reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Generator Operator~~.~~

   4.2. Generator Owner~~.~~

5. **Effective ~~Date:~~ ~~In those jurisdictions where regulatory approval is required, this~~Dates**

   ~~5.~~The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable ~~regulatory~~governmental authority is required for a standard to go into effect. Where approval ~~or as otherwise made effective pursuant to the laws~~by an applicable ~~to such ERO~~ governmental ~~authorities. In those jurisdictions where no regulatory approval~~authority is not required, ~~this standard~~ VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees ~~approval~~or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode as instructed by the Transmission Operator unless: 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- That the generator is being operated in start-up,[1] ~~or~~ shutdown,[2] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in ~~the~~ automatic voltage control mode or in the control mode that was instructed by the Transmission Operator for a reason other than start-up ~~or~~, shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or in a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If a generator is exempted, the Generator Operator shall also have evidence that the generator is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within ~~applicable Facility Ratings[4]) as directed by the Transmission Operator.~~each generating Facility's capabilities[5]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.

[2] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

[3] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator ~~establishing a tolerance band within which the target value is to be maintained during a specified period~~.

[4] ~~When a Generator is operating in manual control, reactive power capability may change based on stability considerations and this may lead to a change in the associated Facility Ratings.~~

[5] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a generator is operating in manual control, reactive power capability may change based on stability considerations.

Reactive Power schedule provided by the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

~~R2.1.~~2.1. When a generator's ~~automatic voltage regulator~~AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator ~~voltage and~~ reactive output to meet the voltage or Reactive Power schedule ~~directed~~provided by the Transmission Operator.

~~R2.2.~~2.2. When ~~directed~~instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage or Reactive Power schedule.

For Part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

For Part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's instructions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the instruction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For Part 2.3, for Generator Operators that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall demonstrate the methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

R3. Each Generator Operator shall notify its associated Transmission Operator ~~as soon as practical, but~~ of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of ~~any of the following:~~ the change. If the status has been restored within 30 minutes of such change, then the Generator Operator is not required to notify the Transmission Operator of the status change *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

~~**3.1.** A status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.~~

~~**3.2.** A status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.~~

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any status change identified in Requirement R3. If the status has been restored within the first 30 minutes, no notification is necessary.

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within 30 minutes of the Generator Operator becoming aware of such change, then the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability in accordance with Requirement R4. If the capability has been restored within the first 30 minutes, no notification is necessary.

~~**R4.**~~**R5.** The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

~~**R4.1.**~~**5.1.** For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

~~**R4.1.1.**~~**5.1.1.** Tap settings.

~~**R4.1.2.**~~**5.1.2.** Available fixed tap ranges.

~~**R4.1.3.**~~**5.1.3.** Impedance data.

~~**4.1.4.** The +/- voltage range with step-change in % for load-tap changing transformers.~~

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirement R5, Part 5.1.1 through Part 5.1.3 within 30 calendar days.

~~**R5.**~~**R6.** After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: ~~Medium~~Lower] [Time Horizon: Real-time Operations]*

~~**R5.1.**~~**6.1.** If the Generator ~~Operator can't~~Owner cannot comply with the Transmission Operator's specifications, the Generator ~~Operator~~Owner shall notify the Transmission Operator and shall provide the technical justification.

~~C. Measures~~

~~**M1.** The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode as specified in Requirement 1. If a generator is being started up or shut down with the automatic voltage control off and no notification of the automatic voltage regulator status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode. Such evidence must include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached.~~

~~**M2.** The Generator Operator shall have evidence to show that it controlled its generator voltage and reactive output to meet the voltage or Reactive Power schedule provided by its associated Transmission Operator as specified in Requirement 2.~~

~~**M3.** The Generator Operator shall have evidence to show that it responded to the Transmission Operator's direction as identified in Requirement 2.1 and Requirement 2.2.~~

~~**M4.** The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any of the changes identified in Requirement 3.~~

~~**M5.** The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirements 4.1.1 through 4.1.4~~

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation ~~as identified in Requirement 5.~~in accordance with Requirement R6. The Generator Owner shall have evidence that it notified its associated Transmission Operator when it could not comply with the Transmission Operator's step-up transformer tap specifications in accordance with Requirement R6, Part 6.1.

~~**M7.** The Generator Operator shall have evidence that it notified its associated Transmission Operator when it couldn't comply with the Transmission Operator's step-up transformer tap specifications as identified in Requirement 5.1.~~

D.C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Monitoring Responsibility

1.1. For entities that do not work for the Regional Entity, the Regional Entity shall serve as the **Compliance Enforcement Authority.:**

For functional entities that work for their Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. DataEvidence Retention:

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

The Generator Operator shall maintain evidence needed for Measure 1 through Measure 4 and Measure 7 for the current and previous calendar year.

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. (Measures 5 and 6) The Generator Operator shall maintain all other evidence for the current and previous calendar year.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and EnforcementAssessment Processes:

The following processes may be used:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None.

Table of Compliance Elements

~~2. Violation Severity Levels~~

R # ~~R #~~	Time Horizon	VRF	Violation Severity Levels					
			Lower VSL	Moderate VSL	High VSL	Severe VSL		
R1~~.~~	Real-time Operations	Medium	N/A	N/A	N/A	~~The responsible entity~~ Unless exempted, the Generator Operator did not operate each generator connected to the interconnected transmission system in the automatic voltage control mode ~~and failed to notify~~or in a different control mode as instructed by the Transmission Operator, and failed to provide the required notifications to Transmission Operator as identified in Requirement R1.		
R2~~.~~	Real-time Operations	Medium	N/A	N/A	~~When directed~~The Generator Operator did not have a conversion methodology when it monitors voltage at a location different from the schedule provided by the Transmission Operator ~~to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for~~	~~When directed~~The Generator Operator did not maintain the voltage or Reactive Power schedule as instructed by the Transmission Operator ~~to maintain the generator voltage or reactive power schedule~~and did not make the ~~Generator Operator failed to meet the directed values for more than 45 minutes up to and including 60 minutes.~~ necessary notifications required by the Transmission Operator.	~~When directed by the Transmission Operator to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for more than 60 minutes up to and including 75 minutes.~~	~~When directed by the Transmission Operator to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for more than 75 minutes.~~ ~~OR~~ ~~When a generator's automatic voltage regulator is out~~

R #	Time Horizon	VRF	Violation Severity Levels					
R #			Lower VSL	Moderate VSL	High VSL	Severe VSL		
					up to and including 45 minutes.	OR When a generator's automatic voltage regulator is out of service, the The Generator Operator failed todid not have an operating AVR, and the responsible entity did not use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operatorfor controlling voltage. OR The Generator Operator failed todid not modify voltage when directed, and the responsible entity did not provide ananyexplanation of why the		of service, the Generator Operator failed to use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator and the Generator Operator failed to provide an explanation of why the voltage schedule could not be met.

R # ~~R #~~	Time Horizon	VRF	Violation Severity Levels					
			Lower VSL	Moderate VSL	High VSL	Severe VSL		
						~~voltage schedule could not be met~~.		
R3~~.~~	**Real-time Operations**	**Medium**	N/A	N/A	~~The Generator Operator failed to notify the Transmission Operator within 30 minutes of the information as specified in either R3.1 or R3.2~~N/A	The Generator Operator ~~failed to notify~~did not make the ~~Transmission Operator~~required notification within 30 minutes of the ~~information as specified in both R3.1 and R3.2~~status change.		
R4	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of becoming aware of the capability change.		
~~R4.~~**R5**	**Real-time Operations**	**Lower**	N/A	N/A	The ~~Responsible entity~~Generator Owner failed to provide ~~to~~ its associated Transmission Operator and Transmission Planner one of the types of data ~~as~~	The ~~Responsible entity~~Generator Owner failed to provide to its associated Transmission Operator and Transmission Planner two or more of the types of data ~~as~~ specified in ~~R4~~Requirement R5	~~The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner three of the types of data as~~	~~The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner any of the types of data as~~

R # ~~R #~~	Time Horizon	VRF	Violation Severity Levels					
			Lower VSL	Moderate VSL	High VSL	Severe VSL		
					specified in ~~R4~~Requirement R5 Parts 5.1.1 ~~or R 4~~, 5.1.2 ~~or 4~~, and 5.1.3 ~~or 4.1.4~~. ~~OR~~ ~~The information was provided in more than 30, but less than or equal to 35 calendar days of the request.~~	Parts 5.1.1 ~~or R 4~~, 5.1.2 ~~or 4~~, and 5.1.3 ~~or 4.1.4~~ ~~OR~~. ~~The information was provided in more than 35, but less than or equal to 40 calendar days of the request.~~	~~specified in R4.1.1 or R 4.1.2 or 4.1.3 or 4.1.4~~ ~~OR~~ ~~The information was provided in more than 40, but less than or equal to 45 calendar days of the request.~~	~~specified in R4.1.1 and R 4.1.2 and 4.1.3 and 4.1.4~~ ~~OR~~ ~~The information was provided in more than 45 calendar days of the request.~~
~~R5.~~**R6**	**Real-time Operations**	**Lower**	N/A	N/A	N/A	The ~~responsible entity failed to~~ Generator Owner did not ensure ~~that transformer~~ the tap ~~positions~~changes were ~~changed~~made according ~~to~~ the Transmission Operator's specifications. OR The ~~provided by~~Generator Owner failed to perform the tap changes, and the Generator Owner did not provide technical justification for why it could not comply with the Transmission Operator ~~when said actions would not have violated safety, an equipment rating, a regulatory requirement, or a statutory requirement.~~ specifications.		
~~R5.1.~~		~~N/A~~	~~N/A~~	~~N/A~~	~~The responsible entity failed to notify the Transmission Operator and to provide~~			

R # ~~R #~~	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~technical justification.~~	

E.D. Regional DifferencesVariances

None identified.

E. Interpretations

None.

F. Associated Documents

1. Appendix 1 — Interpretation of Requirements R1 and R2 (August 1, 2007).

None.

Version History

Version	Date	Action	Change Tracking
1	May 15, 5/1/2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and 2.4.3.	July 5, 2006
1a	December 12/19, /2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	January 1/16, /2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	Errata
1.1a	October 10/29, /2008	BOT adopted errata changes; updated version number to "1.1a"	Errata
1.1b	March 3, /3/2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	Revised
2b	TBD8/16/2012	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4. FERC Order issued approving VAR-002-2b. Adopted by Board of Trustees.	Revised
2b	August 4/16, 2012/2013	FERC Order issued approving VAR-002-2bAdopted by Board of Trustees	

~~2b~~3	~~April 16, 2013~~5/7/2014	Adopted by the NERC Board of Trustees~~FERC Order issued approving VAR-002-2b~~	

Appendix 1

Interpretation of Requirements R1 and R2

Request:

Requirement R1 of Standard VAR-002-1 states that Generation Operators shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (***automatic voltage regulator in service and controlling voltage***) unless the Generator Operator has notified the Transmission Operator.

Requirement R2 goes on to state that each Generation Operator shall maintain the generator voltage ***or Reactive Power output*** as directed by the Transmission Operator.

The two underlined phrases are the reasons for this interpretation request.

Most generation excitation controls include a device known as the Automatic Voltage Regulator, or AVR. This is the device which is referred to by the R1 requirement above. Most AVR's have the option of being set in various operating modes, such as constant voltage, constant power factor, and constant Mvar.

In the course of helping members of the WECC insure that they are in full compliance with NERC Reliability Standards, I have discovered both Transmission Operators and Generation Operators who have interpreted this standard to mean that AVR operation in the constant power factor or constant Mvar modes complies with the R1 and R2 requirements cited above. Their rational is as follows:

- The AVR is clearly in service because it is operating in one of its operating modes
- The AVR is clearly controlling voltage because to maintain constant PF or constant Mvar, it controls the generator terminal voltage
- R2 clearly gives the Transmission Operator the option of directing the Generation Operator to maintain a constant reactive power output rather than a constant voltage.

Other parties have interpreted this standard to require operation in the constant voltage mode only. Their rational stems from the belief that the purpose of the VAR-002-1 standard is to insure the automatic delivery of additional reactive to the system whenever a voltage decline begins to occur.

The material impact of misinterpretation of these standards is twofold.

- First, misinterpretation may result in reduced reactive response during system disturbances, which in turn may contribute to voltage collapse.
- Second, misinterpretation may result in substantial financial penalties imposed on generation operators and transmission operators who believe that they are in full compliance with the standard.

In accordance with the NERC Reliability Standards Development Procedure, I am requesting that a formal interpretation of the VAR-002-1 standard be provided. Two specific questions need to be answered.

- First, does AVR operation in the constant PF or constant Mvar modes comply with R1?

- ~~Second, does R2 give the Transmission Operator the option of directing the Generation Owner to operate the AVR in the constant Pf or constant Mvar modes rather than the constant voltage mode?~~

~~Interpretation:~~

1. ~~First, does AVR operation in the constant PF or constant Mvar modes comply with R1?~~

   ~~Interpretation~~: ~~No, only operation in constant voltage mode meets this requirement. This answer is predicated on the assumption that the generator has the physical equipment that will allow such operation and that the Transmission Operator has not directed the generator to run in a mode other than constant voltage.~~

2. ~~Second, does R2 give the Transmission Operator the option of directing the Generation Owner (sic) to operate the AVR in the constant Pf or constant Mvar modes rather than the constant voltage mode?~~

   ~~Interpretation~~: ~~Yes, if the Transmission Operator specifically directs a Generator Operator to operate the AVR in a mode other than constant voltage mode, then that directed mode of AVR operation is allowed.~~

Appendix 2

Interpretation of VAR-002-1a

Request:

VAR-002 — Generator Operation for Maintaining Network Voltage Schedules, addresses the generator's provision of voltage and VAR control. Confusion exists in the industry and regions as to which requirements in this standard apply to Generator Operators that operate generators that do not have automatic voltage regulation capability.

The Standard's requirements do not identify the subset of generator operators that need to comply – forcing some generator operators that do not have any automatic voltage regulation capability to demonstrate how they complied with the requirements, even when they aren't physically able to comply with the requirements. Generator owners want clarification to verify that they are not expected to acquire AVR devices to comply with the requirements in this standard.

Many generators do not have automatic voltage regulators and do not receive voltage schedules. These entities are at a loss as to how to comply with these requirements and are expending resources attempting to demonstrate compliance with these requirements. A clarification will avoid challenges and potential litigation stemming from sanctions and penalties applied to entities that are being audited for compliance with this standard, but who do not fall within the scope or intent of the standard itself.

Please identify which requirements apply to generators that do not operate generators equipped with AVRs.

Response: All the requirements and associated subrequirements in VAR-002-1a apply to Generator Owners and Generator Operators that own or operate generators whether equipped with an automatic voltage regulator or not. The standard is predicated on the assumption that the generator has the physical equipment (automatic voltage regulator) that is capable of automatic operation. A generator that is not equipped with an automatic voltage regulator results in a functionally equivalent condition to a generator equipped with an automatic voltage regulator that is out of service due to maintenance or failure.

There are no requirements in the standard that require a generator to have an automatic voltage regulator, nor are there any requirements for a Generator Owner to modify its generator to add an automatic voltage regulator. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power output (within applicable Facility Ratings) as directed by the Transmission Operator.

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

Rationale:

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

Rationale for R1:

This requirement has been maintained due to the importance of running a unit with its automatic voltage regulator (AVR) in service and in either voltage controlling mode or the mode instructed by the TOP. However, the requirement has been modified to allow for testing, and the measure has been updated to include some of the evidence that can be used for compliance purposes.

Rationale for R2:

Requirement R2 details how a Generator Operator (GOP) operates its generator(s) to provide voltage support and when the GOP is expected to notify the Transmission Operator (TOP). In an effort to remove prescriptive notification requirements for the entire continent, the VAR-002-3 standard drafting team (SDT) opted to allow each TOP to determine the notification requirements for each of its respective GOPs based on system requirements. Additionally, a new Part 2.3 has been added to detail that each GOP may monitor voltage by using its existing facility equipment.

Conversion Methodology: There are many ways to convert the voltage schedule from one voltage level to another. Some entities may choose to develop voltage regulation curves for their transformers; others may choose to do a straight ratio conversion; others may choose an entirely different methodology. All of these methods have technical challenges, but the studies performed by the TOP, which consider N-1 and credible N-2 contingencies, should compensate for the error introduced by these methodologies, and the TOP possesses the authority to direct the GOP to modify its output if its performance is not satisfactory. During a significant system event, such as a voltage collapse, even a generation unit in automatic voltage control that controls based on the low-side of the generator step-up transformer should see the event on the low-side of the generator step-up transformer and respond accordingly.

Voltage Schedule Tolerances: The bandwidth that accompanies the voltage target in a voltage schedule should reflect the anticipated fluctuation in voltage at the GOP's Facility during normal operations and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a GOP's AVR control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

Rationale for R3:

This requirement has been modified to limit the notifications required when an AVR goes out of service and quickly comes back in service. Notifications of this type of status change provide little to no benefit to reliability. Thirty (30) minutes have been built into the requirement to allow a GOP time to resolve an issue before having to notify the TOP of a status change. The requirement has also been amended to remove the sub-requirement to provide an estimate for the expected duration of the status change.

Rationale for R4:

This requirement has been bifurcated from the prior version VAR-002-2b Requirement R3. This requirement allows GOPs to report reactive capability changes after they are made aware of the change. The current standard requires notification as soon as the change occurs, but many GOPs are not aware of a reactive capability change until it has taken place.

Rationale for R5:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected. The prior version of VAR-002-2b, Requirement R4.1.4 (the +/- voltage range with step-change in % for load-tap changing transformers) has been removed. The percentage information was not needed because the tap settings, ranges and impedance are required. Those inputs can be used to calculate the step-change percentage if needed.

Rationale for R6:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected.

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

VAR Directives Project

Implementation Plan for VAR-001-4 and VAR-002-3

Approvals Required

VAR-001-4 – Voltage and Reactive Control
VAR-002-3 — Generator Operation for Maintaining Network Voltage Schedules

Prerequisite Approvals

There are no other standards that must receive approval prior to the approval of this standard.

Revisions to Glossary Terms

None

Applicable Entities

Generator Operators (VAR-002-3)

Generator Owners (VAR-002-3)

Transmission Operators (VAR-001-4)

Applicable Facilities

N/A

Conforming Changes to Other Standards

None

Effective Dates

VAR-001-4 and VAR-002-3 – All requirements shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-001-4 and VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Justification

The currently effective VAR-002 standard is one of the most violated standards; however, the industry argues these violations do not address any reliability gaps. Instead, Generator Operators and Transmission Operators are required to handle many nuisance phone calls for slight deviations from a voltage schedule. The nuisance phone calls can be a distraction during a scheduled maintenance or a system event; thus, the industry would support making the changes as soon as possible. However, since VAR-001 now requires determining voltage and reactive power schedules with associated tolerance bands in addition to any notification requirements, the Transmission Operators need a quarter to prepare documentation. The VAR-002 standards cannot go into effect without the new TOP schedules and notification requirements. Also for Transmission Operators that do not already provide tolerance bands with voltage schedules, those Transmission Operators will need some time to adjust to providing new data (more specifically, the criteria for schedules) to Generator Operators.

Retirements

VAR-001-3 and VAR-002-2b will be retired at midnight of the day immediately prior to the Effective Date of VAR-001-4 and VAR-002-3 in the particular jurisdiction in which the new standards are becoming effective.

Exhibit C

Order No. 672 Criteria

In Order No. 672,[1] the Commission identified a number of criteria it will use to analyze Reliability Standards proposed for approval to ensure they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The discussion below identifies these factors and explains how proposed Reliability Standards VAR-001-4 and VAR-002-3 have met or exceeded the criteria:

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

The proposed Reliability Standards achieve specific reliability goals. Proposed Reliability Standard VAR-001-4 (Voltage and Reactive Control) ensures that responsible entities monitor, control, and maintain voltage levels, reactive flows, and reactive resources in Real-time to protect equipment and maintain reliable operations. Proposed Reliability Standard VAR-002-3 (Generator Operation for Maintaining Network Voltage Schedules) ensures that responsible entities provide the reactive support and voltage control necessary to protect equipment and maintain reliable operations. Collectively, these proposed Reliability Standards are designed to prevent voltage instability and voltage collapse of the Bulk-Power System.

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

Proposed Reliability Standard VAR-001-4 applies to Transmission Operators and, within the Western Interconnection, Generator Operators and is clear and unambiguous as to what is required and who is required to comply, in accordance with Order No. 672.

---

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

[2] Order No. 672 at PP 321, 324.

[3] *Id.* at PP 322, 325.

Proposed Reliability Standard VAR-001-4 contains six requirements that clearly and unambiguously state to whom each requirement applies and establishes the applicable entities' compliance obligations.

Proposed Reliability Standard VAR-002-3 applies to Generator Operators and Generator Owners and is clear and unambiguous as to what is required and who is required to comply, in accordance with Order No. 672. Proposed Reliability Standard VAR-002-3 contains six requirements that clearly and unambiguously state to whom each requirement applies and establishes the applicable entities' compliance obligations.

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

Proposed Reliability Standards VAR-001-4 and VAR-002-3 include Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) that comport with NERC and Commission guidelines. As explained further in Exhibit F, the severity level assigned to each requirement (for a violation of the requirement) contains a clear explanation of the basis for the assignment, which promotes uniformity and consistency in applying each requirement. The VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

Proposed Reliability Standards VAR-001-4 and VAR-002-3 also include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation. Upon approval by the Commission, the ranges of penalties for violations will be based on the applicable VRF and VSL in accordance with the sanctions table and the supporting penalty determination process described in the Commission-approved NERC Sanction Guidelines, Appendix 4B to the NERC Rules of Procedure.

[4] *Id.* at P 326.

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

The proposed Reliability Standards identify clear and objective criteria or measures for compliance, so that each Reliability Standard can be enforced in a consistent non-preferential manner. Specifically, each proposed Reliability Standard includes a clear statement of its purpose, the rationale behind each requirement, and a statement of the measures to be used in assessing compliance with each requirement. These provisions help provide clarity on how the requirements will be enforced, and ensure that the requirements will be assessed and enforced in a clear, consistent, and non-preferential manner, without prejudice to any party.

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

The proposed Reliability Standards achieve the reliability goals effectively and efficiently in accordance with Order No. 672. Collectively, the proposed Reliability Standards improve reliability by ensuring that the Bulk-Power System operates at acceptable voltage levels and that sufficient Reactive Power on the Bulk-Power System exists to provide the voltage support necessary to maintain voltage stability. Proposed Reliability Standard VAR-001-4 improves reliability by requiring set system voltage schedules and voltage coordination among responsible entities. Proposed Reliability Standard VAR-002-3 improves reliability by requiring reactive support and voltage control from responsible entities necessary to protect equipment and maintain reliable operations. In each case, the proposed Reliability Standard provides flexibility to the responsible

[5] *Id.* at P 327.

[6] *Id.* at P 328.

entities to determine how best to achieve compliance, thereby ensuring reliability without imposing unduly burdensome costs or requiring the adoption of "best practices."

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

The proposed Reliability Standards do not reflect a "lowest common denominator" approach. To the contrary, proposed Reliability Standards VAR-001-4 and VAR-002-3 represent a significant improvement over the previous versions as described herein.

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

The proposed Reliability Standards apply throughout North America and do not favor one geographic area or regional model. The existing regional variance in VAR-001-3 applicable in the Western Interconnection will continue to be enforced in proposed VAR-001-4.

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

The Proposed Reliability Standards do not cause undue negative effect on competition or restriction of the grid. Specifically, neither proposed Reliability Standard

[7] *Id.* at PP 329, 330.

[8] Order No. 672 at PP 331.

[9] *Id.* at P 332.

VAR-001-4 nor VAR-002-3 restricts the available transmission capability or limit use of the Bulk-Power System in a preferential manner.

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

The implementation time and proposed effective dates for the proposed Reliability Standards are just and reasonable and appropriately balance the urgency in the need to implement the Reliability Standards against the reasonableness of the time allowed for those who must comply to develop necessary procedures, software, facilities, staffing, or other relevant capability. The proposed effective dates will allow applicable entities adequate time to ensure compliance with the requirements and are explained in the proposed Implementation Plan, attached as Exhibit B.

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

The proposed Reliability Standards were developed in accordance with NERC's Commission-approved, ANSI-accredited processes for developing and approving Reliability Standards. Exhibit F includes a summary of the Reliability Standards development proceedings, and details the processes followed to develop the proposed Standards.

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

[10] *Id.* at P 333.

[11] *Id.* at P 334.

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

NERC has identified no competing vital public interests regarding the request for approval of proposed Reliability Standards VAR-001-4 and VAR-002-3. No comments were received indicating that the proposed Reliability Standards conflict with other vital public interests.

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

No other negative factors relevant to whether the proposed Reliability Standards satisfy the Commission's criteria for approval were identified.

[12] *Id.* at P 335.

[13] *Id.* at P 323.

Exhibit D-1

Mapping Document for Proposed Reliability Standard VAR-001-4

Project 2013-04 Voltage & Reactive Control

Mapping Document - Transition of VAR-001-3 to VAR-001-4

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3, Requirement R1	VAR-001-4, Requirement R1	Elements of VAR-001-3, Requirement R1 were duplicated in other Reliability Standards. Specifically, currently enforceable Reliability Standard TOP-004-2 Requirements R1, R2, and R3 duplicate monitoring and controlling voltage requirements. To comply with the obligation to operate within the IROLs and SOLs, entities must monitor and control voltage. Further, the Transmission Operations group of Reliability Standards is currently in development but will continue to include requirements that Transmission Operators ("TOPs"): (1) plan to operate within IROLs and SOLs; and (2) operate within IROLs and SOLs. Requirement R1 has been modified to remove the duplication and require the Transmission Operator ("TOPs") to specify a system voltage and Reactive Power schedules. A new part 1.1 has been added to allow for voltage coordination with adjacent TOPs and applicable Reliability Coordinators ("RCs").
VAR-001-3, Requirement R2	VAR-001-4, Requirement R2	The new Requirement R2 consolidates and modifies Requirements R2 and R9 of VAR-001-3 to require that TOPs schedule sufficient reactive resources. New Requirement R2 also clarifies the language with respect to the manner in which Transmission Operators may schedule sufficient reactive resources.

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3, Requirement R3	VAR-001-4, Requirement R4	Requirement R4 carries forward the authority in currently enforceable Reliability Standard VAR-001-03, Requirement R3 for a TOP to exempt a Generator Operator ("GOP") from having to comply with all or some of its Reactive Power obligations. New Requirement R4, however, does not include a requirement for the TOP to maintain an exemption list. Instead, the standard focuses on the transparency of the exemption criteria and whether the TOP notifies the GOP if granted an exemption.
VAR-001-3, Requirement R4	VAR-001-4, Requirement R5	The new requirements have been updated to allow the TOP to provide the voltage or Reactive Power schedule at either the high side or the low side of the GSU. Also a tolerance band is now required under the new requirement. New parts have also been added to direct a GOP to operate in AVR, to require the TOP to provide notification requirements, and to provide the criteria for developing schedules and tolerance bands upon request.
VAR-001-3, Requirement R5	Deleted	The Federal Energy Regulatory Commission approved the retirement requirement as part of the Paragraph 81 project. *Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards*, 145 FERC ¶ 61,147 at PP 25-26, Attachment A (2013).

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3, Requirement R6	Deleted	VAR-001-3, Requirement R6 was deleted because it was duplicative of existing TOP Reliability standards (i.e., TOP-006-2, Requirement R1), which require knowing the status of Reactive Power resources. The TOP standards currently in development would carry forward this obligation. Although power system stabilizers are not specifically named in the TOP standards, the areas that rely on PSS equipment will require monitoring the PSS status under the data specifications of the TOP standards.
VAR-001-3, Requirement R7	VAR-001-4, Requirement R3	VAR-001-4, Requirement R3 carries forward the obligation from VAR-001-3, Requirement R7
VAR-001-3, Requirement R8	VAR-001-4, Requirement R3	The standard drafting team concluded that there was no need to separately carry forward VAR-001-3, Requirement R8 because it was subsumed in proposed VAR-001-4, Requirement R3.
VAR-001-3, Requirement R9	VAR-001-4, Requirement R2	See comments for Requirement R2.
VAR-001-3, Requirement R10	Deleted	VAR-001-3, Requirement R10 was deleted because it was duplicative of existing TOP Reliability standards (i.e., TOP-004-2, Requirements R1 and R4), which require TOPs to correct SOL/IROL violations resulting from reactive resources deficiencies. The TOP standards currently in development would carry forward this obligation.
VAR-001-3, Requirement R11	VAR-001-4, Requirement R6	The requirement has been updated to allow for scheduling consultation.

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3, Requirement R12	Deleted	VAR-001-3, Requirement R10 was deleted because it was duplicative of existing TOP and EOP Reliability standards (i.e., TOP-004-2; EOP-003-2), to take corrective action, including load-shedding, to prevent voltage collapse. The TOP standards currently in development would carry forward this obligation.

Exhibit D-2

Mapping Document for Proposed Reliability Standard VAR-002-3

Project 2013-04 Voltage & Reactive Control

Mapping Document - Transition of VAR-002-2b to VAR-002-3

Standard: VAR-002-3 – Capacity Benefit Margin		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b, Requirement R1	VAR-002-3, Requirement R1	VAR-002-3, Requirement R1 carries forward the obligation in currently effective VAR-002-2b, Requirement R1 for Generator Operators ("GOPs") to operate generators in automatic voltage control mode but modifies the requirement to allow a GOP to operate in a different control mode if instructed by the Transmission Operator ("TOP"). New Requirement R1 also adds testing as a time when a generator need not operate in automatic voltage control mode or a different mode instructed by the Transmission Operator.
VAR-002-2b, Requirement R2	VAR-002-3, Requirement R2	VAR-002-3, Requirement R2 carries forward the affirmative obligation from VAR-003-1, Requirement R2 that the GOP maintain the voltage or Reactive Power schedule provided by the TOP pursuant to VAR-001-4, Requirement R5, unless the TOP exempts the GOP from doing so pursuant to VAR-001-4, Requirement R4. New Requirement R2 also adds that the GOP need not comply with the schedule if it satisfies the notification requirements for deviations established by the TOP VAR-001-4, Requirement R5, Part 5.2. Lastly, new Requirement R2 includes a provision to allow GOPs that do not monitor voltage at the location specified in their voltage schedule provided by the TOP to convert the schedule to the voltage point monitored by the GOP.

Standard: VAR-002-3 – Capacity Benefit Margin		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b, Requirement R3	VAR-002-3, Requirement R3 and R4.	Proposed Requirements R3 and R4 separate the notification requirements in currently-effective VAR-002-2b, Requirement R3 into two requirements: (1) for AVR/PSS status changes (proposed Requirement R3), and (2) for reactive capability changes (proposed Requirement R4). Each of the proposed requirements provides for a 30-minute window to allow a GOPs time to resolve an issue before having to notify the TOP of a change.
VAR-002-2b, Requirement R3	VAR-002-3, Requirement R5	VAR-002-3, Requirement R5 carries forward the obligations in VAR-002-2b, Requirement R3 but modifies it to the sub-part that requires the GOP to provide "[t]he +/- voltage range with step-change in % for load-tap changing transformers." The measure was also modified to add that a GOP must provide the data "within 30 calendar days"
VAR-002-2b, Requirement R4	VAR-002-3, Requirement R6	VAR-002-3, Requirement R6 modifies VAR-002-2b, Requirement R4 only to apply to the same functional entity throughout the requirement.

Exhibit E

Analysis of Violation Risk Factors and Violation Severity Levels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules

This document provides the Standard Drafting Team's (SDT) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project. A copy of the standard with the associated VRFs and VSLs is available here.

NERC Criteria - Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Violation Risk Factor Guidelines

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

The Commission seeks to ensure that Violation Risk Factors assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities

• Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

Guideline (3) – Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) –Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria - Violation Severity Levels

Violation Severity Levels (VSLs) define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

Violation severity levels should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

FERC's VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline 1 – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline 2 – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3 – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline 4 – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the

Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification – VAR-002-3 Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium is necessary because this requirement could affect the stability of the BES, but the requirement itself addresses instances where a GOP will not necessarily operate in with the AVR in different control modes or when the TOP will instruct a GOP to operate in other modes.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although the Blackout Report list Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, the GOP control modes are not as critical because the TOP is monitoring the system. The companion requirement to VAR-002-3 (in VAR-001-4) are properly designated with a HIGH VRF to ensure voltage schedules are provided as part of the TOPs plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The VRF applies to the entire requirement.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: Because maintaining a voltage schedule is critical to preventing a violation of a System Operating Limit, this VRF was drafted to be the same VRFs for VAR-001-4 Requirement R5. VAR-001-4 Requirement R5 requires the TOP to specify a schedule and notification requirements that the GOP must follow.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a GOP not operating in the proper control mode can affect the BES, but a single violation is unlikely to lead to instability, separation, or cascading failure. This is especially the case since a TOP will also be monitoring for voltage deviations.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More Than One Obligation:

	This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level.

VSL Justification – VAR-002-3 Requirement R1	
NERC VSL Guidelines	Consistent with NERC's VSL Guideline, this VSL acknowledges the criticality of this requirement and whether or not a system voltage schedule was created.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The current level of compliance is not lowered with the proposed VSL because this requirement only has a "severe" VSL.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary, and therefore, a single severe VSL is necessary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is consistent with the corresponding requirements.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on a cumulative number of violations.

VRF Justification – VAR-002-3 Requirement R2	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium is consistent with the NERC VRF definition. Requirement R2 focuses on GOPs maintaining a schedule, but there could be system events that will pull a GOP out of schedule. Also, late at night and early in the morning, the system may experience instances of low or high voltage. This could impact the BES, but a single instance is unlikely to lead to instability, separation, or cascading failure. The sub-requirements also require the GOP to modify the voltage schedule when directed by the TOP.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although the Blackout Report lists Reactive Power and voltage control as critical areas where a violation could severely affect the reliability of the Bulk-Power System, there are general times when a GOP will be unable to maintain a voltage schedule due to system condition. These instances occur frequently during the early morning and late at night. The companion requirement to VAR-002-3 (in VAR-001-4) are properly designated

	with a HIGH VRF to ensure voltage schedules are provided as part of the TOP's plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The VRF applies to the entire requirement, including all sub-parts.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: Because maintaining a voltage schedule is critical to preventing a violation of a System Operating Limit, this VRF was drafted to be the same VRFs for VAR-001-4 Requirement R5. VAR-001-4 Requirement R5 requires the TOP to specify a schedule and notification requirements that the GOP must follow.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a GOP not maintaining a schedule can affect the BES, but a single violation is unlikely to lead to instability, separation, or cascading failures. This is especially the case since a TOP will also be monitoring for voltage deviations
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation: This VRF does not co-mingle multiple objectives, nor does it water down the requirement to reflect a lower risk level.

VSL Justification – VAR-002-3 Requirement R2	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines, the VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering	There is no prior compliance obligation related to the subject of this standard.

the Current Level of Compliance	
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation,	The proposed VSL is not based on cumulative number of violations.

Not on A Cumulative Number of Violations	

VRF Justification – VAR-002-3 Requirement R3	
Proposed VRF	**Medium**
NERC VRF Discussion	This requirement warrants a Medium VRF and is consistent with the NERC definition because this requirement is whether the GOP made the required notifications to the TOP within the appropriate timeframes.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although the Blackout Report list Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, the GOP notifications are unlikely to lead to system instability, separation, or cascading failures. This is particularly the case because the TOP is still operating the system to stay within System Operating Limits and Interconnection Reliability Operating Limits.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: There is no sub-part to Requirement 3; therefore, the requirement is consistent.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: This VRF is drafted to be consistent with other standards (e.g., BAL) that address making appropriate notifications.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because not making the appropriate notifications can impact the grid, but the TOPs are still effectively monitoring the system; thus, instability, separation, or cascading failures are unlikely due to a single violation.
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level

VSL Justification – VAR-002-3 Requirement R3	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The current level of compliance is not lowered with the proposed VSL.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary because the standard is violated only when a notification is not made to the TOP; therefore, a severe VSL is warranted. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be	The proposed VSL is worded consistently with the corresponding requirement.

Consistent with the Corresponding Requirement	
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

VRF Justification – VAR-002-3 Requirement R4	
Proposed VRF	**Medium**
NERC VRF Discussion	This requirement warrants a Medium VRF and is consistent with the NERC definition because this requirement is whether the GOP made the required notifications to the TOP within the appropriate timeframes.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although the Blackout Report list Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, the GOP notifications are unlikely to lead to system instability, separation, or cascading failures. This is particularly the case because the TOP is still operating the system to stay within System Operating Limits and Interconnection Reliability Operating Limits.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: There is no sub-part to Requirement 3; therefore, the requirement is consistent.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: This VRF is drafted to be consistent with other standards (e.g., BAL) that address making appropriate notifications.

FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because not making the appropriate notifications can impact the grid, but the TOPs are still effectively monitoring the system; thus, instability, separation, or cascading failures are unlikely due to a single violation.
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level

VSL Justification – VAR-002-3 Requirement R4	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The current level of compliance is not lowered with the proposed VSL.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary because the standard is violated only when a notification is not made to the TOP; therefore, a severe VSL is warranted.

"Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

VRF Justification – VAR-002-3 Requirement R5	
Proposed VRF	**Lower**
NERC VRF Discussion	This requirement is a Lower VRF because the tap setting data does not change frequently, and a violation is not expected adversely affect the BES.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, this requirement would not adversely impact the BES

	if violated. The tap information is provided during interconnection, and it is not expected to change frequently. Therefore, a Lower VRF is warranted.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The parts within Requirement R5 are consistent with Requirement R5 and is considered a Lower VRF.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: There are no other standards that address Tap settings.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a violation is similar to an administrative violation. Further, since tap settings are infrequently changed, a violation would not adversely impact the BES.
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation: This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level.

VSL Justification – VAR-002-3 Requirement R5	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering	There is no prior compliance obligation related to the subject of this standard.

the Current Level of Compliance	
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation,	The proposed VSL is not based on cumulative number of violations.

Not on A Cumulative Number of Violations	

VRF Justification – VAR-002-3 Requirement R6	
Proposed VRF	**Lower**
NERC VRF Discussion	This requirement is a Lower VRF because the tap setting data does not change frequently, and a violation is not expected adversely affect the BES.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, this requirement would not adversely impact the BES if violated. The tap information is provided during interconnection, and it is not expected to change frequently. If a violation were to occur, the system would still operate at the level prior to making any tap setting changes. Therefore, a Lower VRF is warranted.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The part within Requirement R6 is consistent with Requirement R6 and is considered a Lower VRF.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: There are no other standards that address Tap settings.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a violation is similar to an administrative violation. Further, since tap settings are infrequently changed, a violation would not adversely impact the BES.
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation:

	This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level.

VSL Justification – VAR-002-3 Requirement R6	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary because the requirement focuses on whether tap changes were made. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

Exhibit F

Summary of Development History and Record of Development

Project 2013-04 Voltage & Reactive Control

Related Files

Status:
The NERC Board of Trustees adopted VAR-002-3 on May 7, 2014. The standard will be filed for regulatory approval.

Background:
When the first versions of the VAR standards were approved in FERC Order No. 693,[1] the Commission also issued several directives with regard to how to improve the standard. Each of the outstanding directives are explained in detail in the technical white paper (see project page).

The informal consensus building for VAR began in February 2013. Specifically, the ad hoc group engaged stakeholders on how best to address the FERC directives, remove paragraph 81 candidates, and implement results-based approaches. A discussion of the ad hoc group's consensus building and collaborative activities are also included in the technical white paper.

Based on stakeholder outreach, the VAR-001 and VAR-002 standards have been modified. The proposed VAR-001 answers most of the FERC directives from Order No. 693, and VAR-002 has been modified to address certain compliance issues today. This posting is soliciting comment on a pro forma standard and a Standard Authorization Request (SAR).

---

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

Draft	Action	Dates	Results	Consideration of Comments
VAR-002-3 Clean (72)|Redline to last posted (73) Implementation Plan Clean (74) |Redline to last posted (75) Supporting Materials: Compliance Input (76) Mapping Document Clean (77)|Redline to last posted (78) Draft Reliability Standard Audit Worksheet VAR-002-3 (79) VRF and VSL Justifications (80)	Final Ballot Info (81) Vote>>	04/24/14 - 05/05/14	Summary (82) Ballot Results (83)	
VAR-002-3 Clean (56) |Redline to last posted (57) Implementation Plan Clean (58) |Redline to last posted (59)	Additional Ballot and Non-binding Poll Info (66) Vote>>	04/04/14 – 04/14/14 (Extended in order to achieve quorum) (Closed)	Summary (68) Ballot Results (69) Non-Binding Poll Results (70)	

Supporting Materials: Unofficial Comment Form (Word) (60) Compliance Input (61) Mapping Document Clean (62) |Redline to last posted (63) Draft Reliability Standard Audit Worksheet VAR-002-3 (64) VRF and VSL Justifications (65)	Comment Period Info (67) Submit Comments>>	02/27/14 - 04/14/14		Consideration of Comments (71)
VAR-001-4 Clean (42)|Redline to last posted (43) Implementation Plan Clean (44) |Redline to last posted (45) Supporting Materials: Compliance Input (46) Mapping Document Clean (47) |Redline to last posted (48) Draft Reliability Standard Audit Worksheet VAR-001-4 (49) VRF/VSL Justifications (50) Consideration of Issues and Directives (51)	Final Ballot Updated Info (52) Info (53) Vote>>	12/13/13 - 12/23/13 (Revised) (closed)	Summary (54) Ballot Results (55)	
VAR-001-4 Clean (20) |Redline to last posted (21) VAR-002-3 Clean (22) |Redline to last posted (23) Implementation Plan Clean (24)|Redline to last posted (25)	Additional Ballots and Non-binding Polls Updated Info (32) Info (33) Vote>>	11/15/13 – 11/26/13 Extended 1 additional day, closing 11/26/13. (closed)	Summary (35) Ballot Results: VAR-001-4 (36) VAR-002-3 (37)	

Supporting Materials: Unofficial Comment Form (Word) (26) Compliance Input (27)			Non-Binding Poll: VAR-001-4 (38) VAR-002-3 (39)	
Mapping Document Clean (28) |Redline to last posted (29) Draft Reliability Standard Audit Worksheet VAR-001-4 (30) VAR-002-3 (31)	Comment Period Info (34) Submit Comments>>	10/11/13 – 11/25/13 (closed)	Comments Received (40)	Consideration of Comments (41)
Draft Standard VAR-001-4 (1) VAR-002-3 (2) Implementation Plan(3) Standard Authorization Request (4) Supporting Materials: Unofficial Comment Form (Word) (5) Technical White Paper (6) Mapping Document (7) Compliance Input (8) Proposed Timeline for the Formal Development (9)	VAR-001-4 and VAR-002-3 Ballot and Non-binding Poll Updated Info (10) Vote>>	08/23/13 - 09/03/13 Extended 1 additional day, closing 9/4/13. (closed)	Summary (14) Ballot Results (15) Non-binding Poll Results (16)	Consideration of Comments for VAR-002-3 (18) Consideration of Comments (19)
	Comment Period Info (11) Submit Comments>>	07/19/13 - 09/03/13 Extended 1 additional day, closing 9/4/13. (closed)	Comments Received (17)	
	Join Ballot Pool>>	07/19/13 - 08/19/13 (closed)		
	Info (12) Submit Nomination>> Unofficial Nomination Form (13)	07/24/13 - 08/02/13 (closed)		

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on July 19, 2013

Description of Current Draft

This draft standard is concluding informal development and will move to formal development when authorized by the Standards Committee.

Anticipated Actions	Anticipated Date
SAR Authorized by the Standards Committee	July
45 Day SAR Comment and Initial Ballot Open	July
Nomination Period Opens	July
Standard Drafting Team Appointed	July
Initial Comment and Initial Ballot Closes	August
Final Ballot Opens	October
Final Ballot Closes	October
BOT Adoption	November
Filing to Applicable Regulatory Authorities	December

Effective Dates

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

Version History

Version	Date	Action	Change Tracking
1	6/18/2007	Initial Standard is FERC approved	
2	1/10/2011	FERC approved added LSEs and Controllable Load to the standard.	
3	6/20/2013	WECC Variance is approved by FERC	

Definitions of Terms Used in the Standard

None.

Introduction

1. **Title:** Voltage and Reactive Control
2. **Number:** VAR-001-4
3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real time to protect equipment and the reliable operation of the Interconnection.
4. **Applicability:**
   - **4.1.** Transmission Operators
   - **4.2.** Reliability Coordinators
   - **4.3.** Generator Operators within the Western Interconnection

Requirements and Measures

Rationale for R1: This requirement will allow each Transmission Operator (TOP) to establish its own policies and procedures, and the criteria for periodic updates will be individualized based on the stability of each TOP's regions. The language is refined to show that coordination with neighboring TOPs is required. It also states TOP shall provide data to the Reliability Coordinator (RC) for its monitoring functions to respond to address the FERC directive in P 1855 of Order No. 693, which directed NERC to add RC monitoring to the VAR standards. P 1868 requires NERC to add more "detailed and definitive requirements to include more detailed and definitive requirements on “established limits” and “sufficient reactive resources” and identify acceptable margins (i.e. voltage and/or reactive power margins)."

R1. Each Transmission Operator shall have documented policies or procedures that are implemented to establish, monitor, and control voltage levels and Reactive Power flows (Mvar flows) within limits as defined below. *[Violation Risk Factor: High] [Time Horizon: Operations]*

1.1. These documented policies or procedures shall include criteria used in system assessments. The criteria for the assessments shall include established steady-state limits, voltage stability limits and associated operating margins, and voltage schedules along with associated tolerance bands.

1.2. Each Transmission Operator shall provide a copy of these documented policies or procedures to adjacent Transmission Operators.

1.3. Each Transmission Operator shall provide a copy of these documented policies or procedures to its Reliability Coordinator.

M1. The Transmission Operator shall have evidence of documented policies or procedures as specified in Requirement 1. As stated in R1, the policies and procedures must detail how criteria for steady-state and voltage stability limits are used in the Transmission Operator’s assessments of the system. In order to demonstrate the Transmission Operator is implementing the policies or procedures, the Transmission Operator must be able to provide evidence that proves voltage is currently being monitored. Such evidence may include, but is not limited to: 1) proof that points are telemetered, 2) alarms are functioning, and 3) during events of low or high voltage the policies and procedures are being followed to respond to control voltage levels. The Transmission Operator must also provide evidence that the policies or procedures were communicated to adjacent Transmission Operators and to its Reliability Coordinator. Evidence may include, but is not limited to, emails, website postings, and meeting minutes. Simply posting a copy of the policies or procedure on a public website is not sufficient if the Transmission Operator and Reliability Coordinator were not notified as to where to find the policies or procedures.

Rationale for R2:

P 1875 from Order No. 693 directed NERC to include requirements to run voltage stability analysis periodically. The informal ad hoc group and industry participants concluded that the best models and tools are the ones that have been proven over time, and that the requirement should not require any utility to purchase new online simulations tools. Therefore, the new requirement does not specify when to use online tools. The sub-requirements detail the real-time and day-ahead assessments necessary under R1. The existing VAR-001 also requires a list of sufficient reactive resources; this was retained in the proposed requirement as FERC determined in a letter order that this list answered the directive in P 1868 to detail the list of "sufficient reactive resources." Controllable load is specifically included to answer FERC's directive in P 1879.

R2. Each Transmission Operator and Reliability Coordinator shall perform assessments on their respective areas in order to ensure sufficient reactive resources are available for scheduling to maintain voltage stability under normal and contingency conditions in order to provide the voltage levels as defined in Requirement R1. *[Violation Risk Factor: High] [Time Horizon: Operations]*

2.1. Each Transmission Operator shall operate or direct the real-time operation of devices necessary to regulate transmission voltage and reactive flow necessary to regulate transmission voltage and reactive flow which may include, but is not limited to reactive generation scheduling; transmission line and reactive resource switching; controllable load; and, if necessary, load shedding, to maintain system voltages within established limits.

2.2. As a result of the assessments, each Transmission Operator shall ensure that sufficient reactive resources have been scheduled to meet acceptable day-ahead voltage limits identified in Requirement R1. Sufficient reactive resources may include, but is not limited to reactive generation scheduling; transmission line and reactive resource switching; and controllable load.

M2. Each Transmission Operator and Reliability Coordinator shall have evidence of current or past studies used to schedule sufficient reactive resources. Each Transmission Operator shall also provide proof that additional resources were scheduled when necessary. During a real-time event where voltage must be adjusted, a Transmission Operator shall show evidence to show directions were given to adjust the operation of capacitive and inductive resources. This may include directions to Generator Operators to operate within new tolerance bands or to make manual adjustments if necessary. Transmission Operators shall also have evidence to show proof of directing new resources to come online. Those resources can include, but is not limited to capacitor banks, switching, adjusting controllable load, and when necessary load can be shed. For the day-ahead scheduling, Transmission Operators shall provide copies of provide day-ahead studies used to schedule enough resources to meet expected voltage requirements.

Rationale for R3:

These exemptions offer TOPs the option to exempt certain generators during maintenance or system events when those units are not able to maintain voltage schedules. Sub-requirements containing an exemption list were removed from the existing standard because this created more compliance issues with regard to how often the list would be updated and maintained.

R3. The Transmission Operator shall specify the criteria that will exempt generators from compliance with the requirements defined in Requirement 4 and any associated notification requirements. *[Violation Risk Factor: Lower] [Time Horizon: Operations]*

3.1. In the event a Transmission Operator approves a generator as satisfying the criteria, it shall notify the associated Generator Operator.

M3. Each Transmission Operator shall have evidence of the documented criteria for generator exemptions. The Transmission Operator shall also have evidence to show that, for each generating unit in its area that is exempt from following a voltage or Reactive Power schedule, the associated Generator Owner was notified of this exemption in accordance with Requirement 3. Temporary exemptions maybe provided to generators during scenarios where notifications/communications are not necessary due to a system event that prevents a Generator Operator from maintaining a schedule. Similarly, when an Automatic Voltage Regulator (AVR) is malfunctioning, which prevents a Generator Operator from maintaining a voltage schedule and tolerance band, temporary exemptions may be provided. For temporary exemptions, evidence showing the exemptions were granted must be provided. If the exemptions were given verbally from the Transmission Operator, the phone recordings or emails commemorating the phone call must be provided. For temporary exemptions, the evidence of communication must also include the timeframe for how long the exemption will last.

Rationale for R4:

The new requirement adds “tolerance band” in order to provide more detailed information when establishing limits.

R4. Each Transmission Operator shall specify a voltage or Reactive Power schedule and tolerance band (at either the high side or low side of the Generator Step-Up transformer at the TOP's discretion)

at the interconnection point between the generator facility and the Transmission Owner's facilities to be maintained by each generator. *[Violation Risk Factor: Medium] [Time Horizon: Operations]*

4.1. The Transmission Operator shall provide the voltage or Reactive Power schedule and tolerance band to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).

M4. The Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule and tolerance band as specified in Requirement 4 to the applicable Generator Operators. For real-time directives, evidence may include recorded phone logs.

Rationale for R5:

Since power system stabilizers (PSS) equipment is not highlighted in any other standard, the VAR standard is the appropriate place to ensure the equipment is being monitored. This requirement is not duplicative of the TOP standards because the voltage regulators and power system stabilizer are highlighted.

R5. The Transmission Operator shall know the status of all transmission Reactive Power resources, automatic voltage regulators, and power system stabilizers in their system. *[Violation Risk Factor: Medium] [Time Horizon: Operations]*

M5. The Transmission Operator shall have evidence to show Reactive Power resources are being monitored. Evidence may include, but is not limited to screen shots of EMS/SCADA data, alarms, and phone logs. In the event the monitoring system does not work, each Transmission Operator should have a protocol in place to show these resources are being monitored.

Rationale for R6:

Although tap settings are first established at interconnection, this requirement could not be deleted because no other standard addresses when a tap setting must be adjusted. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

R6. After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes. *[Violation Risk Factor: Lower] [Time Horizon: Operations]*

M6. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit’s step-up transformer tap in accordance with the requirement.

Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The Transmission Operator shall retain evidence for Measures 1 through 4 for 12 months. The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations**	**High**	The Transmission Operator has documented criteria for assessments, but has provided a copy to only one of the parties that should have received a copy (either a neighboring TOPs or its RC).	The Transmission Operator has documented policies and procedures, but has not provided copies to either the neighboring TOPs or its RC.	The Transmission Operator has documented policies or procedures, but none of the sub-requirements were followed.	The Transmission Operator has no documented policies or procedures.
R2	**Operations**	**High**	N/A	The Transmission Operator only performs day-ahead assessments and only schedules day-ahead resources.	N/A	The Transmission Operator does not perform assessments and therefore does not have policies and procedures implemented to have sufficient Mvars. A lack of real-time operations is also severe.
R3	**Operations Planning**	**Lower**	N/A	N/A	N/A	The Transmission Operator does not have exemption criteria.
R4	**Operations**	**Medium**	N/A	N/A	The Transmission Operator provides voltage or Reactive Power schedules to only some of the GOPs.	The Transmission Operator does not provide voltage or Reactive Power schedules and tolerance bands at all.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	**Operations**	**Lower**	N/A	The Transmission Operator is unaware of the status in a stable area.	The Transmission Operator does not know the status of important equipment in weaker areas that were identified in assessments as part of R1.	N/A
R6	**Operations**	**Lower**	Either the technical justification or timeframe are not provided.	Neither the technical justification nor the timeframe are provided.	N/A	N/A

Regional Variances

Regional Variance for the Western Electricity Coordinating Council from VAR-001-3 is retained.

Interpretations

None.

Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please see the VAR White Paper for further technical information.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on July XX, 2013

Description of Current Draft

This draft standard is concluding informal development and will move to formal development when authorized by the Standards Committee.

Anticipated Actions	Anticipated Date
SAR Authorized by the Standards Committee	July
45 Day SAR Comment and Initial Ballot Open	July
Nomination Period Opens	July
Standard Drafting Team Appointed	July
Initial Comment and Initial Ballot Closes	August
Final Ballot Opens	October
Final Ballot Closes	October
BOT Adoption	November
Filing to Applicable Regulatory Authorities	December

Effective Dates

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

Version History

Version	Date	Action	Change Tracking
1	5/1/2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and 2.4.3.	July 5, 2006
1a	12/19/2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	1/16/2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	**Errata**
1.1a	10/29/2008	BOT adopted errata changes; updated version number to "1.1a"	**Errata**
1.1b	3/3/2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	**Revised**
2b	4/16/2013	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4. FERC Order issued approving VAR-002-2b.	Revised

Definitions of Terms Used in the Standard

None.

Introduction

1. **Title:** **Generator Operation for Maintaining Network Voltage Schedules**
2. **Number:** VAR-002-3
3. **Purpose:** To ensure generators provide reactive and voltage control necessary to ensure voltage levels, reactive flows, and reactive resources are maintained within applicable Facility Ratings to protect equipment and the reliable operation of the Interconnection.
4. **Applicability:**
   - **4.1.** Generator Operator
   - **4.2.** Generator Owner

Requirements and Measures

Rationale for R1: This requirement has been maintained due to the importance of running a unit with its automatic voltage regulator (AVR) in service and in voltage controlling mode. The measure has been updated include some of the evidence that can be used for Compliance purposes.

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless the Generator Operator has notified the Transmission Operator of one of the following: [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]

- That the generator is being operated in start-up[1] or shutdown[2] mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in the automatic voltage control mode for a reason other than start-up or shutdown.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode as specified in Requirement 1. If a generator is being started up or shut down with the automatic voltage control off and no notification of the automatic voltage regulator status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode. Such evidence must include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached.

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.
[2] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

Rationale for R2:

R2 details how a Generator Operator (GOP) operates the system to a maintain voltage schedule and when the GOP is expected to notify the Transmission Operator (TOP). Sub-requirement 2.1 provides guidance on a non-compliance window in the event a unit is deviating from schedule, and the GOP must notify the TOP if it is unable to return to schedule. Thus, the non-compliance window allows for notifications when a unit is unable to provide additional VAR support (e.g., when hitting an operational limit) or when the unit is too small to raise voltage. In both instances, the TOP may then provide some type of temporary exemption as outlined in VAR-001.

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within applicable Facility Ratings[4]) as directed by the Transmission Operator. [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]

2.1. If a GOP drifts out of schedule, each Generator Operator shall notify its associated Transmission Operator within 15 minutes when both of the following conditions are met: 1) the GOP is operating outside of the prescribed voltage or Reactive Power schedule tolerance band[5] for 15 minutes; and 2) the GOP is no longer able to return to its voltage or Reactive Power schedule.

2.2. When a generator's automatic voltage regulator is out-of-service, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.

2.3. When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

M2. Generator Operators will still make all attempts to operate within the tolerance bands provided by the TOP, but natural drifting may occur. In instances where there is an event occurring to pull a unit out of the tolerance band, the Generator Operator will not be held in non-compliance with this requirement if the sub-requirements 2.1, 2.2, and 2.3 are met. In order to identify when a unit is deviating from its schedule, GOPs will monitor voltage based on existing equipment at its facility. Therefore, GOPs have the option to operate on a voltage schedule on either the high-side or convert the high-side schedule to a low-side schedule at the GOP's discretion. For units that monitor on the low-side/terminal voltage, Generator Operators shall provide evidence of the method of conversion from the high-side schedule to low-side monitoring. For sub-requirement 2.1, most units will not be able to return to schedule due to a limiting factor. Such limiting factors may include, but are not limited to: 1) terminal voltage, 2) bus voltage, 3) equipment temperature,

[3] The voltage or Reactive Power schedule is a target value communicated by the Transmission Operator to the Generator Operator establishing a tolerance band within which the target value is to be maintained during a specified period.

[4] When a Generator is operating in manual control, reactive power capability may change based on stability considerations and this may lead to a change in the associated Facility Ratings.

[5] GOPs monitor and control voltage based on their equipment limitations. GOPs will monitor their voltage or Reactive Power schedule tolerance bands either at the high-side or low-side/terminal voltage.

4) transformer, 5) auxiliary equipment, 6) Volts/Hz limits, and 7) excitation or regulator limits. GOP shall have evidence to show compliance with requirement R2 by providing 1) Communications with the TOP when the Generator Operator was operating outside of the prescribed voltage or Reactive Power schedule tolerance band for 30 minutes or less (the 30 minutes allow for 15 minutes to call and 15 minutes to be outside of the tolerance band) AND Generator Operator is no longer able to return to its voltage or Reactive Power schedule; 2) Generator Operator implemented an alternative method to control reactive output when the AVR was out-of-service or unavailable; 3) compliance with directive to modify voltage or a notification that the directive could not be met. Evidence may include, but is not limited to Generator Operator logs, SCADA data, phone logs, and any other alarming notifications that would alert the Transmission Operator that both conditions were met. Timing for Requirement R2.1 is crucial, and Generator Operators are expected to begin timing an event as soon as the unit is operating outside of the tolerance band. Further, voltage documentation during a system event maybe requested by an auditor to show measures were taken to bring the unit back into schedule.

Rationale for R3:

This requirement has been modified to reduce the number of violations for when an AVR goes out-of-service and then comes back in-service. Fifteen (15) minutes have been built into the requirement to allow a Generator Operator time to resolve an issue before having to notify the Transmission Operator of a status or capability change. The requirement has also been amended to remove the sub-requirement to provide an estimate for the expected duration of the status change. The 15-minute window should resolve most issues, and further trouble-shooting will probably be required if the status change is unresolved within 15 minutes.

R3. Each Generator Operator shall notify its associated Transmission Operator of a status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability within 30 minutes of the change. If the status has been restored within the first 15 minutes of such change, then there is no need to call the TOP. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any of the changes identified in Requirement 3. If the status has been restored within the first 15 minutes, no call is necessary; therefore, if a status on Reactive Power resource has changed, and that change lasts greater than 15 minutes, the GOP must notify its associated TOP within 30 minutes of when the change first occurred.

Rationale for R4:

This requirement and corresponding measure language has been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

R4. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

4.1. For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

4.1.1. Tap settings.

4.1.2. Available fixed tap ranges.

4.1.3. Impedance data.

M4. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirements 4.1.1 through 4.1.3.

Rationale for R5:

This requirement and corresponding measure language has been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

R5. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations].*

5.1. If the Generator Operator can't comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.

M5. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation as identified in Requirement 5. The Generator Operator shall have evidence that it notified its associated Transmission Operator when it couldn't comply

with the Transmission Operator's step-up transformer tap specifications as identified in Requirement 5.1.

Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. The Generator Operator shall maintain all other evidence for the current and previous calendar year.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The responsible entity did not operate each generator in the automatic voltage control mode and failed to notify the Transmission Operator as identified in R1.
R2	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The responsible entity did not perform any of the sub-requirements.
R3	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The responsible entity did not make the notification within 30 minutes.
R4	**Real-time Operations**	**Lower**	When directed by the Transmission Operator to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for up to and including 45 minutes.	When directed by the Transmission Operator to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for more than 45 minutes up to and including 60 minutes. OR When a generator's automatic voltage regulator is out of service, the Generator Operator	When directed by the Transmission Operator to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for more than 60 minutes up to and including 75 minutes.	When directed by the Transmission Operator to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for more than 75 minutes. OR When a generator's automatic voltage regulator is out of service, the Generator Operator failed to use an alternative method to control the

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				failed to use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator. OR The Generator Operator failed to provide an explanation of why the voltage schedule could not be met.		generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator and the Generator Operator failed to provide an explanation of why the voltage schedule could not be met.
R5	**Real-time Operations**	**Lower**	N/A	N/A	N/A	The GOP failed to perform the tap changes, and the GOP did not provide technical justification for why it cannot comply with the TOP directive

Regional Variances

None.

Interpretations

None.

Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please see the VAR White Paper for further technical information.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan
VAR Directives Project

Implementation Plan for VAR-001 and VAR-002

Approvals Required
VAR-001-4 – Voltage and Reactive Control
VAR-002-3 — Generator Operation for Maintaining Network Voltage Schedules

Prerequisite Approvals
There are no other standards that must receive approval prior to the approval of this standard.

Revisions to Glossary Terms
None

Applicable Entities
Generator Operators
Generator Owners
Transmission Operators
Reliability Coordinators

Applicable Facilities
N/A

Conforming Changes to Other Standards
None

Effective Dates
VAR-001-4 and VAR-002-3 - In those jurisdictions where regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter after applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter after Board of Trustees approval.

Justification

The currently effective VAR-002 standard is one of the most violated standards; however, the industry argues these violations do not address any reliability gaps. Instead, Generator Operators and Transmission Operators are required to handle many nuisance phone calls for slight deviations from a voltage schedule. The nuisance phone calls can be a distraction during a scheduled maintenance or a system event; thus, the industry would support making the changes as soon as possible. However, since VAR-001 now requires a documented policy or procedure for assessments; the Transmission Operators need a quarter to prepare documentation. Also for Transmission Operators that do not provide tolerance bands with voltage schedules, those Transmission Operators will need some time to adjust to providing new data to Generator Operators.

Retirements

VAR-001-3 and VAR-002-2b will be retired at midnight of the day immediately prior to the Effective Date of VAR-001-4 and VAR-002-3 in the particular Jurisdiction in which the new standards are becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, please email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard:	Voltage and Reactive Control; Generator Operation for Maintaining Network Voltage Schedules		
Date Submitted:	July 18, 2013		
SAR Requester Information			
Name:	Soo Jin Kim		
Organization:	NERC		
Telephone:	404-446-9742	E-mail:	soo.jin.kim@nerc.net
SAR Type (Check as many as applicable)			
☐ New Standard ☒ Revision to existing Standard		☐ Withdrawal of existing Standard ☐ Urgent Action	

SAR Information
Industry Need (What is the industry problem this request is trying to solve?):
Resolve FERC directives from FERC Order No. 693 and improve upon the existing VAR standards.
Purpose or Goal (How does this request propose to address the problem described above?):
The pro forma standard consolidates the reliability components of the existing VAR-001 standard, adds new requirements to address FERC's directives in Order No. 693, and provides a non-compliance window in VAR-002 notification requirements.

SAR Information
Identify the Objectives of the proposed standard's requirements (What specific reliability deliverables are required to achieve the goal?):
The objectives are to address the outstanding directives from FERC Order 693 and added a non-compliance window for when a GOP must notifiy a TOP when a unit is deviating from a voltage schedule.
Brief Description (Provide a paragraph that describes the scope of this standard action.)

• The drafting team will answer the outstanding VAR directives from FERC Order No. 693. The VAR-001 directives are summarized from P 1880 of Order No. 693 as:
  ○ Expand the applicability to include reliability coordinators and LSEs;
  ○ Include detailed and definitive requirements on "established limits" and "sufficient reactive resources" and identify acceptable margins above the voltage instability points;
  ○ Include Requirements to perform voltage stability analysis periodically, using online techniques where commercially available and offline techniques where online techniques are not available, to assist real-time operations, for areas susceptible to voltage instability;
  ○ Include controllable load among the reactive resources to satisfy reactive Requirements; and
  ○ Address the power factor range at the interface between LSEs and the transmission grid.
• The VAR-002 directive is to simply consider adding more detail around what would constitute an incident of non-compliance for a Generator.
• The drafting team will also modify the VAR-002 standard in order to address some of the numerous notifications that are required by the currently enforceable standard.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
Detailed description of this project can be found in the Attachment (pro forma VAR standards) and White Paper of this SAR submittal package.

Reliability Functions

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☐ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☐ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐ Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐ Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐ Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☐ Transmission Owner	Owns and maintains transmission facilities.
☒ Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☐ Distribution Provider	Delivers electrical energy to the End-use customer.
☒ Generator Owner	Owns and maintains generation facilities.
☒ Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐ Purchasing-Selling	Purchases or sells energy, capacity, and necessary reliability-related

Reliability Functions		
	Entity	services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☐	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.
Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to	Yes

Reliability and Market Interface Principles	
access commercially non-sensitive information that is required for compliance with reliability standards.	

Related Standards	
Standard No.	Explanation
VAR-001- 3	Voltage and Reactive Control
VAR-002-2b	Generator Operation for Maintaining Network Voltage Schedules

Related SARs	
SAR ID	Explanation
Project 2008-01	Voltage and Reactive Planning and Control

Regional Variances	
Region	Explanation
ERCOT	None
FRCC	None
MRO	None

Regional Variances	
NPCC	None
RFC	None
SERC	None
SPP	None
WECC	VAR-001-3 WECC variance is retained.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2013-04 Voltage and Reactive Control (VAR) Revisions

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments on the draft VAR-001-4 and VAR-002-3 standards. The electronic comment form must be completed by 8:00 p.m. ET by **Tuesday, September 3, 2013**.

If you have questions please contact Soo Jin Kim via email or by telephone at 404-446-9742.

The project page may be accessed by clicking here.

Background Information

When the first versions of the VAR standards were approved in FERC Order No. 693,[1] the Commission also issued FERC issued several directives with regard to how to improve the standard. Each of the outstanding directives are explained in detail in the technical white paper (see project page).

The informal consensus building for VAR began in February 2013. Specifically, the ad hoc group engaged stakeholders on how best to address the FERC directives, remove paragraph 81 candidates, and implement results-based approaches. A discussion of the ad hoc group's consensus building and collaborative activities are also included in the technical white paper.

Based on stakeholder outreach, the VAR-001 and VAR-002 standards have been modified. The proposed VAR-001 answers most of the FERC directives from Order No. 693, and VAR-002 has been modified to address certain compliance issues today. This posting is soliciting comment on a pro forma standard and a Standard Authorization Request (SAR).

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

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

Question

1. Do you have any specific questions or comments relating to the scope of the proposed pro forma standard or SAR?

☐ Yes
☐ No

Comments:

2. Do you have any specific questions or comments relating to the requirements in the proposed pro forma standards?

☐ Yes
☐ No

Comments:

3. Do you have any issues with the proposed timeframes for the notification requirements in VAR-002 R2 and R3? If you propose different timeframes, please explain how a change in the timeframe will not create a reliability gap?

☐ Yes
☐ No

Comments:

4. During outreach, several issues pertaining to voltage coordination were discussed, as outlined in the 'minority issues' section of the technical white paper. However, those issues are not addressed because such issues are outside of the scope of this project. What suggestions do you have for improving voltage coordination between TOPs and GOPs? Is it appropriate to address this issue in a Standards project?

Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

White Paper on the VAR Standards

VAR-001 and VAR-002

July 18, 2013

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road N
Suite 600, North Tow
Atlanta, GA 3032
404-446-2560 | www.nerc.co

Table of Contents

Table of Contents 2
Executive Summary 3
Purpose 5
History of the VAR Informal Development 6
Technical Discussion 7
Background 7
VAR-001 7
VAR-002 8
Outstanding FERC Directives 11
Directive from P 1855 of Order No. 693 11
Directive from P 1858 of Order No. 693 11
Directive from P 1861 of Order No. 693 12
Directive from P 1862 of Order No. 693 12
Directive from P 1868 of Order No. 693 13
Directive from P 1869 of Order No. 693 13
Directive from P 1875 of Order No. 693 13
Directive from P 1879 of Order No. 693 14
Directive from P 1885 of Order No. 693 14
Conclusion 17
Entity Participants 18

Executive Summary

The VAR Reliability Standards provide the minimum requirements for maintaining voltage stability on the bulk-power system. The industry considers VAR-001 to represent transmission requirements for monitoring the reactive power performance of the system, and VAR-002 represents generator obligations for voltage support. When the VAR standards were initially approved by the Federal Energy Regulatory Commission ("FERC" or the "Commission") in 2006, the Commission provided several directives on how to improve the VAR standards. NERC initiated Project 2008-01 to address these FERC directives, but that project was unable to be completed due to a project reprioritization. Project 2008-01 and its Standard Authorization Request (SAR) used a prescriptive approach to address the FERC directives, and that project also contemplated adding an additional planning standard. This project took a different approach by implementing the Paragraph 81[1] and results-based standards initiatives. This project also utilized the recommendations from a panel of Independent Experts' Review of the NERC Reliability Standards. Due to this variance in approach, the informal development group is presenting a new SAR to post for industry comment.

In summary, FERC gave the following directives to modify VAR-001:

- Expand the applicability to include Reliability Coordinators (RCs) and load-serving entities (LSEs).
- Include detailed and definitive requirements on "established limits" and "sufficient reactive resources" and identify acceptable margins above the voltage instability points.
- To assist real-time operations for areas susceptible to voltage instability, include requirements to perform voltage stability analysis periodically, using online techniques where commercially available and offline techniques where online techniques are not available.
- Include controllable load among the reactive resources to satisfy reactive requirements.
- Address the power factor range at the interface between LSEs and the transmission grid.

FERC directed NERC to consider modifying VAR-002 to require more detailed and definitive requirements when defining the time frame associated with an "incident" of noncompliance. Hence, FERC directed NERC to consider a timeframe for allowing a generator to be out of schedule before having to make a notification to its TOP.

In early 2013, NERC initiated an informal development project to address the directives, and an informal development group was formed from industry subject matter experts, NERC staff, and staff from FERC's Office of Electric Regulation. The informal development group sought to answer FERC's directives and improve some of the compliance issues that exist today for the VAR standards. The informal development group drafted several pro forma versions of the VAR standard and sought broad industry feedback through individual phone conversations, conference calls, technical conferences, and webinars.

Since 2006, many changes have occurred that impact the VAR standards. Several new standards have been drafted and approved in the last seven years. Also, FERC recently issued a Notice of Proposed Rulemaking (NOPR) addressing Paragraph 81, and that NOPR recommends retiring certain VAR requirements that are redundant with Open-Access Transmission Tariffs (OATTs). In addition, VAR-002 has consistently been identified as one of the most violated standards, so certain compliance issues surround VAR-002 had to be addressed.

In concert with the Paragraph 81 initiative, each of the above-mentioned directives does not equate to a new VAR requirement. Instead, the informal development group removed certain redundancies with other standards and created requirements that provide for documented policies and procedures to address the above directives for VAR-001.

The pro forma VAR-001 has added RC monitoring requirements, and the standard requires each Transmission Operator (TOP) to have written operating policies and procedures used to define voltage limits. Those policies and procedures must set definitive guidelines on the frequency of system assessments. Further, the pro forma standard states that controllable load is a viable reactive power resource that can be used in the day-ahead and real-time operations. The informal development project did not address power factor, because the relevant requirement that currently addresses LSEs and

[1] *See North American Electric Reliability Corp.*, 138 FERC ¶ 61,193, at P 81, *order on reh'g and clarification*, 139 FERC ¶ 61,168 (2012).

power factor is proposed for retirement by FERC in its June 2013 NOPR on Paragraph 81 because the OATT covers the arrangement for ancillary services that include VAR purchases to maintain power factor.

Additionally, VAR-002 has been amended in the pro forma standard to provide for a noncompliance timeframe when a generator is out of voltage schedule and when reactive power equipment is out-of-service and then back in-service status again. The language not only addresses FERC's directive, but it also provides resolution to several compliance issues in existence today. Certain timing elements for VAR-002 may be debated during the formal development process, but the informal development group has reached a consensus on the principles of providing these time periods.

As detailed further below, the informal development group drafted the pro forma VAR standard in a manner that would accomplish three objectives: 1) address the FERC directives; 2) mitigate compliance issues for generators in VAR-002; and 3) simplify the TOP's requirements in VAR-001 while maintaining reliability and eliminating nuisance phone calls. The pro forma standard is not overly prescriptive, and Compliance has prepared guidance that will develop into RSAWs and auditor training. This guidance will allow for more predictability when the new VAR standard is implemented, and it will hopefully alleviate some industry concerns regarding future audits.

Purpose

The purpose of this white paper is to provide a summary of the issues, rationale, and support for the proposed revisions to the currently enforceable VAR standards, VAR-001 and VAR-002. This white paper also provides an explanation of how outstanding VAR directives from the Commission contained in Order No. 693[2] are addressed going forward. This white paper is a product of the informal development process, which provides for the formation of an informal development group. The informal development group met several times and conducted numerous webinars and technical conferences from February through June 2013. The information obtained through industry outreach was discussed thoroughly by the informal development group, and several of the discussion topics are reflected throughout this paper. In addition, the contents of this paper will give a foundation to the formal development process.

The ultimate goal of the Standards team is present the new VAR standards to the Board of Trustees in their November 2013 meeting. Thus, the formal Standards Drafting Team will be seeking final industry approval of the VAR standards by October 2013.

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

History of the VAR Informal Development

The informal development group started with a group of individuals that were originally part of Project 2008-01. Due to a project reprioritization conducted by the Standards Committee and NERC, Project 2008-01 was halted. There is some overlap between the current VAR project and project 2008-01, but the scope is slightly different. Project 2008-01 was moving toward creating a VAR planning standard in addition to modifying VAR-001 and VAR-002. The current project is only amending VAR-001 and VAR-002, and the current project remains predominantly focused on addressing the outstanding FERC directives.

The informal development group first met on a February 15, 2013 conference call. The meeting was to introduce the various parties and a coordinate logistics for the informal development process. The informal development group is currently comprised of the following:

- Dennis Chastain – Tennessee Valley Authority
- Bill Harm – PJM Interconnection L.L.C.
- Steve Hitchens – Bonneville Power Administration
- Sharma Kolluri – Entergy Services Inc.
- Martin Kaufman – ExxonMobil Research and Engineering Company
- Joshua Pierce – Southern Company
- Hari Singh – Xcel Energy
- Hamid Zakery – Calpine Corporation
- Scott Berry – Indiana Municipal Power Agency

Members of the informal development group met in person on February 27 and 28 in Atlanta. The group then convened several times over conference calls before an April 11 webinar.

The April 11 webinar was the first time the group proposed new VAR language to address a majority of the directives from Order No. 693. The industry provided significant feedback during two subsequent technical conferences. The first technical conference was hosted by Southern Company in Atlanta, Georgia, on April 18, 2013. The second technical conference was held at Xcel Energy in Denver, Colorado, on April 29, 2013. Both conferences provided an opportunity for the informal development group to listen to industry concerns regarding the VAR standards, and the informal development group answered numerous questions on the current draft of the pro forma standards.

The informal development group reconvened for a two-day meeting at Entergy on May 15, 2013. The group also invited several individuals who participated in the webinars and technical conferences to attend the meeting. During the May meeting, the VAR pro forma standard was modified several times. The informal development group continued the discussion on how to best address industry's concerns through electronic communications and several conference calls.

The next iteration of the pro forma standard was then presented to the industry on a June 14 webinar. The webinar contained several survey questions, and the informal development group was able to gauge whether a majority of industry supported the pro forma standard. Based on the survey and webinar feedback, the informal development group was able to amend the pro forma standard further before presenting the final draft to the Standards Committee on July 18, 2013.

Technical Discussion

Background

What is Reactive Power?

Reactive power does not have the same characteristics as real power. Real power is measured in watts and able to be transmitted over long distances. Real power is an energy supply that is eventually distributed to end-use customers. Reactive power is just as important as real power because it is necessary to maintain system stability. Reactive power supports voltage. Voltage is measured in volts, and electrical current is measured in amperes. Reactive power is measured in volt-amperes reactive (VARs). When the Bulk Electric System (BES) does not have enough reactive power, there is risk of a voltage collapse, which could lead to cascading outages. In fact, a lack of reactive power supply was a contributing factor to the large blackouts in 2003 and 2011.

Nature of Reactive Power and Why it is Necessary

Generally reactive power is needed to provide voltage support and maintain system stability. Prabha Kundur, a leading subject matter expert in system stability, explains, "[p]ower system stability may be broadly defined as that property of a power system that enables it to remain in a state of operating equilibrium under normal operating conditions and to regain an acceptable state of equilibrium after being subjected to a disturbance."[3] The VAR standards ensure that there is enough reactive power on the system to provide the voltage support necessary to avoid voltage collapse. Although there are numerous reactive power resources, the best and largest source of reactive power or VAR support comes from generators. However, the amount of reactive power that a generator can create is proportional to the amount of MWs being produced. Therefore, the more VARs produced at a generating facility, the fewer MWs produced.

VAR-001

The stated purpose of the VAR-001 standard is to ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real time to protect equipment and the reliable operation of the interconnection. The VAR standards focus on the Operations horizon (which is real-time up to one year into the future). The informal development group is cognizant of the fact that the nature of reactive power on the network varies depending on local conditions. Thus, the group focused on the process that the requirements would detail, not the proper numbers a TOP should enforce in the standard. For VAR-001, the group would not put operational limits on how a TOP should manage voltage stability for its regions; more specifically, the informal development group did not want to place numerical requirements on what the proper operational limits should be for the continent. Operating margins vary due to specific system characteristics as well as the operating conditions. Rather than detailing a continent-wide back-off margin, the informal development group designed the pro forma VAR-001 to require the Transmission Operator to document policies and procedures used to establish, monitor, and control voltage and reactive power flows (Mvars). Those policies are then used to establish voltage and reactive power schedules for the generators.

Requirement R1

R1 requires that documented policies and procedures are in place. These policies and procedures must include criteria for the assessments of the TOP's systems. The policies will consequently include studies used to establish voltage schedules and associated tolerance bands. In addition, the system assessments must include dynamic voltage limits and operating margins. By requiring a documented policy and procedure, the reliability standard removes the opportunity for auditors or other parties to scrutinize a TOP's own system studies.

R1 also requires Transmission Operators to communicate their policies and procedures with their associated RC and neighboring TOPs. This type of communication relates to R2, which details how a TOP and RC take a system study and ensure sufficient reactive power is available to support both real-time and day-ahead operations.

Requirement R2

[3] Prabha Kundur, *Power System Stability and Control,* Electric Power Research Institute, p. 17 (1994).

R2 requires both TOPs and RCs to perform system assessments in order to schedule reactive resources for both the real-time and day-ahead time frames. By scheduling sufficient reactive resources, the TOP and RC are maintaining voltage levels (and consequently system stability) under both normal and contingency situation. R2 further defines "sufficient reactive resources," and those resources include controllable load pursuant to FERC Order No. 693.

Requirement R3

R3 requires each TOP to specify what criteria will exempt a generator from 1) having to follow a provided voltage schedule; or 2) providing a notification under VAR-002. The TOP must notify the generator when an exemption is given, but there are no requirements on what the criteria should be for exemptions. This enables TOPs to have flexibility when providing exemptions during maintenance or system events. For example, if a unit is experiencing a malfunction in AVR equipment, the TOP may provide a temporary exemption to the generator until the equipment is repaired.

Requirement R4

R4 requires each TOP to specify a voltage or reactive power schedule and associated tolerance band for each generator. By requiring both a tolerance band and a documented policy or procedure for establishing voltage schedules, there is a level of transparency as to how voltage or reactive power schedules were created. The informal development group refrained from providing any language that requires GOPs to mutually agree with TOPs on specific numbers. Such language could create disputes between the parties as to what the appropriate voltage schedule should be for a unit. To preserve a TOP's ability to assess and monitor its system, and in an effort not to undermine the TOP standards, R4 provides more transparency while clearly maintaining a TOP's role in determining voltage schedules.

Requirement R5

R5 ensures that the TOP knows the status of all reactive power resources, automatic voltage regulators, and power system stabilizers in its system. This requirement mandates that the TOP actively monitor the system for voltage issues, and the new measure language now specifies that electronically metered points and EMS data will serve as a compliance mechanism for this particular requirement.

Requirement R6

The informal development group did not modify the requirement regarding step-up transformer tap changes.

WECC Variance

FERC approved the WECC variance to VAR-001 on June 20, 2013.[4] The WECC variance eliminates the TOP's ability to allow for exemptions, and it also requires a TOP to (1) issue a choice of voltage schedules for each of the generating resources that are on-line and part of the BES in its area; (2) provide to Generator Operators (GOPs) a voltage schedule reference point; and (3) provide transmission equipment data and operating data requested by GOPs to support their set point conversion methodology.[5] The informal development group did not adopt the WECC variance because it is more stringent than the existing standard, and numerous TOPs want the flexibility to allow for exemptions from notification requirements, particularly when maintenance is being performed or when a generator's AVR is malfunctioning. However, the current pro forma standard does not affect the WECC variance. Since the WECC variance is retained, the VAR-001 standard is applicable to GOPs in the WECC region.

VAR-002

The purpose behind the VAR-002 standard is for generators to provide reactive and voltage control necessary to ensure voltage levels, reactive flows, and reactive resources are maintained within applicable Facility Ratings to protect equipment and the reliable operation of the interconnection. Currently, VAR-002 is problematic due the numerous violations for GOPs 1) when a unit deviates from schedule; and 2) when an AVR turns on, then off. In both instances, a generator has an obligation under the currently enforceable standard to call a TOP within 30 minutes. The current standard does not allow for any deviations from notification requirements; thus, the GOP must determine if it is more appropriate to make a notification or address a potential issue that is affecting the voltage schedule or AVR status. The notifications themselves also create "nuisance" phone calls for TOPs. Most TOPs have the ability to monitor voltage through telemeter equipment.

[4] *See Petition for Approval of Proposed Reliability Standard VAR-001-3 (WECC Variance)*, Letter Order, Docket No. RD13-6-000 (issued June 20, 2013).
[5] *See* VAR-001-3

Thus, most TOPs already know when a unit drifts out of schedule. In order to address both the compliance issues and FERC's directive to consider a noncompliance window, the pro forma VAR-002 proposes language that gives a GOP time to respond to an issue before notifying its TOP.

Requirement R2

R2 requires GOPs to follow a TOP-provided voltage or reactive power schedule. However, there is universal agreement among TOPs and GOPs that if a unit drifts out of schedule momentarily and then drifts back into schedule, there is no risk to the reliability of the system. However, under the current VAR-002 standard in effect, when a unit drifts out of schedule there is an obligation to notify the TOP. Also, when the unit goes back into schedule there is an obligation to notify the TOP again. Thus, for a slight deviation, a GOP may face two potential violations for failure to make notifications to the TOP.

Based on industry feedback, a TOP should be notified when a unit cannot follow a voltage schedule. However, notifications for every schedule change are harmful to reliability because such calls detract focus from addressing system issues as they occur. The new language in the pro forma standard for R2 requires a GOP to notify a TOP when 1) the unit has been out of schedule for 15 minutes; AND 2) when a unit cannot return to schedule. In most cases, a unit will not be able to return to schedule when it has encountered an operating limit. There are also instances when a system event is pulling the unit out of schedule, and the unit is too small to move its voltage back in schedule. In these situations, it is important for the TOP to be notified, because those units cannot provide anymore voltage support to combat a system event.

Requirement R3

R3 requires a GOP to notify its TOP within 30 minutes of a "status" change. The status change identifies whether a reactive resource is available for voltage support. In an effort to allow GOP to first identify and address why a status change has occurred, the new pro forma standard Requirement R3 gives the GOP an initial 15 minutes to correct and restore the status of any reactive power resource. However, if the status has not been corrected after 15 minutes, the GOP has 15 minutes to notify its associated TOP of the status change.

Requirements R1, R4, and R5

The informal development group did not modify the requirement regarding AVR and tap changes.

Monitoring

Both R2 and R3 inherently have several compliance issues with regard to how voltage is monitored and controlled. Most TOPs provide GOPs with a voltage schedule as the high side of the generator step-up transformer, but a large number of GOPs only have metering equipment on the low side of the transformer. Therefore, in order to meet a voltage schedule, but these GOPs will convert the "high-side" schedule to a "low-side" schedule. The low-side schedule is then usually translated into an AVR control point or target. However, for several smaller facilities and nuclear facilities, those generators have installed metering on the high-side. Also, some facilities have made additions to their facilities to add load-drop compensation to see monitoring on the high-side. Thus, although many Generators monitor voltage on the low side of the terminal, there are a significant number of facilities that monitor voltage on the high side. Generators that use high-side voltage reference for regulation receive voltage reference signals from their associated TOP. This can create an issue during audits, because the standard does not dictate which method is acceptable for monitoring voltage.

In order to develop a continent-wide standard that allows GOPs to monitor voltage based on existing equipment limitations, the language of pro forma VAR-002's measures was greatly augmented. Specifically, the GOPs were explicitly given the discretion to monitor on either the high side or low side of the transformer. The pertinent language added to M2 is, "[i]n order to identify when a unit is deviating from its schedule, GOPs will monitor voltage based on existing equipment at its facility. Therefore, GOPs have the option to operate on a voltage schedule on the high side or convert the high-side schedule to a low-side schedule at the GOP's discretion." This language is necessary to assure GOPs that the standard will not determine where specific equipment should be installed at a facility. Further, this language clarifies to an auditor that either high-side or low-side monitoring is sufficient for VAR-002 compliance.

AVR

Once the AVR is set and in "voltage controlling" mode, the AVR should automatically adjust to voltage swings. At issue is whether a generator is required to make any adjustments to a control-point or AVR setting when the AVR response is not enough to react to a voltage deviation or system event. There is a current debate in the industry as to what actions are

required to maintain system stability. From the Generator's perspective, the AVR is the best mechanism to address voltage, and several Generators advocate that if an AVR setting should be adjusted, then the respective TOP should direct that AVR change. The TOPs argue that if an event is occurring, there is not enough time to call each generator to dictate the specifications for an adjustment; further, the TOPs assert that generators have an obligation to maintain a voltage schedule that includes making the necessary AVR adjustments. This industry divide is not addressed in the pro forma standard presented today. The informal development group did not address changing underlying principles of the VAR-002 standard, because the scope of the project with regard to VAR-002 was merely to consider a non-compliance window. However, the issue may be revisited during the formal development stage by the standard development team.

Minority Issue on Voltage Coordination

Another issue that arose during the informal outreach was the need for more voltage coordination between GOPs and TOPs. Some GOPs advocated for VAR standards to be re-written in order require more coordination, but again since the scope of this project is to focus on FERC directives, the informal development group opted to require more detail on how the TOPs study their systems. This issue will be presented for comment during the balloting of the pro forma, and the formal drafting team will make recommendations based on comments received as to how to address this issue in the future.

Outstanding FERC Directives

The VAR standards were first approved in FERC Order No. 693.[6] However, in approving the standards, the Commission also gave several directives on how to improve the VAR standards for reliability purposes. VAR-001 targets the transmission responsibilities for maintaining voltage stability while VAR-002 focuses on generator functions. Order No. 693 summarized the directives for VAR-001 as requiring NERC to do the following:

> (1) expand the applicability to include RCs and LSEs; (2) include detailed and definitive requirements on "established limits" and "sufficient reactive resources" as discussed above, and identify acceptable margins above the voltage instability points; (3) to assist real-time operations for areas susceptible to voltage instability include requirements to perform voltage stability analysis periodically, using online techniques where commercially available and offline techniques where online techniques are not available; (4) include controllable load among the reactive resources to satisfy reactive requirements; and (5) address the power factor range at the interface between LSEs and the transmission grid.[7]

For VAR-002, FERC directed NERC to consider providing more definitive requirements on what a noncompliance window should be for mandatory notifications. Each of the relevant directives is explained in further detail below.

Directive from P 1855 of Order No. 693

"Accordingly, the ERO should modify VAR-001-1 to include reliability coordinators as applicable entities and include a new requirement(s) that identifies the reliability coordinator's monitoring responsibilities."

VAR Informal Consideration

The informal development group amended VAR-001 to make RCs applicable to this standard, and requirements were added that identify RC monitoring for voltage stability. The informal development group did not expand the VAR standards to be overly prescriptive with regard to how an RC should monitor its own system; further, the group did not want to duplicate the efforts of the IRO standards pending before FERC. Instead the group focused on the most critical elements necessary for an RC to monitor its system for voltage stability. An RC performs many monitoring functions, but for voltage stability it is necessary to ensure that 1) the RC is aware of how its TOPs are monitoring voltage, and 2) the RC is performing the adequate studies to ensure reactive resources are properly scheduled for both real-time and day-ahead operations. Although some entities in Texas provided feedback that certain RCs perform functions equivalent to a TOP, the informal development group did not expand VAR-001 to give parity to TOPs and RCs. Upon further investigation, these situations are addressed through contractual obligations that clearly outline the reliability roles of both parties. The new RC functions are reflected in the new VAR pro forma standard through requirements R1 and R2. Both requirements are detailed further below.

Directive from P 1858 of Order No. 693

"The Commission directs the ERO to address the reactive power requirements for LSEs on a comparable basis with purchasing-selling entities."

VAR Informal Consideration

This FERC directive was addressed in VAR-001-2.[8] The Commission also recently issued a NOPR regarding Paragraph 81 that recommended retiring the existing VAR requirement that initially answered FERC's directive in P 1858.[9] FERC's support for Paragraph 81 and rationale for proposing the retirement is:

---

[6] *See generally,* Order No. 693 at PP 1846-1885.

[7] Order No. 693 at P 1880.

[8] *See* FERC letter order, *NERC Petition for Approval of Proposed Modifications to Reliability Standards BAL-002-1; EOP-002-3; FAC-002-1; MOD-021-2; PRC-004-2; and VAR-001-2,* 134 FERC ¶ 61,015 (2011).

[9] *See Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards,* Notice of Proposed Rulemaking, 143 FERC ¶ 61,251 (2013) ("NOPR").

> We propose to approve the retirement of VAR-001-2, Requirement R5 based on NERC's assertion that Requirement R5 is redundant with provisions of the *pro forma* OATT. Specifically, Schedule 2 of the open access transmission tariff requires transmission providers to provide reactive power resources, either directly or indirectly, and requires transmission customers to either purchase or self-supply reactive power resources.[10]

In light of this NOPR, the informal development group is not adding new language to the VAR standard that would address this directive. Further, there is an ongoing NERC effort to evaluate if purchasing-selling entities (PSEs) should continue to be a registered function. The informal development group may address this directive in the future, pending a final rulemaking from FERC and a determination on the status of the future applicability of standards to PSEs.

Directive from P 1861 of Order No. 693

"In the NOPR, the Commission asked for comments on acceptable ranges of net power factor at the interface at which the LSEs receive service from the Bulk-Power System during normal and extreme load conditions... The Commission believes that Reliability Standard VAR-001-1 is an appropriate place for the ERO to take steps to address these concerns by setting out requirements for transmission owners and LSEs to maintain an appropriate power factor range at their interface. **We direct the ERO to develop appropriate modifications to this Reliability Standard to address the power factor range at the interface between LSEs and the Bulk- Power System."**

VAR Informal Consideration

Initially, the informal development group addressed the directive on power factor in two ways. First, based on P 1863,[11] the informal development group considered requiring seasonal power factor data to be provided to the TOPs on request. This would ensure the system studies were based on accurate data. Second, the informal development group considered whether entities could ensure power factor is maintained by arranging for VARs when MWs are purchased. However, the recently issued NOPR recommends retiring the requirement that currently requires VARs to be acquired due to redundancy with OATT. The NOPR also recommends withdrawing P 1863 as a directive because the Commission clarified the paragraph to be general guidance, not a FERC directive to modify the standard.[12]

In addition, the informal development group did not further amend the pro forma standard to add obligations to maintain power factors, because the FAC-001 standard requires Transmission Owners (TOs) to set interconnection requirements including "Voltage, Reactive Power, and **power factor control**."[13] Interconnection agreements also define minimum power factor requirements as a contractual obligation.[14] In an effort to keep the VAR standard consistent with interconnection requirements established by contract, and consistent with the pro forma Generator Interconnection agreements pursuant to FERC Order No. 2003 which requires a 0.95 leading to 0.95 lagging power factor,[15] the informal group did not add any additional requirements at this time to address power factor.

Directive from P 1862 of Order No. 693

"We direct the ERO to include APPA's concern in the Reliability Standards development process. We note that transmission operators currently have access to data through their energy management systems to determine a range of

[10] NOPR at P 83.

[11] Order No. 693 at P 1863 (stating "[t]he Commission expects that the appropriate power factor range developed for the interface between the bulk electric system and the LSE from VAR-001-1 would be used as an input to the transmission and operations planning Reliability Standards").

[12] *See* NOPR at Attachment A.

[13] *See* FAC-001-0, R 2.1.9. (available at: http://www.nerc.com/files/FAC-001-0.pdf) (emphasis added).

[14] *See, e.g., Standardization of Generator Interconnection Agreements and Procedures, Order No. 2003, FERC Stats. & Regs. ¶ 31,146 (2003), order on reh'g, Order No. 2003- A, FERC Stats. & Regs. ¶ 31,160, order on reh'g, Order No. 2003-B, FERC Stats. &Regs. ¶ 31,171 (2004), order on reh'g, Order No. 2003-C, FERC Stats. & Regs. ¶ 31,190 (2005), aff'd sub nom. Nat'l Ass'n of Regulatory Util. Comm'rs v. FERC, 475 F.3d 1277 (D.C. Cir. 2007), cert. denied, 552 U.S. 1230 (2008) (*establishing Large Generator Interconnection Agreement requirement).

[15] Order No. 2003 at P 542 (finding "[w]e adopt the power factor requirement of 0.95 leading to 0.95 lagging because it is a common practice in some NERC regions. If a Transmission Provider wants to adopt a different power factor requirement, Final Rule LGIA Article 9.6.1 permits it to do so as long as the power factor requirement applies to all generators on a comparable basis").

power factors at which load operates during various conditions, and **we suggest that the ERO use this type of data as a starting point for developing this modification."**

VAR Informal Consideration
APPA stated, "It may be difficult to reach an agreement on acceptable ranges of net power factors at the interfaces where LSEs receive service from the Bulk-Power System because the acceptable range of power factors at any particular point on the electrical system varies based on many location-specific factors. APPA further states that system power factors will be affected by the transmission infrastructure used to supply the load."[16] APPA's concerns were discussed, and the informal development group did not want to establish a particular range on power factor, especially since power factor requirements are detailed in interconnection agreements as discussed with the P 1861 directive.

Directive from P 1868 of Order No. 693

"In the NOPR, the Commission expressed concern that the technical requirements containing terms such as "established limits" or "sufficient reactive resources" are not definitive enough to address voltage instability and ensure reliable operations. To address this concern, the NOPR proposed directing the ERO to modify VAR-001-1 to include more detailed and definitive requirements on "established limits" and "sufficient reactive resources" and identify acceptable margins (i.e. voltage and/or reactive power margins) above voltage instability points to prevent voltage instability and to ensure reliable operations. **We will keep this direction, and direct the ERO to include this modification in this Reliability Standard**."

Directive from P 1869 of Order No. 693

We recognize that our proposed modification does not identify what definitive requirements the Reliability Standard should use for "established limits" and "sufficient reactive resources." **Rather, the ERO should develop appropriate requirements that address the Commission's concerns through the ERO Reliability Standards development process.** The Commission believes that the concerns of Dynegy, EEI and MISO are best addressed by the ERO in the Reliability Standards development process.

VAR Informal Consideration for PP 1868 and 1869.
In an effort to address this directive and in order to preserve the TOs' flexibility to monitor their systems accordingly, the informal development group added requirements in the pro forma standard VAR-001 Requirement R1 that require steady-state and voltage limits to be included in the criteria used to assess transmission systems:

> R1. Each Transmission Operator shall have documented policies or procedures that are implemented to establish, monitor, and control voltage levels and Reactive Power flows (Mvar flows) within limits as defined below:
>
> > R. 1.1. These documented policies or procedures shall include criteria used in system assessments. The criteria for the assessments shall include established steady-state and voltage stability limits with associated tolerance bands and operating margins.

Also, a new Requirement R2 was updated to include existing language on reactive resources that a TOP can schedule in both the real-time and day-ahead time frame. That list of sufficient reactive resources includes reactive generation scheduling, transmission line and reactive resource switching, and controllable load.

Directive from P 1875 of Order No. 693

In response to the concerns of APPA, SDG&E and EEI on the availability of tools, the Commission recognizes that transient voltage stability analysis is often conducted as an offline study, and that steady-state voltage stability analysis can be done online. The Commission clarifies that it does not wish to require anyone to use tools that are not validated for real-time operations. Taking these comments into consideration, the Commission clarifies its proposed modification from the NOPR. For the Final Rule, **we direct the ERO, through its Reliability Standards development process, to modify Reliability Standard VAR-001-1 to include Requirements to perform voltage stability analysis periodically, using online techniques where commercially-available, and offline simulation tools where online tools are not available, to assist real-time**

[16] Order No. 693 at P 1860.

operations. The ERO should consider the available technologies and software as it develops this modification to VAR-001-1 and identify a process to assure that the Reliability Standard is not limiting the application of validated software or other tools.

VAR Informal Consideration
The informal group determined that the Commission is not requiring TOPs to purchase new online models or to implement tools that will not adequately study a TOP's reactive power requirements. Instead, the group allowed the TOPs to create their own documented procedures for performing assessments in pro forma standard Requirement R1.

Further, TOPs may under the new pro forma standard align their voltage planning with the pending TPL standards currently being reviewed by the Commission. The TPL standards require voltage studies, as outlined below:

> **R5.** Each Transmission Planner and Planning Coordinator shall have criteria for acceptable System steady-state voltage limits, post-Contingency voltage deviations, and the transient voltage response for its System. For transient voltage response, the criteria shall at a minimum specify a low voltage level and a maximum length of time that transient voltages may remain below that level. [17]

Directive from P 1879 of Order No. 693

The Commission noted in the NOPR that in many cases, load response and demand-side investment can reduce the need for reactive power capability in the system. Based on this assertion, the Commission proposed to direct the ERO to include controllable load among the reactive resources to satisfy reactive requirements for incorporation into Reliability Standard VAR-001-1. **While we affirm this requirement, we expect the ERO to consider the comments of SoCal Edison with regard to reliability and SMA in its process for developing the technical capability requirements for using controllable load as a reactive resource in the applicable Reliability Standards.**

VAR Informal Consideration
NERC addressed this directive in a prior version of the VAR standard,[18] but as mentioned above, the list for sufficient reactive resources that includes controllable load has been retained in R2.

Directive from P 1885 of Order No. 693

"Dynegy has suggested an improvement to Reliability Standard VAR-002-1, and NERC should consider this in its Reliability Standards development process."

Dynegy requested that VAR-002 be modified to include "more detailed and definitive requirements when defining the time frame associated with an 'incident'of non compliance."[19]

VAR Informal Consideration
The informal development team addressed this directive in two separate requirements. The noncompliance incidences at issue occur 1) when a generator deviates from a voltage or reactive power schedule; and 2) when a generator is not operating a unit in automatic voltage control mode; more specifically, automatic voltage regulator (AVR) should be in service and controlling voltage.

The new pro forma VAR-002 R2.1 addresses when a unit must notify its TOP when a unit is out of schedule:

> R.2.1. If a GOP drifts out of schedule, each Generator Operator shall notify its associated Transmission Operator within 15 minutes when both of the following conditions are met: 1) the GOP is operating outside of the prescribed voltage or

[17] *See*TPL-001-2, R5 (available at http://www.nerc.com/files/TPL-001-2.pdf).
[18] *See NERC Petition for Approval of Proposed Modifications to Reliability Standards BAL-002-1; EOP-002-3; FAC-002-1; MOD-021-2; PRC-004-2; and VAR-001-2,* 134 FERC ¶ 61,015 (2011).
[19] Order No. 693 at P 1883.

> Reactive Power schedule tolerance band[20] for 15 minutes; and 2) the GOP is no longer able to return to its voltage or Reactive Power schedule.

The new pro forma VAR-002 R3 addresses when a unit must contact its TOP when the facility is out of AVR:

> R3. Each Generator Operator shall notify its associated Transmission Operator of a status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability within 30 minutes of the change. If the status has been restored within the first 15 minutes of such change, then there is no need to call TOP.

The informal development group established the 15-minute time requirements following much discussion. Several industry stakeholders advocated for a larger window of time before a notification must be made; however, there is no consensus on when a reliability gap would be created by expanding the time requirements. Some stakeholders also argued that 15 minutes was excessive.

[20] GOPs monitor and control voltage based on their equipment limitations. GOPs will monitor their voltage or Reactive Power schedule tolerance bands either at the high-side or low-side/terminal voltage.

Conclusion

The goal of the VAR informal development project is to provide a venue for addressing many of the issues that can arise during the formal development process. By engaging with industry stakeholders through an active dialogue, the informal development group was able to efficiently address the concerns of many entities through conference calls, webinars, and informal group meetings. The informal group collaborated over the past five months to develop robust pro forma VAR standards that will serve as the basis for a new VAR standard, which should be posted for industry comment in August 2013. This white paper serves to memorialize some of the discussions surrounding contentious VAR issues, and it provides a basis for the technical discussion that occurred during the informal process. For the aforementioned discussion, the informal development group recommends approval of the accompanying SAR and the posting of the pro forma standards in order to continue the progress on the VAR standards.

Entity Participants

Appendix B: Entity Participants

The below entities represent a non-exhaustive list of entities that had personnel that participated in the VAR informal development effort in some manner, which may include one of the following: direct participation on the ad-hoc group, inclusion on the wider distribution (the "plus" list), attendance at workshops or other technical discussions, participation in a webinar or teleconference, or by providing feedback to the group through a variety of methods (e.g., email, phone calls, etc.). Additionally, though not listed here, announcements were distributed to wider NERC distribution lists to provide the opportunity for entities that were not actively participating to join the effort.

Table 2: Entity Participation in VAR Informal Development

AES	DTE Energy	ISO-NE	Pepco Holdings	TECO Energy
Alcoa	Duke	ITC Transmission	PGE	Tenaska
Ameren	Dynegy	KCP&L	PGN	Texas MPA
Arizona Public Service	Edison Mission Generation	Luminant	PJM	Tri-State G&T
ATC	EDPR	MEAG	PNM	TVA
Austin Energy	Enervision	MidAmerican Energy	PPL	WAPA
BGE	Entegra power	Midwest ISO	PSC	WE Energies
Black Hills Corporation	Entergy	MN Power	PSE	WFEC
Bonneville Power Admin.	Entergy Fossil & Hydro	National Grid	PSEG	WICF
BP	epelectric	NCEMC	Rayburn Electric	Wisconsin Public Service
Calpine	ERCOT	NERC	San Francisco PU	Xcel Energy
CenterPoint Energy	Essential Power LLC	NextEra	SCANA	**Regional Entities:**
City of Tallahassee	Exelon Corp	NiSource	SCE	FRCC
Colorado Springs Utilities	ExxonMobil	Northeast Utilities	Seminole electric	MRO
ComEd	FERC	Nova Scotia Power	Siemens	NPCC
ConEd	FPL	NPPD	SMUD	RFC
Constellation	Garland Power & Light	NYISO	Snohomish County PUD	SERC
Constellation Energy Nuclear Group (CENG)	Hydro Quebec	Occidental Energy Ventures Corp.	Southern Company Services	SPP
CSU	Iberdrola Renewables	OGE	Southwest Generation	TRE
Dominion	IMPA	PacifiCorp	Southwest Power Pool	WECC

Table 3: Other Outreach	
NERC Standards and Compliance Workshop	ISO/RTO Council
NAGF	NERC News
NERC Standards Committee	EPRI

VAR Mapping Document

Transition of VAR-001-3 and VAR-002-2b (the *pro forma* standard)

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R1	Requirement R1	The *pro forma* creates adds additional sub-requirements that requires the policies and procedures to include criteria for system assessments. The assessments must now include steady-state limits, voltage stability limits and associated operating margins, and voltage schedules along with associated tolerance bands. The sub-requirements also now mandate that information is shared with neighboring TOPs and the applicable RC.
VAR-001-3 R2	Requirement R2	The new requirement has been updated to incorporate real-time and day-ahead scheduling of resources. It eliminates the need for the existing R7, R8, and R9.
VAR-001-3 R3	Requirement R3	The new requirement has been simplified by removing the need to maintain an exemption list. Instead, the standard focuses on whether the exemption criteria are known and whether a granted exemption was communicated to the applicable Generator.

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R4	Requirement R4	The new requirements have been updated to allow the TOP to provide the voltage or Reactive Power schedule at either the high side or the low side of the GSU. Also as tolerance band is now required under the new requirement.
VAR-001-3 R5	Deleted	Pending a final rulemaking on P81, this requirement has been deleted.
VAR-001-3 R6	Requirement R5	The sub-requirement R6.1 was deleted because it is duplicative of VAR-002's requirement R1 and R2.
VAR-001-3 R7	Deleted	See comments for new R2.
VAR-001-3 R8	Deleted	See comments for new R2.
VAR-001-3 R9	Deleted	See comments for new R2.
VAR-001-3 R10	Deleted	This is duplicative of TOP-001-2 and the Tv definition.
VAR-001-3 R11	Requirement R6	The only change is the numbering due to other deletions.
VAR-001-3 R12	Deleted	This requirement was deleted because the EOP standards address taking any corrective action including load-shedding. Also the new TOP-002-3 R2 and TOP-001-2 R11 address the TOP taking corrective actions.

Standard: VAR-002-3 – Capacity Benefit Margin		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b R1	Requirement R1	The requirement has not been modified.

Standard: VAR-002-3 – Capacity Benefit Margin		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b R2	Requirement R2	The new *pro forma* requirement has been updated by including a new sub-requirement to allowing GOPs to only call in certain instances when deviating from voltage schedules .
VAR-002-2b R2	Requirement R3	The new *pro forma* requirement has been updated by including a new sub-requirement to allowing GOPs to investigate why the status has changed on AVR equipment before having to notify the TOP.
VAR-002-2b R2	Requirement R4	The requirement has not been modified.
VAR-002-2b R2	Requirement R5	The requirement has not been modified.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Operations

Draft Reliability Standard Compliance Guidance for VAR-001 and VAR-002

July 8, 2013

Introduction

The NERC Compliance department (Compliance) worked with the Informal VAR Group (IVG) in a review of pro forma VAR-001 and VAR-002 standards. The purpose of the review is to discuss the requirements of the pro forma standards to obtain an understanding of its intended purpose and necessary evidence to support compliance. The purpose of this document is to address specific questions posed by the IVG in order to aid in the wording of the requirements and provide a level of understanding regarding evidentiary support necessary to demonstrate compliance. In addition, a conclusion related to whether the pro forma standards provide reasonable guidance for compliance auditors is provided. However, this document makes no assessment as to the enforceability of the standard.

While all testing requires levels of auditor judgment, participating in these reviews allows Compliance to develop training and approaches to support a high level of consistency in audits conducted by the Regional Entities. The following questions will be used to aid in such auditor training.

IVG VAR-001 and VAR-002 Questions

Question 1

To show that VAR-001 policies or procedures are "implemented," would Compliance ask for a TOP to provide data around an "event?" Otherwise, would Compliance request TOPs to prove compliance over the entire audit period? What is the best way to provide sample data to support that VAR-001 requirements are being met?

Compliance Response to Question 1 (Compliance response in context of VAR-001 R1)

Part 1 – Compliance can use a range of approaches to understand and verify implementation. With regard to this standard, those approaches may include observing, interviewing, reviewing an entity's response to instances of voltage deviation that require operator intervention, as well as reviewing documentation for notifications of voltage deviations that may include exemption requests. Registered entities may also demonstrate the implementation of policies or procedures by providing documentation in connection with an event. Also, auditors may be independently aware of events occurring within the TOP's area, and the use of such events to determine the nature of an entity's response is evidence of implementation of policies and procedures. Alternatively, a lack of response to a known event could be evidence of noncompliance with implementation of policies and procedures.

Part 2 – Yes, the Rules of Procedure provide that a registered entity is required to be compliant with Reliability Standards during the audit period. A compliance audit should be appropriately scoped and testing designed to obtain a reasonable assurance of compliance. In this regard, though possible, it is unlikely an auditor would require levels of proof of compliance for an entire audit period and would use approaches such as those noted in Part 1 to gain reasonable assurance of compliance.

Part 3 – As noted in the answer to Part 1, there are a range of approaches to help an auditor determine compliance and those range of approaches should be used to help the registered entity demonstrate compliance. As noted above, those approaches may include observing, interviewing, providing documentation relative to an event, as well as documents generated during normal operations such as notifications of voltage deviations.

Question 2
For VAR-001 R2, would Compliance focus more on real-time directives? For the day-ahead time frame, is it enough to show studies that were used to schedule resources?

Compliance Response to Question 2
Part 1 – Compliance cannot commit to the level of testing that would or would not be performed on a requirement by requirement basis or favoring the testing of one sub-requirement over another. These determinations would be made in connection with the scoping of an audit for a specific registered entity.

Part 2 – No. The entity would be expected to provide the documentation for the day ahead scheduling in addition to documentation supporting that it was scheduled, as noted in the requirement.
The auditor would first gain an understanding of the entity's process for conducting the studies and the frequency the studies are performed. Based on the entities response, the auditor most likely would select a sample of studies to verify and ascertain whether the resulting actions, or non actions, were supported by such studies. Documented evidence existing at the time of the study selected by the auditor for verification would be considered stronger evidence than verbal explanations given by entities in response to inquiries during an audit.

Question 3
For VAR-001 R3, is the standard clear enough to allow for temporary exemptions?

Compliance Response to Question 3
Yes. The TOP would need to provide the criteria and evidence supporting the delivery of the exemption notification.

Question 4
With regard to VAR-002, will generators receive a violation for instances where a system event is affecting system voltage, but the generators made the appropriate conversions and set the AVRs to meet the original schedule provided by the TOP?

Compliance Response to Question 4 (Compliance response in context of VAR-002 R2)
No, the generator operators can only be responsible for maintaining the schedule provided by the TOP; if the TOP provides a new directive or schedule, the GOP is required to follow the new directive.

Question 5
Related to VAR-002, generators monitor voltage on both the low side and high side of the GSU and the "number" being monitored by the Generator will not always equate to the number provided by the TOP. Does this need to be spelled out in the requirement?

Compliance Response to Question 5 (Compliance response in context of VAR-002 R2)
The Generator should be able to provide documentation that identifies the "number" being monitored and the calculation demonstrating how the "number" equates to the schedule provided by the TOP.

Question 6
For VAR-002 R2, the Generator demonstrates compliance by executing the three sub-tasks. Is it clear that those are the only items that a Generator will need to do to maintain voltage? There are events when a unit will be dragged out of voltage schedule, and a unit is limited by its operating capacity to prevent such instances. Those instances should not be a violation under VAR-002 R2, if the GOP is doing everything possible to bring the unit back into a voltage schedule (i.e., the three sub-requirements).

Compliance Response to Question 6
The main requirement is clearly stated, that except for an exemption, each of the three sub-requirements must be performed. In this regard, the Generator must document their performance to provide evidence to the auditor of compliance. We have provided additional notes for R2.1-.3 below:

R2.1: Based on the language modification, the Generator may operate up to 30 minutes prior to notifying the TOP that the Generator cannot return to its schedule. The sub-requirement would not require the documentation for instances where a Generator returned to their schedule in 30 minutes or less. Instances greater than 30 minutes would require documentation supporting the Generator contacting the TOP, documentation showing when the Generator first began operating outside of the schedule and when the determination was made the GOP was no longer able to return to its schedule.

R2.2: Based on conversations with the IVG, the only alternative is to manually control the reactive output. In this regard, it is suggested that, unless another method exists, the language be changed to "shall use a manual method."

R2.3 The sub-requirement is self explanatory and would require the Generator to provide documentation supporting compliance or the written explanation.

Question 7

For VAR-002 requirement R3, the requirement allows for a 15 minute grace-period to reporting a status change, if the issue with reactive resource is corrected. Is that point clear? This requirement is concerned with allowing a Generator to resolve an issue with a resource without having to call or notify the TOP every time the status of the resources goes in and out of service. Also, the IVG would like for telemetered points to count as an automatic notification to the TOP. Is such notification acceptable to Compliance?

Compliance Response to Question 7

Part 1 – The Requirement is clear, notification is only required between minutes 16 and 30, regardless of restoration.

Part 2 – If telemetered points meet the requirement of a notification, the requirement will need to explain the supporting documentation that substantiates compliance (what evidence can be provided to an auditor.)

Conclusion

In general, Compliance finds the pro forma standards provide a reasonable level of guidance for Compliance Auditors to conduct audits in a consistent manner. The standard establishes timelines, data requirements, and ownership of specific actions. In general, the standard would provide reasonable guidance to develop training for Compliance Auditors to execute their reviews. Compliance does recommend the IVG address the issues noted in the previous section of this document related to the standards.

Following final approval of the Reliability Standard, Compliance will develop the final Reliability Standards Auditor Worksheet (RSAW) and associated training.

Proposed Timeline for the VAR Standard Drafting Team (SDT)		
Anticipated Date	**Location**	**Event**
July 2013	-	SC Authorizes SAR and pro forma Standards for Posting
July 2013		Conduct Nominations for VAR Project
July 2013	-	Post SAR and pro forma Standards for 45-Day Initial Comment Period
August 2013	-	Conduct Ballot
September 2013	-	45-Day Comment Period and Ballot Closes
September 2013	TBD	VAR Standard Drafting Team Face to Face Meeting to Respond to Respond to Initial Comments and Revise as Necessary
September 2013	-	Conduct Final Ballot
November 7, 2013	-	NERC Board of Trustees Adoption
December 31, 2013	-	NERC Files Petition with the Applicable Governmental Authorities

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-001-4 & VAR-002-3

Ballot and Non-Binding Poll now open through September 3, 2013

Now Available

A ballot for **VAR-001-4 and VAR-002-3** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels is open through **8 p.m. Eastern on Tuesday, September 3, 2013.**

Background information for this project can be found on the project page.

Instructions

Members of the ballot pool associated with this project may log in and submit their vote for the standard by clicking here.

As a reminder, this ballot is being conducted under the revised Standard Processes Manual, which requires all negative votes to have an associated comment submitted (or an indication of support of another entity's comments). Please see NERC's announcement regarding the balloting software updates and the guidance document, which explains how to cast your ballot and note if you've made a comment in the online comment form or support another entity's comment.

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the standard(s). If the comments do not show the need for significant revisions, the standard(s) will proceed to a final ballot.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, at wendy.muller@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-001-4 & VAR-002-3

Comment Period: July 19, 2013 – September 3, 2013
Ballot Pools Forming Now: July 19, 2013 – August 19, 2013

Upcoming:
Ballot and Non-Binding Poll: August 23, 2013 – September 3, 2013

Now Available

A 45-day formal comment period for **VAR-001-4 and VAR-002-3** is open through **8 p.m. Eastern on Tuesday, September 3, 2013.** The standard authorization request (SAR) for this project is also posted for comment. Additional supporting documents are posted for information. A ballot pool is being formed and the ballot pool window is open through 8 a.m. Eastern on **Monday, August 19, 2013** *(please note that ballot pools close at 8 a.m. Eastern and mark your calendar accordingly).*

This project began with an informal development process to address outstanding FERC directives from Order 693 and compliance issues. The modifications to VAR-001 and VAR-002 were drafted in tandem, and several requirements in one standard reference the other standard. Accordingly, the standards are being balloted together. Further, in an effort to support Paragraph 81 and the results-based standard concepts, informal development is proposing six requirements for retirement. The goal is to present the standards to the NERC Board of Trustees in November 2013.

Background information, including other supporting documents for this project, can be found on the project page. Please contact either Soo Jin Kim, the standards developer or a participant on the informal development group if you would like additional information.

Instructions for Joining Ballot Pool(s)

Ballot pools are being formed for the standards mentioned and the associated non-binding polls in this project. Registered Ballot Body members must join the ballot pools to be eligible to vote in the balloting and submit an opinion for the non-binding polls of the associated VRFs and VSLs. Registered Ballot Body members may join the ballot pools at the following page: Join Ballot Pools

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list servers for this project are:

Ballot for VAR-001-4 & VAR-002-3: bp-2013-04_VAR_1_in@nerc.com
Non-Binding Poll for VAR-001-4 & VAR-002-3: bp-2013-04_VAR_NB_1_in@nerc.com

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Tuesday, September 3, 2013**. Please use the electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment forms are posted on the project page.

Next Steps

A ballot for the standards and non-binding poll of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) will be conducted as previously outlined.

Standards Development Process

The Standards Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, at wendy.muller@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Standard Drafting Team Nominations

Project 2010-03 Modeling Data: MOD-032-1, MOD-033-1
Project 2010-04 Demand Data: MOD-031-1
Project 2013-04 Voltage and Reactive Control: VAR-001-3, VAR-002-4
Project 2010-01 Training: PER-005-2

Nomination Period Open: July 24, 2013 – August 2, 2013

Link to Official Nomination Form
Link to Word Version of Nomination Form

Background
These projects have recently transitioned from informal development to formal development. Ad hoc groups developed Standard Authorization Requests, pro-forma Reliability Standards, a technical white paper and supporting documents through the stakeholder consensus building informal development process which are currently posted for comment with upcoming ballots. The NERC Standards Committee is seeking industry experts to serve on standard drafting teams for formal development.

Each standard drafting team (SDT) is proposed to consist of a maximum of 10 members. SDT members are expected to attend all (or at least the vast majority) of the face-to-face SDT meetings (projected to be 3 days a month) as well as participate in all the SDT meetings held via conference calls (projected to be 2 to 5 days a month) for the remainder of 2013. Nominees are asked to be mindful of the time commitment this project will require, and volunteer only if their schedule will allow them to actively participate.

Background information about each project including the projected schedule is available on the project pages. The stakeholders who comprised the ad hoc group participants can be found at the links below:

- Project 2010-03 Modeling Data
- Project 2010-04 Demand Data
- Project 2013-04 Voltage and Reactive Control
- Project 2010-01 Training

Notice to all ad hoc group participants: if you are interested in continuing on the SDT you must nominate yourself to be considered for possible inclusion on the team.

For all projects below, the following are beneficial, but not required: team members with experience in compliance, legal, regulatory, facilitation, technical writing, previous drafting team experience, or experience with developing standards inside or outside (e.g., IEEE, NAESB, ANSI, etc.) of the NERC process. Any person interested in being chair of a SDT must be willing to undergo one half day of facilitation training prior to the first team meeting.

Further, nominees should have technical expertise in the subject matter of the standard drafting team on which they wish to serve, as identified below:

- Project 2010-03 Modeling Data: MOD-032-1, MOD-033-1 – Nominees should have experience in one or more of the following areas: transmission planning, steady-state and dynamics modeling, and system model validation. The project is also seeking perspectives from each Interconnection and from various organizations whose functions are contemplated to be subject to the Reliability Standards.
- Project 2010-04 Demand Data: MOD-031-1 – Nominees should have experience in one or more of the following areas: transmission operations, transmission planning, operations planning, and resource planning.
- Project 2013-04 Voltage and Reactive Control: VAR-001-4, VAR-002-3 – Nominees should have experience in one or more of the following areas: transmission operations, transmission planning, reliability coordination, and generator operation.
- Project 2010-01 Training: PER-005-2 – Nominees should have experience in training or transmission and generation operations.

Instructions for Submitting a Nomination to Participate on a Standard Drafting Team

If you are interested in serving on a SDT, please complete this nomination form by **August 2, 2013**. One nomination form must be submitted for each SDT an individual wishes to volunteer for, describing the individual's experience or qualifications related to that project.

An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies page.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our gratitude to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, at wendy.muller@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Nomination Form

Standard Drafting Team Members

Project 2010-03 Modeling Data: MOD-032-1, MOD-033-1
Project 2010-04 Demand Data: MOD-031-1
Project 2013-04 Voltage and Reactive Control: VAR-001-3, VAR-002-4
Project 2010-01 Training: PER-005-2

If you are interested in serving on a standard drafting team for one of the projects above, please complete this nomination form by **August 2, 2013**. One nomination form should be submitted for each standard drafting team an individual wishes to volunteer for, describing the individual's experience or qualifications related to that project. If you have any questions, please contact Valerie Agnew at valerie.agnew@nerc.net.

By submitting the following information, you are indicating your willingness and agreement to actively participate in the Standard Drafting Team (SDT) meetings if appointed to the SDT by the Standards Committee. This means that if you are appointed to the SDT, you are expected to attend all (or at least the vast majority) of the face-to-face SDT meetings (projected to be 3 days a month) within the projected schedule as well as participate in all the SDT meetings held via conference calls (projected to be 3-5 days a month) for the durations of 2013. Nominees are asked to be mindful of the time commitment this project will require, and volunteer only if their schedule will allow them to actively participate. The projected schedules can be found on the project pages below.

- Project 2010-03 Modeling Data
- Project 2010-04 Demand Data
- Project 2013-04 Voltage and Reactive Control
- Project 2010-01 Training

Thank you for volunteering! All nominees will be contacted with the disposition of their nomination after the Standards Committee appoints a team for the project for which you have volunteered.

Name:	
Select the Project for which the nominee is volunteering:	☐ Project 2010-03 Modeling Data: MOD-032-1, MOD-033-1 ☐ Project 2010-04 Demand Data: MOD-031-1 ☐ Project 2013-04 Voltage and Reactive Control: VAR-001-3, VAR-002-4

	☐ Project 2010-01 Training: PER-005-2
Organization:	
Address:	
Telephone:	
E-mail:	

Please briefly describe your experience and qualifications to serve on the selected Standard Drafting Team:

If you are currently a member of any NERC drafting team, please list each team here:

☐ Not currently on any active SAR drafting team, standard drafting team, standard review team, or informal ad hoc group.

☐ Currently a member of the following SAR, standard drafting team(s), standard review team(s), or informal ad hoc group:

If you previously worked on any NERC drafting team please identify the team(s):

☐ No prior NERC SAR or standard drafting team experience.

☐ Prior experience on the following team(s):

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:

☐ ERCOT	☐ NPCC	☐ SPP
☐ FRCC	☐ RFC	☐ WECC
☐ MRO	☐ SERC	☐ NA – Not Applicable

Select each Function[1] in which you have current or prior expertise:	
☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:		Telephone:	
Organization:		E-mail:	
Name:		Telephone:	
Organization:		E-mail:	

Provide the name of your immediate supervisor if not provided above:			
Name:		Telephone:	
Organization:		E-mail:	

[1] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-001-4 & VAR-002-3

Ballot and Non-Binding Poll Results

Now Available

A ballot for **VAR-001-4 and VAR-002-3** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels concluded at **8 p.m. Eastern on Tuesday, September 3, 2013.**

Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results for the ballot.

Approval	Non-binding Poll Results
Quorum: 81.89%	Quorum: 79.95%
Approval: 43.79%	Supportive Opinions: 44.23%

Background information for this project can be found on the project page.

Next Steps

The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the standard. The standard will then proceed to an additional comment period and ballot.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, at wendy.muller@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results	
Ballot Name:	Project 2013-04 Voltage and Reactive Control VAR-001-4 and VAR-002-3 ballot 1
Ballot Period:	8/23/2013 - 9/4/2013
Ballot Type:	Initial
Total # Votes:	330
Total Ballot Pool:	403
Quorum:	**81.89 % The Quorum has been reached**
Weighted Segment Vote:	43.79 %
Ballot Results:	**The drafting team will review comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	107	1	35	0.449	43	0.551	0	10	19
2 - Segment 2	9	0.9	2	0.2	7	0.7	0	0	0
3 - Segment 3	90	1	33	0.493	34	0.507	0	6	17
4 - Segment 4	30	1	18	0.75	6	0.25	0	1	5
5 - Segment 5	99	1	27	0.38	44	0.62	0	5	23
6 - Segment 6	53	1	16	0.381	26	0.619	1	3	7
7 - Segment 7	0	0	0	0	0	0	0	0	0
8 - Segment 8	4	0.3	1	0.1	2	0.2	0	0	1
9 - Segment 9	3	0.3	1	0.1	2	0.2	0	0	0
10 - Segment 10	8	0.7	3	0.3	4	0.4	0	0	1
Totals	**403**	**7.2**	**136**	**3.153**	**168**	**4.047**	**1**	**25**	**73**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	COMMENT RECEIVED
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	COMMENT RECEIVED

1	Arizona Public Service Co.	Robert Smith	Negative	COMMENT RECEIVED
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Abstain	
1	Avista Utilities	Heather Rosentrater		
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Negative	COMMENT RECEIVED
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot		
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	COMMENT RECEIVED
1	Cleco Power LLC	Danny McDaniel	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
1	Colorado Springs Utilities	Paul Morland	Negative	SUPPORTS THIRD PARTY COMMENTS - (Group comments submitted by CAL ISO and Xcel Energy)
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC group comments)
1	CPS Energy	Richard Castrejana	Abstain	
1	Dairyland Power Coop.	Robert W. Roddy		
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
1	Duke Energy Carolina	Douglas E. Hils	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
1	El Paso Electric Company	Pablo Onate	Abstain	
1	Entergy Transmission	Oliver A Burke	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC Generation Subcommittee Review Group)
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF and ACES)
1	Hydro One Networks, Inc.	Ajay Garg		
				SUPPORTS

1	Hydro-Quebec TransEnergie	Martin Boisvert	Negative	THIRD PARTY COMMENTS (NPCC)
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted Hobson	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Jennifer Flandermeyer		
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Negative	COMMENT RECEIVED
1	Long Island Power Authority	Robert Ganley		
1	Los Angeles Department of Water & Power	John Burnett	Abstain	
1	Lower Colorado River Authority	Martyn Turner	Abstain	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Negative	COMMENT RECEIVED
1	MEAG Power	Danny Dees	Abstain	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (NERC Standards Review Forum)
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (National Grid's supports comments provided by NPCC Reliability Standards Committee (RSC).)
1	Nebraska Public Power District	Cole C Brodine	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO-NSRF)
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Bruce Metruck	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (NIPSCO)
1	NorthWestern Energy	John Canavan	Negative	COMMENT RECEIVED
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	COMMENT RECEIVED
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards

				Review Group)
1	Omaha Public Power District	Doug Peterchuck	Abstain	
1	Oncor Electric Delivery	Jen Fiegel	Abstain	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	SUPPORTS THIRD PARTY COMMENTS - (Northeast Power Coordinating Council group comments)
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	PacifiCorp	Ryan Millard	Abstain	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments submitted under the title 'PPL NERC Registered Affiliates')
1	Public Service Company of New Mexico	Laurie Williams	Negative	COMMENT RECEIVED
1	Public Service Electric and Gas Co.	Kenneth D. Brown		
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer		
1	SaskPower	Wayne Guttormson		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	COMMENT RECEIVED
1	South Carolina Public Service Authority	Shawn T Abrams	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC Generation Subcommittee Comments)
1	Southern California Edison Company	Steven Mavis	Negative	COMMENT RECEIVED
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC OC Review Group)
1	Texas Municipal Power Agency	Brent J Hebert	Affirmative	
1	Trans Bay Cable LLC	Steven Powell		
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED

1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
1	Western Area Power Administration	Lloyd A Linke	Negative	COMMENT RECEIVED
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Negative	SUPPORTS THIRD PARTY COMMENTS - (IRC/Standards Review Committee)
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Negative	SUPPORTS THIRD PARTY COMMENTS - (SRC)
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	COMMENT RECEIVED
2	ISO New England, Inc.	Kathleen Goodman	Negative	SUPPORTS THIRD PARTY COMMENTS - (IRC SRC)
2	Midwest ISO, Inc.	Marie Knox	Negative	SUPPORTS THIRD PARTY COMMENTS - (ISO/RTO SRC)
2	New York Independent System Operator	Gregory Campoli	Negative	SUPPORTS THIRD PARTY COMMENTS - (IRC/SRC - NPCC)
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Negative	COMMENT RECEIVED
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Services	Mark Peters	Negative	SUPPORTS THIRD PARTY COMMENTS - (Ameren)
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blue Ridge Electric	James L Layton		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	COMMENT RECEIVED
3	City of Bartow, Florida	Matt Culverhouse		
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson		
3	City of Garland	Ronnie C Hoeinghaus	Negative	COMMENT RECEIVED
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
				SUPPORTS THIRD PARTY COMMENTS -

3	Colorado Springs Utilities	Charles Morgan	Negative	(Group comments by CAL ISO and Xcel Energy)
3	ComEd	John Bee	Negative	COMMENT RECEIVED
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	SUPPORTS THIRD PARTY COMMENTS - (supporting NPCC group comments)
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	CPS Energy	Jose Escamilla	Abstain	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
3	Entergy	Joel T Plessinger	Abstain	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C Esquerre		
3	Florida Power Corporation	Lee Schuster	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
3	Georgia Power Company	Danny Lindsey	Negative	COMMENT RECEIVED
3	Georgia System Operations Corporation	Scott McGough	Abstain	
3	Great River Energy	Brian Glover	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF & ACES)
3	Gulf Power Company	Paul C Caldwell	Negative	COMMENT RECEIVED
3	Hydro One Networks, Inc.	David Kiguel		
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Kansas City Power & Light Co.	Charles Locke	Negative	COMMENT RECEIVED
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Negative	COMMENT RECEIVED
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
3	Manitoba Hydro	Greg C. Parent	Negative	COMMENT RECEIVED
3	MEAG Power	Roger Brand	Abstain	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (I support comments submitted by the MRO NERC Standards Review Forum (NSRF))
3	Mississippi Power	Jeff Franklin	Negative	COMMENT RECEIVED

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	National Grid USA	Brian E Shanahan	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC RegStandards Committee)
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NERC Standards Review Forum (NSRF))
3	New York Power Authority	David R Rivera		
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (NIPSCO)
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Review Group)
3	Old Dominion Electric Coop.	Bill Watson		
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC group comments)
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Abstain	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz		
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC Generation Subcommittee Comments)
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	COMMENT RECEIVED
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Negative	SUPPORTS THIRD PARTY COMMENTS - (TVA)
3	Tri-County Electric Cooperative, Inc.	Mike Swearingen	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
				SUPPORTS

3	Westar Energy	Bo Jones	Negative	THIRD PARTY COMMENTS - (SPP Standards Group)
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	SUPPORTS THIRD PARTY COMMENTS - (Xcel Energy Comments)
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO)
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell	Negative	COMMENT RECEIVED
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	COMMENT RECEIVED
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas		
4	Georgia System Operations Corporation	Guy Andrews	Abstain	
4	Herb Schrayshuen	Herb Schrayshuen	Negative	COMMENT RECEIVED
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC Regional Standards Committee)
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Ameren, SERC GS Committee)
5	Arizona Public Service Co.	Scott Takinen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cooments submitted by AZPS)
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke	Affirmative	
5	BC Hydro and Power Authority	Clement Ma		
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	

5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Calpine Corporation	Hamid Zakery		
5	City and County of San Francisco	Daniel Mason	Negative	COMMENT RECEIVED
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	COMMENT RECEIVED
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC OC Standards Working Group)
5	Colorado Springs Utilities	Kaleb Brimhall	Negative	SUPPORTS THIRD PARTY COMMENTS - (SRC ISO Comments)
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC group comments)
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Alexander Eizans	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC EC Generation Subcommittee)
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	El Paso Electric Company	Gustavo Estrada	Abstain	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Entergy Services, Inc.	Tracey Stubbs	Negative	SUPPORTS THIRD PARTY COMMENTS - SERC
5	Essential Power, LLC	Patrick Brown	Negative	COMMENT RECEIVED
5	Exelon Nuclear	Mark F Draper	Negative	COMMENT RECEIVED
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF & ACES)
5	Hydro-Québec Production	Roger Dufresne	Negative	COMMENT RECEIVED
5	JEA	John J Babik	Negative	SUPPORTS THIRD PARTY COMMENTS -

				(FMPA)
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lafayette Utilities System	Jamie B Webb		
5	Lakeland Electric	James M Howard		
5	Liberty Electric Power LLC	Daniel Duff	Negative	SUPPORTS THIRD PARTY COMMENTS - (Generator Forum Standards Review Team)
5	Lincoln Electric System	Dennis Florom	Negative	COMMENT RECEIVED
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Karin Schweitzer		
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	S N Fernando	Negative	COMMENT RECEIVED
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Abstain	
5	MidAmerican Energy Co.	Neil D Hammer		
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
5	New York Power Authority	Wayne Sipperly	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
5	NextEra Energy	Allen D Schriver		
5	NiSource	Huston Ferguson	Negative	SUPPORTS THIRD PARTY COMMENTS - (NIPSCO)
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson		
5	Oklahoma Gas and Electric Co.	Leo Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (We support comments previously submitted by SPP Standards Review Group.)
5	Omaha Public Power District	Mahmood Z. Safi	Abstain	
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Negative	SUPPORTS THIRD PARTY COMMENTS - (NAGF Standard's Review Team)
5	PacifiCorp	Bonnie Marino-Blair	Negative	SUPPORTS THIRD PARTY COMMENTS - (Kelly Cumiskey, PacifiCorp)
5	Pattern Gulf Wind LLC	Grit Schmieder-Copeland	Negative	SUPPORTS THIRD PARTY COMMENTS - (NAGF SRT)
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	

5	PowerSouth Energy Cooperative	Tim Hattaway		
5	PPL Generation LLC	Annette M Bannon	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
5	PSEG Fossil LLC	Tim Kucey		
5	Public Utility District No. 1 of Chelan County	John Yale	Negative	SUPPORTS THIRD PARTY COMMENTS - (NAGF SRT)
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	SUPPORTS THIRD PARTY COMMENTS - (NAGF Standard's Review Team)
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Raven Power	Scott A Etnoyer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC Generation Subcommittee Comments)
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Feather Power Project	Kathryn Zancanella	Affirmative	
5	Southern California Edison Company	Denise Yaffe	Negative	COMMENT RECEIVED
5	Southern Company Generation	William D Shultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southern Company)
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tenaska, Inc.	Scott M. Helyer	Negative	COMMENT RECEIVED
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State G & T Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Utility System Effeciencies, Inc. (USE)	Robert L Dintelman		
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Westar Energy	Bryan Taggart	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Comments)
5	Western Farmers Electric Coop.	Clem Cassmeyer		
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Negative	SUPPORTS THIRD PARTY COMMENTS - (Alice Ireland)
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Ameren, SERC GS Committee)
6	APS	Randy A. Young	Negative	COMMENT RECEIVED
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	

6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	COMMENT RECEIVED
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
6	Colorado Springs Utilities	Shannon Fair	Negative	SUPPORTS THIRD PARTY COMMENTS - (CAL ISO)
6	Con Edison Company of New York	David Balban	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC group comments)
6	Constellation Energy Commodities Group	David J Carlson	Negative	COMMENT RECEIVED
6	Dominion Resources, Inc.	Louis S. Slade	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
6	Duke Energy	Greg Cecil		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Municipal Power Pool	Thomas Washburn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF / ACES)
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Negative	COMMENT RECEIVED
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brenda Hampton	Abstain	
6	Manitoba Hydro	Blair Mukanik	Negative	COMMENT RECEIVED
6	MidAmerican Energy Co.	Dennis Kimm		
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley		
6	New York Power Authority	Saul Rojas	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
6	Northern California Power Agency	Steve C Hill	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	SUPPORTS THIRD PARTY COMMENTS - (NIPSCO Comments)
6	NRG Energy, Inc.	Alan Johnson		
6	Oklahoma Gas & Electric Services	Jerry Nottnagel	Negative	NO COMMENT RECEIVED
6	Omaha Public Power District	Douglas Collins	Abstain	
6	PacifiCorp	Kelly Cumiskey	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Elizabeth Davis	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)

6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC Generation Subcommittee comments.)
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	Southern California Edison Company	Lujuanna Medina		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	COMMENT RECEIVED
6	Westar Energy	Grant L Wilkerson	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP's comments)
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS - (Lloyd Linke)
6	Wisconsin Public Service Corp.	David Hathaway	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (Alice Ireland, Xcel Energy)
8		Edward C Stein		
8		Roger C Zaklukiewicz	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	COMMENT RECEIVED
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Negative	COMMENT RECEIVED
10	Florida Reliability Coordinating Council	Linda Campbell		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	COMMENT RECEIVED
10	ReliabilityFirst Corporation	Anthony E Jablonski	Negative	COMMENT RECEIVED
10	SERC Reliability Corporation	Joseph W Spencer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments from the SERC EC Generation Subcommittee submitted by Ben Deutsch on 9/3/13)
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	COMMENT RECEIVED

10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Non-binding Poll

Project 2013-04 VAR

Non-binding Poll Results	
Non-binding Poll Name:	Project 2013-04 VRC VAR-001-4, and VAR-002-3 NB Poll
Poll Period:	8/23/2013 - 9/4/2013
Total # Opinions:	295
Total Ballot Pool:	369
Summary Results:	79.95% of those who registerd to participate provided an opinion or an abstention; 44.23% of those who provided an opinion indicated support for the VRFs and VSLs.

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson	Abstain	
1	Arizona Public Service Co.	Robert Smith	Negative	COMMENT RECEIVED
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Abstain	
1	Avista Utilities	Heather Rosentrater		
1	Balancing Authority of Northern California	Kevin Smith	Abstain	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot		
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	COMMENT RECEIVED
1	Cleco Power LLC	Danny McDaniel	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC group comments)

1	CPS Energy	Richard Castrejana	Abstain	
1	Dairyland Power Coop.	Robert W. Roddy		
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Negative	SUPPORTS THIRD PARTY COMMENTS - (Dominion)
1	Duke Energy Carolina	Douglas E. Hils	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
1	El Paso Electric Company	Pablo Onate	Abstain	
1	Entergy Transmission	Oliver A Burke	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC Generation Subcommittee Review Group)
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF and ACES)
1	Hydro One Networks, Inc.	Ajay Garg		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Negative	SUPPORTS THIRD PARTY COMMENTS (NPCC)
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted Hobson	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Jennifer Flandermeyer		
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Long Island Power Authority	Robert Ganley		
1	Los Angeles Department of Water & Power	John Burnett	Abstain	
1	Lower Colorado River Authority	Martyn Turner	Abstain	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Negative	COMMENT RECEIVED
1	MEAG Power	Danny Dees	Abstain	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD

				PARTY COMMENTS - (NERC Standards Review Forum)
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (National Grid supports comments provided by NPCC Reliability Standards Committee (RSC).)
1	Nebraska Public Power District	Cole C Brodine	Abstain	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Bruce Metruck	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
1	Northern Indiana Public Service Co.	Julaine Dyke	Negative	SUPPORTS THIRD PARTY COMMENTS - (NIPSCO)
1	NorthWestern Energy	John Canavan	Negative	COMMENT RECEIVED
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Review Group)
1	Omaha Public Power District	Doug Peterchuck	Abstain	
1	Oncor Electric Delivery	Jen Fiegel	Abstain	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	SUPPORTS THIRD PARTY COMMENTS - (Northeast Power Coordinating Council group comments)
1	Orlando Utilities Commission	Brad Chase		
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	PacifiCorp	Ryan Millard	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments submitted under the title 'PPL NERC Registered Affiliates')
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown		
1	Public Utility District No. 1 of	Dale Dunckel	Affirmative	

	Okanogan County			
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Abstain	
1	Sacramento Municipal Utility District	Tim Kelley	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Negative	COMMENT RECEIVED
1	SaskPower	Wayne Guttormson		
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Negative	COMMENT RECEIVED
1	South Carolina Public Service Authority	Shawn T Abrams	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC Generation Subcommittee Comments)
1	Southern California Edison Company	Steven Mavis	Negative	COMMENT RECEIVED
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	COMMENT RECEIVED
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Texas Municipal Power Agency	Brent J Hebert		
1	Trans Bay Cable LLC	Steven Powell		
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
1	Western Area Power Administration	Lloyd A Linke	Negative	COMMENT RECEIVED
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Negative	SUPPORTS THIRD PARTY COMMENTS - (IRC/Standards Review Committee)
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Negative	SUPPORTS THIRD PARTY COMMENTS - (SRC)
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	COMMENT RECEIVED
2	ISO New England, Inc.	Kathleen Goodman		
2	Midwest ISO, Inc.	Marie Knox	Negative	SUPPORTS THIRD PARTY COMMENTS - (ISO/RTO SRC)
2	New York Independent System	Gregory Campoli	Abstain	

	Operator			
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Negative	COMMENT RECEIVED
3	AEP	Michael E Deloach	Abstain	
3	Alabama Power Company	Robert S Moore	Negative	COMMENT RECEIVED
3	Ameren Services	Mark Peters	Abstain	
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Avista Corp.	Scott J Kinney	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	COMMENT RECEIVED
3	City of Bartow, Florida	Matt Culverhouse		
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson		
3	City of Garland	Ronnie C Hoeinghaus	Negative	COMMENT RECEIVED
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	SUPPORTS THIRD PARTY COMMENTS - (supporting NPCC group comments)
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	CPS Energy	Jose Escamilla	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	Entergy	Joel T Plessinger	Abstain	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C Esquerre		
3	Florida Power Corporation	Lee Schuster	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
3	Georgia Power Company	Danny Lindsey	Negative	COMMENT RECEIVED
3	Georgia System Operations Corporation	Scott McGough	Abstain	
3	Great River Energy	Brian Glover	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF & ACES)
3	Gulf Power Company	Paul C Caldwell	Negative	COMMENT RECEIVED
3	Hydro One Networks, Inc.	David Kiguel		
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Kansas City Power & Light Co.	Charles Locke	Negative	COMMENT RECEIVED

3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lincoln Electric System	Jason Fortik	Abstain	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	Manitoba Hydro	Greg C. Parent	Negative	COMMENT RECEIVED
3	MEAG Power	Roger Brand	Abstain	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (I support comments submitted by the MRO NERC Standards Review Forum (NSRF))
3	Mississippi Power	Jeff Franklin	Negative	COMMENT RECEIVED
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	National Grid USA	Brian E Shanahan	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC Regional Standards Committee)
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera		
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Negative	SUPPORTS THIRD PARTY COMMENTS - (NIPSCO)
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Review Group)
3	Old Dominion Electric Coop.	Bill Watson		
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC group comments)
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Abstain	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz		
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Abstain	

3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC Generation Subcommittee Comments)
3	Seminole Electric Cooperative, Inc.	James R Frauen	Abstain	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-County Electric Cooperative, Inc.	Mike Swearingen	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Group)
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO)
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	COMMENT RECEIVED
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Georgia System Operations Corporation	Guy Andrews	Abstain	
4	Herb Schrayshuen	Herb Schrayshuen	Negative	COMMENT RECEIVED
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Abstain	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Abstain	
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	

4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Abstain	
5	Amerenue	Sam Dwyer	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments submitted by AZPS)
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke	Abstain	
5	BC Hydro and Power Authority	Clement Ma		
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Calpine Corporation	Hamid Zakery		
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	COMMENT RECEIVED
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC OC Standards Working Group)
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC group comments)
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Alexander Eizans	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC EC Generation Subcommittee)
5	Dynegy Inc.	Dan Roethemeyer	Negative	COMMENT RECEIVED
5	El Paso Electric Company	Gustavo Estrada	Abstain	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Entergy Services, Inc.	Tracey Stubbs	Negative	SUPPORTS THIRD PARTY COMMENTS - SERC

5	Essential Power, LLC	Patrick Brown	Negative	COMMENT RECEIVED
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF & ACES)
5	Hydro-Québec Production	Roger Dufresne	Negative	COMMENT RECEIVED
5	JEA	John J Babik	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Negative	SUPPORTS THIRD PARTY COMMENTS - (Generator Forum Standards Review Team)
5	Lincoln Electric System	Dennis Florom	Abstain	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Karin Schweitzer		
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	S N Fernando	Negative	COMMENT RECEIVED
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Abstain	
5	MidAmerican Energy Co.	Neil D Hammer		
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
5	NextEra Energy	Allen D Schriver		
5	NiSource	Huston Ferguson	Negative	SUPPORTS THIRD PARTY COMMENTS - (NIPSCO)
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson		
5	Oklahoma Gas and Electric Co.	Leo Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (We support comments previously submitted by SPP Standards Review Group.)

5	Omaha Public Power District	Mahmood Z. Safi	Abstain	
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Negative	SUPPORTS THIRD PARTY COMMENTS - (NAGF SRT)
5	PacifiCorp	Bonnie Marino-Blair	Abstain	
5	Pattern Gulf Wind LLC	Grit Schmieder-Copeland	Negative	SUPPORTS THIRD PARTY COMMENTS - (NAGF SRT)
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway		
5	PPL Generation LLC	Annette M Bannon	Negative	SUPPORTS THIRD PARTY COMMENTS - (PPL NERC Registered Affiliates)
5	PSEG Fossil LLC	Tim Kucey		
5	Public Utility District No. 1 of Chelan County	John Yale		
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	SUPPORTS THIRD PARTY COMMENTS - (NAGF Standard's Review Team)
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Raven Power	Scott A Etnoyer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Abstain	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC Generation Subcommittee Comments)
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Abstain	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	Southern California Edison Company	Denise Yaffe	Negative	COMMENT RECEIVED
5	Southern Company Generation	William D Shultz	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southern Company)
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha		
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State G & T Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Utility System Effeciencies, Inc. (USE)	Robert L Dintelman		
5	Western Farmers Electric Coop.	Clem Cassmeyer		
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles		
6	AEP Marketing	Edward P. Cox	Abstain	

6	Ameren Energy Marketing Co.	Jennifer Richardson	Abstain	
6	APS	Randy A. Young	Negative	COMMENT RECEIVED
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	COMMENT RECEIVED
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
6	Colorado Springs Utilities	Shannon Fair	Negative	SUPPORTS THIRD PARTY COMMENTS - (Cal ISO)
6	Con Edison Company of New York	David Balban	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC group comments)
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Municipal Power Pool	Thomas Washburn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF / ACES)
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Abstain	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brenda Hampton	Abstain	
6	Manitoba Hydro	Blair Mukanik	Negative	COMMENT RECEIVED
6	MidAmerican Energy Co.	Dennis Kimm		
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley		
6	New York Power Authority	Saul Rojas	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
6	Northern California Power Agency	Steve C Hill	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	SUPPORTS THIRD PARTY COMMENTS - (NIPSCO Comments)
6	NRG Energy, Inc.	Alan Johnson		
6	Oklahoma Gas & Electric Services	Jerry Nottnagel	Negative	NO COMMENT RECEIVED
6	Omaha Public Power District	Douglas Collins	Abstain	
6	PacifiCorp	Kelly Cumiskey	Abstain	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	PPL EnergyPlus LLC	Elizabeth Davis	Negative	SUPPORTS THIRD

				PARTY COMMENTS - (PPL NERC Registered Affiliates)
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Abstain	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC Generation Subcommittee comments.)
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Abstain	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	Southern California Edison Company	Lujuanna Medina		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	COMMENT RECEIVED
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS - (Lloyd Linke)
8		Edward C Stein		
8		Roger C Zaklukiewicz	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC)
10	Florida Reliability Coordinating Council	Linda Campbell		
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	COMMENT RECEIVED
10	ReliabilityFirst Corporation	Anthony E Jablonski	Negative	COMMENT RECEIVED
10	SERC Reliability Corporation	Joseph W Spencer	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments from the SERC EC Generation Subcommittee submitted by Ben Deutsch on 9/3/13)
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Individual or group. (79 Responses)
Name (52 Responses)
Organization (52 Responses)
Group Name (27 Responses)
Lead Contact (27 Responses)
IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE. (8 Responses)
Comments (79 Responses)
Question 1 (65 Responses)
Question 1 Comments (71 Responses)
Question 2 (67 Responses)
Question 2 Comments (71 Responses)
Question 3 (59 Responses)
Question 3 Comments (71 Responses)
Question 4 (0 Responses)
Question 4 Comments (71 Responses)

Group
Northeast Power Coordinating Council
Guy Zito
Yes
The SAR should not be posted with the Standard. The intent of posting a SAR for comment is to seek industry's input on the need and scope of a proposed standard's development or revision. Posting the Standard for comments and ballot means that the SAR is "water under the bridge", and that industry's input on the SAR doesn't mean anything.
Yes
VAR-002 uses footnote (3) on page 6 to clarify the phrase "voltage or Reactive Power schedule." VAR-001 does not use a footnote or otherwise define "voltage or Reactive Power schedule." Intead of using a footnote to clarify/define the phrase, add the phrase "voltage or Reactive Power schedule" to the Definitions of Terms Used in the Standard, making sure it is applicable to both VAR-001 and VAR-002. Suggest adding the following wording to both VAR-001 and VAR-002: Definitions of Terms Used in the Standard: Voltage or Reactive Power Schedule – A target value communicated by the Transmission Operator to the Generator Operator establishing a tolerance band within which the target value is to be maintained during a specified period. If this definition is added to VAR-001 and VAR-002, then VAR-002 footnote (3) should be deleted. For VAR-001-4: Recommend adding "upon request" to this sub-requirement to make it read: "Each Transmission Operator shall provide a copy of these documented policies or procedures to adjacent Transmission Operators, upon request." VAR-001 uses the term "real-time" (no capitalization) throughout, whereas VAR-002 uses the term "Real-time" (capitalized) in R1. The capitalized term is defined in the NERC Glossary of Terms Used. The Glossary definition is the meaning intended for both standards. Please use consistent terminology employing the capitalized Glossary term "Real-time" throughout both Standards. Regarding VAR-001, typically, the voltage and Reactive Power (VAR) output of a generator may be adjusted by one or more of three means: a no-load tap changer (NLTC), a load-tap changer (LTC), or an automatic voltage regulator (AVR). The requirements in the VAR-001 Standards should more fully and clearly address these Real-time and periodic NLTC, LTC and AVR changes or adjustments. The following wording changes are proposed for VAR-001 Requirements R1, R3, R4 and R6: The language of R1 includes key words such as "implemented" and "control voltage," representing Real-time actions taken by a TOP to keep voltages within limits that could be interpreted to include actions such as switching shunt capacitors/reactors, adjusting transformer taps, adjusting transfers, adjusting generation or other dynamic VAR sources (like SVC's). The intent of R1 may simply be to address the RC monitoring issue, as directed by FERC Order 742 (see Rationale for R1). However, the R1 language can also be interpreted to include the Real-time aspects of R4 creating a potential overlap. Depending on the interpretation and intent of the drafting team for R1, might R4 be a candidate for elimination? Regardless, clarity of wording and intent in R1 is needed. If the intent in R1 is to respond to FERC's

Order 742 directive to assure “monitoring,” then the Drafting Team should consider deleting the action verb “implemented.” The revised wording would read: R1. Each Transmission Operator shall have documented policies or procedures that are to establish, monitor, and control voltage levels and Reactive Power flows (Mvar flows) within limits … If “implemented” is not deleted, then it should be replaced by words conveying the intended meaning, e.g., “that are monitored and enforced.” However, there enforcement is inherent in all standards that all “documented policies or procedures” will be enforced. Application is verified by audit. Adding the phrase “that are implemented” is not needed, and can possibly lead to confusion. The TOP should only be required to develop exemption criteria in R3 if there is an established need for generator exemptions. Once the TOP has determined that there is a need for generator exemptions, only then should it be required to develop and implement exemption criteria. We recommend changing to word of R3 to not only conform to the appropriate Requirement format but include the preceding: R3. Each Transmission Operator shall determine the criteria that shall exempt generators from R4. Requirement R4 may already be covered by FAC-001 and Requirement R1 and may be deleted. But if not, it should be clarified recognizing the following: NLTCs are typically mechanically-fixed at time of generator interconnection and are only adjusted, if necessary, during a generator outage. The NLTCs may not be adjusted in Real-time. The TOP typically establishes initial voltage and Reactive Power requirements in the Interconnection Agreement under FAC-001-0, which states: R2. The Transmission Owner’s facility connection requirements shall address … R2.1.9. Voltage, Reactive Power, and power factor control. The interconnection provisions of R4 are covered in FAC standards. Non-Real-time Periodic timeframe changes in the NLTC settings may be addressed under Requirement R6. Requirement R6 does not appear to refer to Real-time operations and may be deleted from the Real-time standard. However, if it is not deleted, the wording should be revised to address NLTCs only. NLTCs are typically mechanically-fixed at time of generator interconnection and are only adjusted, if necessary, during a generator outage. The NLTCs may not be adjusted in Real-time. The initial NLTC settings are typically addressed during the generator interconnection process (see FAC-001). The need for a NLTC change is typically determined by the TOP through periodic (e.g., seasonal, 5-yr.) system studies. NLTCs adjustment are determined by and directed by the TOP. Alternatively, a load tap changer (LTC) may be adjusted by the GOP under load in Real-time. The setting of any LTC and the automatic voltage regulator (AVR) are typically under the control of the GOP. If this Requirement is referring to a LTC operation in Real-time, it is inappropriately assigned to the TOP. The GOP should have the flexibility to follow its voltage and Reactive Power schedule using the LTC and/or AVR. Alternatively, if the requirement is addressing changes applicable only to the NLTC, then it should be reworded accordingly. We assume the intent is to address NLTC tap changes only and recommend a wording/format change as follows: R6. Each Transmission Operator shall determine the need for generator step-up transformer no-load tap changes. 6.1 After consulting the Generator Operator regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Operator specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes. R1 can be interpreted to require a TOP to have documented policies or procedures in place that can be implemented to establish, monitor, and control voltage levels and Reactive Power flows (Mvar flows) within limits as defined in Parts 1.1 to 1.3. However, Part 1.1 requires that the policy/procedure shall include criteria used in system assessments. What is “system assessments” intended to mean? What is “criteria for the assessments” intended to mean, especially in relation to “established steady-state limits, voltage stability limits, etc.? If the assessments were meant to yield the “limits”, then there it is confusing as to what limits are intended to be developed in relation to the “established” limits. In Order 693, P. 1868, FERC directs the ERO to modify VAR-001-1 to include more detailed and definitive requirements on “established limits”. Does it mean more detailed and definitive requirements on stipulating voltage and reactive requirements with respect to established limits (SOLs, IROLs, voltage level, etc.), or does it mean more details on limits (boundaries) of the interconnection voltages as implied by Requirement R8 of the existing VAR-001 Standard? Requirement R1 does not provide clarity since Part 1.1. refers to “established steady-state limits, voltage stability limits”, which is different from the “established limits” presented in the R8 of the existing VAR-001 standard. Requirement R1 as presented does not provide any clarity as to what practice a TOP is required to meet. Requirement R1 as presented is unclear on its objective and the exact actions required of the Responsible Entity as there are a number of “criteria” and “limits” in the main requirement and its part 1.1 that are confusing and subject to different interpretations. R1 as presented will leave a Responsible Entity not knowing what it needs to do to meet Requirement and its reliability objectives.

Suggest that R1 and its parts be revised to clarify its intent, especially on the who, the specific actions and expected outcome according to the results-based principle and guideline. With respect to part 1.1, Measure M1 asks for evidence that proves voltage is currently being monitored. “Such evidence may include, but is not limited to: 1) proof that points are telemetered, 2) alarms are functioning, and 3) during events of low or high voltage the policies and procedures are being followed to respond to control voltage levels.” These examples of evidence do not reflect the scope and depth of R1 and Parts 1.1 (the criteria and assessment parts). R2 as presented appears to go beyond the FERC directive that RC be included to be assigned the “monitoring responsibility” as R2 now requires the RC to “….perform assessments on their respective areas in order to ensure sufficient reactive resources are available for scheduling to maintain voltage stability under normal and contingency conditions in order to provide the voltage levels as defined in Requirement R1.” The inclusion of RC in this requirement is also inconsistent with the view presented in the Informal Consideration with respect to parity between TOPs and RCs. Parts 2.1 and 2.2 stipulate a number of tasks for the TOPs with respect to operating or directing the real-time operation of devices necessary to regulate transmission voltage and reactive flow, and to ensure that sufficient reactive resources have been scheduled to meet the acceptable day-ahead voltage limits identified in Requirement R1. These tasks do not involve the RC. It thus raises a question on the need for including RC in the main requirement when it is not required to take further actions to assure its assessment of “sufficient reactive resources are available for scheduling to maintain voltage stability under normal and contingency conditions” can be fulfilled in real-time operations. We believe the inclusion of RC in this requirement is inappropriate, or if there is a compelling reason to include the RC, then Parts 2.1 and 2.2 are insufficient to assure the RC’s assessment can be supported in real-time operations. Requirement R2, Part 2.1 stipulates that the Transmission Operator has two things (operate or direct) that can be done to “…regulate transmission voltage and reactive flow necessary to regulate transmission voltage and reactive flow which may include…”. Part 2.1 should only contain one thing. The order of Requirements R3 and R4 should be reversed since the exemption criteria (R3) should appear after the overarching requirements for GOs to maintain a voltage or Reactive Power schedule and tolerance band. Regarding Requirement R5, suggest replacing “know” with “monitor”. This provides an active approach, which is appropriately reflected by the wording in Measure M5. In the Compliance Section, there is no requirement for the RC to retain evidence for Measure M2. Further, there is no requirement for the TOP to retain evidence for Measures M5 and M6. Regarding the VSL for R1, there is no explicit requirement in R1 for the TOP to provide a copy of the assessment criteria to its RC or neighbor TOPs since the assessment criteria are supposed to be included in the policy or procedure document. The Low VSL thus serves no purpose. Further, from the standpoint of meeting the intent of Requirement R1, there is little to no difference between having documented policies or procedures which do not include any of the elements stipulated in Parts 1.1 to 1.3, and having no documented policies or procedures at all. Suggest to remove the Low VSL and the High VSL, and keep the Moderate VSL and revise the Severe VSL to include the condition presented in the High VSL as an “OR” condition under the Severe VSL. Regarding the VSL for R2, throughout R2 there are no specific requirements for having policies and procedures implemented to have sufficient MVARs. R2 requires the TOP and RC to perform assessments on their respective areas in order to ensure sufficient reactive resources are available for scheduling to maintain voltage stability under normal and contingency conditions. Part 2.2 stipulates the requirements for scheduling reactive resources to meet the reactive requirements resulting from day-ahead assessments. Part 2.1 stipulates the requirement to operate or direct the real-time operation of devices necessary to regulate transmission voltage and reactive flow. While the Moderate VSL, which addresses non-compliance with Part 2.2 and appears to be reasonable, the Severe VSL does not correspond to how Part 2.1 is presented. The condition that “A lack of real-time operations is also severe.” seems irrelevant to Part 2.1 when it comes to operating or directing the real-time operation of devices necessary to regulate transmission voltage and reactive flow. There can be no lack of real-time operations, but a TOP may totally ignore the operations or directing the operations of devices necessary to regulate transmission voltage and reactive flow. There is no VSL for the RC failing to meet R2. Hence, the RC is assigned a responsibility but its compliance is not measured and there is no VSL to determine its non-compliance. Regarding the VSL for R5, the conditions in the Moderate and High VSLs are irrelevant to the requirement. R5 requires a TOP to know (monitor) the status of all transmission Reactive Power resources, automatic voltage regulators, and power system stabilizers in its system. The Moderate VSL makes reference to a “stable area”, which is totally irrelevant and out of context of R5. In the High VSL, the TOP not knowing “the status of important equipment in weaker areas that were identified in assessments as part of R1.” are also irrelevant and

out of context of R5. Finally, there is no Severe VSL. What constitutes a total failure to comply with Requirement R5? Regarding the VSL for R6, the Low VSL should have an “is”, not an “are”. There is no Severe VSL and hence there is no condition to constitute a total failure to comply with Requirement R6. VAR-002-3 Regarding Measure M2, M2 presents the scenarios where a Generator Operator may not be able to meet a voltage schedule or comply with the TOP’s directive, and how a GOP may manage the situations. The description part does not belong in a Measure, and should be moved to the Background Information Section that a Results-based standard template has made provision for. Regarding Measure M3, the latter part of M3 is not presented in a manner to require the evidence to demonstrate compliance. Suggest revising M3 to read: The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any of the changes identified in Requirement 3, or evidence that the status had been restored within the first 15 minutes of such change. For all Measures, there are no examples of evidence provided. It would be appropriate if after each of the “evidence”, additional wording “such as log, recording, or other documents” so as to be consistent with the way Measures are presented in other standards. Regarding Evidence Retention, it would be appropriate to reference the Measure Number for the GO’s and the GOP’s data retention requirements.
No
NERC’s Reliability Issue Steering Committee (RISC) is charged to address emerging reliability issues and recommend preferred approaches to manage such issues. Whether or not the TOP/GOP voltage coordination issue should rise up to a risk level that warrants special attention by the industry, and whether the appropriate way to address this issue in a standard project will be best evaluated and determined by the RISC. We suggest that the Drafting Team nominate this issue for RISC consideration. The Requirements in both VAR-001-4 and VAR-002-3 should be reviewed to ensure they are in the correct NERC Standard Development format.
Group
Arizona Public Service Company
Janet Smith, Regulatory Affairs Supervisor
No
Yes
VAR-001-4: R1: In addition to controlling voltage, R1 also requires procedure for control of reactive flow. Reactive flows are hard to control and there is no reliability benefits for controlling the reactive flow. Reference to reactive flow should be deleted. R2: This requirement is a duplication of requirements in other standards such as in TPL standards. Reactive assessment should not be part of this standard. R5: This requirement is unnecessary. A GO is already obligated to provide the status of AVR and PSS information to TO (VAR-002-3). This requirement puts unnecessary burden on TO to monitor status of all AVR and PSS. Particularly, TO does not have any value in knowing the PSS status. He cannot do anything with that information. There is no reliability benefit of this requirement. If the drafting team thinks that knowing the status of PSS is necessary for TO, please provide the rational. VAR-002-3: R3: Notifying the status of PSS is unnecessary since TO will not use that information for operating system any differently or do anything with that information. If the drafting team thinks that this information is necessary, please provide the rational.
Yes
There is no need to restrict the time to 15 minutes. It should be at least 30 minutes. For any system changes typically 30 minutes are allowed to readjust the system. A TO not knowing the status of AVR for 60 minutes is not going to cause any reliability issue. GO should be given 30 minutes to fix the problem and then 30 minutes to notify the TO if the problem is not fixed.
Individual
Terry Volkmann
Volkmann Consulting

No
Yes
VAR-001-4 R3 establishes the ability for the TOP to exempt a GOP from maintaining a voltage schedule and directing the GOP to perform in automatic and exempts from the report requirements that would be established under R4. VAR-002-3 R1 establishes the GOP requirement to operate in the automatic mode. This requirement is not prefaced with "unless exempted by the TOP". It is unclear that if the TOP has exempted the GOP from maintaining a voltage schedule in automatic and reporting AVR status changes, the GOP still needs to keep the AVR in automatic. If a generator is equipped with an AVR, but exempted by the TOP, one can interpret that the GOP still must maintain a voltage schedule (not TOP established) in automatic. Recommend modifying R1 with the lead in "unless exempted by the TOP,". This would clarify the intended operation of the GOP.
No
Individual
Thomas Foltz
American Electric Power
No
Yes
R5: We recommend that Requirement 5 and the associated subrequirement be applicable only to the Generator Owner and not split between the Generator Owner and Generator Operator.
No
AEP believes that additional coordination regarding high-side voltage schedules compared to low-side measurement (which is typical at the power plants) would be beneficial.
Individual
Dan Roethemeyer
Dynegy
Yes
In VAR-001-4 Applicability section 4.3 says “Generator Operators within the Western Interconnection”. But nowhere in the Standard does it discuss what are the responsibilities of the GOPs in the Western Interconnection. It has to do with the WECC variance to VAR-001 issued by FERC on 6-20-13 but VAR-001-4 does not explain it.
No
Yes
VAR-002-2 R2 requires the GOP to notify its associated TO within 15 minutes if both: 1) the GOP operated outside the voltage schedule for 15 minutes and 2) the GOP is no longer able to return to its voltage schedule. Regarding item 2) above, how long does the GOP have to return to its voltage schedule? Most GOPs eventually return to the voltage schedule, e.g., either a sister unit at the plant site returns from a forced outage boosting voltage or the wider area voltage returns to normal due to circumstances beyond the GOP’s control. If the GOP returns to its voltage schedule 24 hrs later, does that require notification? Regarding item 1) above, setting the threshold for operating outside the voltage schedule at 15 minutes seems overly prescriptive. Suppose a generator operates outside the voltage schedule for 14 mintues and then operates inside the schedule for 5 minutes, and the process repeats itself. The hourly average voltage may be outside the schedule, but the 15 minute threshold is never reached, so no notification is required. A simpler alternative to the 15 minute threshold would be to use a one hour clock average before reporting is required and eliminate item 2).

Group
US Bureau of Reclamation
Erika Doot
Yes
The Bureau of Reclamation (Reclamation) suggests that VAR-001-4 and VAR-002-3 should be combined into one standard because of the reciprocal requirements in each standard (e.g., VAR-001-4 R6 would require the Transmission Operator (TOP) to consult with the Generator Owner (GO) regarding TAP setting changes, and VAR-002-3 R5 requires the GO to ensure that tap positions are changed when possible). If the drafting team prefers not to combine the two standards, Reclamation requests that the drafting team explain why two standards are more appropriate. The Bureau of Reclamation (Reclamation) notes that VAR-001-4 appears to apply to Generator Operators within the Western Interconnection, and the White Paper on the VAR Standards dated July 18, 2013 explains that this is because the WECC variance in VAR-001-3 is retained in VAR-001-4. If the variance is retained, Reclamation suggests that the entire text of the variance should be included in VAR-001-4 rather than incorporated by reference in order to prevent confusion among registered entities. Reclamation also requests that the drafting team explain why the WECC variance would not be beneficial for reliability continent-wide.
Yes
The Bureau of Reclamation (Reclamation) notes that VAR-001-4 appears to apply to Generator Operators within the Western Interconnection, and the White Paper on the VAR Standards dated July 18, 2013 explains that this is because the WECC variance in VAR-001-3 is retained in VAR-001-4. If the variance is retained, Reclamation suggests that the entire text of the variance should be included in VAR-001-4 rather than incorporated by reference in order to prevent confusion among registered entities. Reclamation also requests that the drafting team explain why the WECC variance would not be beneficial for reliability continent-wide.
No
Reclamation believes that the scope of the project is appropriate.
Individual
Dave Willis
Idaho Power Company
No
Yes
VAR-002-3 R2, I think that this requirement is going to be very hard to document compliance. Monitoring voltage at the POI, tracking the time the voltage exceeds the limits and notification to the TOP all will need to be captured.
Yes
I think that the 30 minute notification after a 15 minute violations is reasonable but it think this requirement will be very hard to prove or disprove compliance. Is the intent for the TOP to monitor the GOP or is the GOP responsible to show compliance when there is a deviation. A GOP may not be monitoring the voltage at the POI and unaware that they are outside the voltage limits. If the GOP is not able to bring the bus voltage to within limits and contacts the TOP is there a length of time that they can be outside the bounds.
Coordination is a problem for the requirements in many standards and I'm not sure of a good way to improve coordination. I do not believe that this Standards Project is the time or place to address the issue.
Individual
R. J. Mattey
Ohio Valley Electric Corporation

No
Yes
VAR-001-4, R1, includes details about assessments and critierial that are more related to MOD and TPL standards. VAR-002-3, R2, now has two 15 minute times to track for compliance related to not maintaining a voltage schedule.
Yes
Only that additional compliance time frames have been added. Will a shorter time frame reduce the reliability gap?
This issue should not be addressed in compliance standards. Voltage coordination should be a function of the ERO as part of its normal function, handled through the appropriate committees.
Individual
Jonathan Appelbaum
The United Illuminating Company
Yes
The technical discussion paper last paragraph has a topic on the minority issue of voltage control and states the drafting team will investigate. I believe this should be included in the SAR.
Yes.
Individual
Ronnie C. Hoeinghaus
City of Garland
No
Yes
On all the requirements in VAR-001-4, the Time Horizons are defined as “Operations”. The NERC Document defining Time Horizons lists Operations Planning, Same-day Operations, Real-time Operations, and Operations Assessment – which one do you mean for each requirement? This needs to be corrected for each requirement.
No
Individual
John Seelke
Public Service Enterprise Group
Agree
NAGF SRT (North American Generator Forum Standards Review Team)
Individual
Steve Hill
Northern California Power Agency
Yes
Directive from P1875 states, "... we direct the ERO, through its Reliability Standards development process, to modify Reliability Standard VAR-001-1 to include Requirements to perform voltage stability analysis periodically, using online techniques where commercially-available and offline simulation tools where online tools are not available, to assist real time Operations." What online

models are being referred to? How do we know they are correct in their assessment? If the new TPL standard R5 is approved would this directive and R1 & R5 in the proposed VAR standard be redundant?
Yes
Same comment as in questions and comments as in Comment 1 in regards to R1 & R5. Controllable Load should be defined in R2.
Yes
There does not seem to be consensus on when a reliability gap would be created when expanding the time requirement, but is there consensus that there is no reliability gap with the 15 minute timeframe? There should be data to justify the timeframe to some confidence level.
I need to think about the first question more, but in regard to the second question I think the issue of improving votage coordination between TOP's and GOPs is vital to address in a Standards project since the Standard applies to GOPs
Group
MRO NERC Standards Review Forum
Russel Mountjoy
Yes
VAR-001-4: R4 of VAR-001-4 seems to have a potential inconsistency between the parenthetical statement and the balance of the requirement. It is suggested that R4 be rewritten and simplified as follows: “Each Transmission Operator shall specify a voltage or Reactive Power schedule and tolerance band for Generator Operators at either the high side or low side of the Generator Step-Up transformer at the TOP's discretion”.[Note the SDT may want to review the concept of “mutually agreed upon” instead of the TOP’s discretion] Additionally, there needs to be a feedback loop from the GOP to the TOP regarding the voltage schedule. The following allows the GOP to provide feedback regarding the feasability of the schedule. A recommended R4.2 for VAR-001 : R4.2 The Generator Operator shall review the voltage or Reactive Power schedule and tolerance band provided by the Transmission Operator and inform the Transmission Operator of any conditions that would prevent the Generator Operator from complying with the schedule or tolerance band, along with the technical basis for that determination. The question that then comes up is, what does the TOP do if the GOP cannot comply with the schedule as presented? Recommended R4.3 to read: R4.3 If the Generator Operator is unable to comply with the voltage or Reactive Power schedule or tolerance band as provided by the Transmission Operator, the Transmission Operator shall (a) modify the voltage schedule within the parameters established in the documented policies and procedures established in R1, taking into account the Generator Operator’s limitations, or (b) exempt the Generator Operator from following the voltage schedule or tolerance band using the criteria established in R3.To allow for coordination of operations between Transmission Operators and Generator Operators, it is suggest the the words “that is mutually agreed” after the words “timeframe for making the changes” be added in requirement R6 of VAR-001-4. A recommended change to R6 of VAR-001 is as follows: “After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes that is mutually agreed, and technical justification for these changes.” That is, the change should normally wait until it can be rolled into a scheduled downtime event. VAR-002-3 The following change to the rationale for R2 of VAR-002-3 is suggested: Change “…or when the unit is too small to raise voltage” to, “…or when the unit is too small to control voltage within the tolerance band.” The implications of footnote 4 to requirement R2 of VAR-002 is unclear in that it is not identified what stablility limit is being referred to: that of the voltage regulator or a transmission system stablility limit. If it is a transmission system stability limit it is unclear how a generator operator would be aware of it and how the generator operator should change the unit capability accordingly. R2 should read, “Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule (within each unit’s capabilities4) as directed by the Transmission Operator.” R2.1 should read, “If the voltage drifts out of schedule, each Generator Operator shall notify its associated Transmission Operator when both of the following conditions are met: 1) the parameter being controlled has been outside the prescribed voltage or Reactive Power schedule tolerance band for 15 minutes; and 2) the GOP is

unable to return the parameter being controlled to within the voltage or Reactive Power schedule tolerance band." What's drifting is the grid, not the generators. R2.2 should read, "When a generator's automatic voltage regulator is out-of-service, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator, unless the TOP grants an exemption." The purpose of this change is to reference the process established in R3 of VAR-001.

No

The NSRF request that "within 30 calendar days of a request." (of R4) be modified to "within 30 calendar days or agreed upon schedule of a request." This will allow small GOPss to establish a working rapport with their TOPs, since many small GOPs may only have one subject matter expert that has this technical information. Please break the Standards apart into separate ballots. Since the applicable entities are different and the Standards cover different reliability related requirements. Please clarify within Measure 2, that not every day of "system studies" are required to be on-hand as evidence, if the study has not changed, as stated in the last sentence of measure 2.

Group

Tennessee Valley Authority

Brandy Spraker

No

Yes

TVA appreciates the effort that the ad-hoc group has put into this revision. For VAR-001-4, TVA supports the SERC OC Review Group comments. For VAR-002-3, TVA has the following two comments: In R1, please add language to ensure that the TOp has the authority to exempt a generator unit. M2 reads like another requirement or technical rationale. Timing requirements should be made clear in the requirement itself, and the measurement should only detail the evidence needed for the corresponding requirement.

Yes

For R2, TVA requests that notification be based on voltage readings taken no more often than 60 minutes and no less often than 30 minutes. The degree of signal conditioning allowed should be addressed, expressed as a maximum interval for averaging the variable on which the reading is based. The time that the Generator Operator has to notify the Transmission Operator of a voltage reading outside the published schedule would be no greater than 15 minutes. Paragraph 2.1 would then read: "Each Generator Operator shall take voltage readings no less often than every 60 minutes. Voltage readings shall be averaged over a time interval no greater than 30 minutes. The Generator Operator shall notify its associated Transmission Operator within 15 minutes or a length of time determined and communicated by the Transmission Operator when the following conditions are met: 1) the GOP is operating outside of the prescribed voltage or Reactive Power schedule tolerance band at the time of the latest reading; 2) the GOP is no longer able to return to its voltage or Reactive Power schedule; and 3) no previous notification has been made for the same continuous excursion out of schedule."

Individual

Christy Koncz

Public Service Enterprise Group

No

Yes

VAR-001-4 a. In R4, the standard provides the TOP discretion on whether the voltage schedule provided is on the high or low side of the GSU "at the interconnection point between the generator facilitry and the Transmission Owner's facilities to be maintained by each generator. As written, the

sentence makes no sense. The interconnection point MAY BE on the GSU high side, our it MAY BE at a point where the GO's interconnection facilities connect to the TO's facilities. In other words, the GSU low side, the GSU high side, and the interconnection point may be three different places for a particular generator. To avoid this confusion, we recommend that R4 should be rewritten as the first sentence in R4 in VAR-001-3, with the footnote omitted, as shown below: "R4. Each Transmission Operator shall specify a voltage or Reactive Power schedule at the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator." This change maintains the framework which has existed through three versions of VAR-001. b. With regard to the WECC exception, page 11 under the "Regional Variance" section states: "Regional Variance for the Western Electricity Coordinating Council from VAR-001-3 is retained." We understand it is the intent for VAR-001-3 to be retired, so this reference presents a potential reference problem unless all parts of VAR-001-3 are retired EXCEPT Section E, which contains the WECC Variance. We recommend that Section E in VAR-001-3 in its entirety be brought into VAR-001-4 so that the new standard stands alone. VAR-002-3 With the suggested modifications in VAR-001-4 above, we suggest the following changes to VAR-002-3: c. In R2, subpart 2.1, the phrase "If a GOP drifts out of schedule" should be modified to "If a GOP's generator drifts out of schedule." d. In M2, we have both questions and suggested modifications. i. We do not understand why, in this sentence is in M2 what the phrase "based on existing equipment at its facility" refers to. Is the team referring to the equipment for monitoring the voltage? If not, what is intended? ii. Delete the following: "Therefore, GOPs have the option to operate on a voltage schedule on either the high-side or convert the high-side schedule to a low-side schedule at the GOP's discretion. For units that monitor on the low-side/terminal voltage, Generator Operators shall provide evidence of the method of conversion from the high-side schedule to low-side monitoring." This is not longer needed based upon the changes recommended in VAR-001-4 to NOT provide the TOP with discretion on the reference point for the voltage schedule. iii. For the sentence "Evidence may include, but is not limited to Generator Operator logs, SCADA data, phone logs, and any other alarming notifications that would alert the Transmission Operator that both conditions were met," we suggest that "and" be changed to "or."
No
In M3, the phrase "no call is necessary" should be changed to "no notification is necessary."
The single paragraph in the white paper was not specific enough to warrant a comment. Those that have concerns should express them through suggested modifications of the SAR, which defines the project's scope.
Individual
Jack Stamper
Clark Public Utilities
No
No
Yes
I do not see why there is a need for a fifteen minute cutuoff if the status has been restored. The requirement should allow 30 minutes to provide notification of a stauts change and if at any time during the 30 minutes the status is restored there should be no notification required. Under the current language, if the status is restored at 16 minutes, the GOP then needs to notify its TOP within the next 14 minutes that that generator status changed but returned to normal. How is that improving reliabiilty? It does not improve reliability. The purpose of the 30 minute delay is to allow a GOP to breifly investigate why the status or capabilty has changed and if the solution is at the plant, fix it quickly. I believe 30 minutes is a reasonable amount of time before the GOP needs to notify its TOP that a status or capability change has occured. The GOP will still attempt to fix it but has now notified the TOP. Whether the GOP fixed it in 2 minutes or 25 minutes it still does not need to notify the TOP until 30 minutes. If the problem is fixed before 30 minutes, the event is a non-event as far as the TOP is concerned (except that the TOP knows that it was briefly broken and is now fixed). The TOP is not going to change its operations or invoke some emergency plan for a generator that had a status or capabilty issue for 10 or 20 minutes but is now fine.

Individual
Michael Falvo
Independent Electricity System Operator
Yes
We question the need to ask this question when the consolidated standard is already posted for commenting and balloting. The intent of posting a SAR for comment is to seek industry's input on the need and scope of a proposed standard development/revision project. Posting the standard for balloting at the same time suggests that there is already a foregone conclusion on the need and the scope for this project , and that the industry's input on SAR would seem irrelevant. The IESO understands that posting a SAR and the draft standards for comment at the same time can improve standard development efficiency, and we support it to the extent that sufficient technical information has been obtained to facilitate the development of a draft standard at the informal outreach stage. However, we are very concerned about the fact that the industry was asked to ballot the draft standard when the need and scope of the draft standard have not been commented on and supported by the industry, and the standard itself has not been drafted by a formal standard drafting team. Such an approach appears to: a. Deviates from the normal standards development process as presented in the Standards Process Manual (SPM); b. Contradicts and perhaps violates the intent of the established standard development process and ANSI principles to have new and revised standard formally developed through an open and inclusive process before being presented to the RBB for balloting. The industry is being asked to ballot a set of standards that has not been formally developed. This concept appears to be fundamentally flawed. We propose that the SDT convey our concern to the NERC senior management and the Standards Committee. We further suggest that NERC and the SC evaluate alternative approaches or make revisions to the SPM to provide the needed flexibility that can further improve the efficiency in standard development if certain elements in the existing SPM are assessed to restrict such improvements.
Yes
VAR-001-4 a. It is unclear on the main objective and the target reliability outcome of Requirement R1, and the intent of the proposed changes in relation to the directive in P. 1868 in Order 693. We interpret R1 to require a TOP to have documented policies or procedures in place that can be implemented to establish, monitor, and control voltage levels and Reactive Power flows (Mvar flows) within limits as defined in Parts 1.1 to 1.3. However, Part 1.1 requires that the policy/procedure shall include criteria used in system assessments. It is unclear as to what "system assessments" means? Does it mean assessments of the TOP area's reliability performance with respect to the voltage levels and Mvar flows and any limits (SOLs, IROLs, reactive capability)? Or does it mean the system assessment that yields the "limits" (SOLs, IROLs, reactive requirements, etc.) which provide the target and guideline for the establishment, monitoring, and control of voltage levels and Mvar flows? It is also unclear as to what the "criteria of the assessments" means in the second sentence of Part 1.1, especially in relation to "established steady-state limits, voltage stability limits, etc. if the answer to the above question is that the assessments were meant to yield the "limits", then there is a confusion as to what limits are intended to be developed in relation to the "established" limits. In Order 693, P. 1868, FERC directs the ERO to modify VAR-001-1 to include more detailed and definitive requirements on "established limits". However, it is unclear what this directive really means. Does it mean more details and definitive requirement on stipulating voltage and reactive requirements with respect to established limits (SOLs, IROLs, voltage level, etc.) or does it mean more details on limits (boundaries) of the interconnection voltages as implied by Requirement R8 of the existing VAR-001 standard? Requirement R1 does not provide this clarity since Part 1.1. refers to "established steady-state limits, voltage stability limits", which is different than the "established limits" presented in the R8 of the existing VAR-001 standard. It is our understanding that as a general practice, a TOP will assess if there exists any reliability concerns that can be caused by voltage levels and instability to develop operating limits (SOLs or IROLs) to ensure reliable operations. The operating limits may be expressed in voltage level, pre and post-contingency power flow level, reactive support requirements or any combination of the above. The operating limits so established will provide a linkage between the SOL, voltage level and reactive power capability/reserve requirement either explicitly or implicitly. System Operators will monitor the key parameters including

voltage level, power flow level and reactive power flow/reserve/capability to meet the SOL boundary conditions. Requirement R1 as presented does not provide any clarity as to what is it that in the practice that a TOP is required to meet. Requirement R1 as presented is unclear on its objective and the exact actions required of the Responsible Entity as there are a number of "criteria" and "limits" in the main requirement and its Part 1.1 that are confusing and subject to different interpretation. R1 as presented will leave a Responsible Entity not knowing what it needs to do to meet Requirement and its reliability objectives. We suggest the SDT to revise R1 and its parts to clarify its intent, especially on the who, the specific actions and expected outcome according to the results-based principle and guideline. Note that with respect to Part 1.1, Measure M1 asks for evidence that proves voltage is currently being monitored. Such evidence may include, but is not limited to: 1) proof that points are telemetered, 2) alarms are functioning, and 3) during events of low or high voltage the policies and procedures are being followed to respond to control voltage levels. These examples of evidence do not reflect the scope and depth of R1 and Parts 1.1 (the criteria and the assessment parts). b. FERC directive 1855 directs NERC to include Reliability Coordinator as applicable entities and include a new requirement(s) that identifies the reliability coordinator's monitoring responsibilities. In the Informal Consideration specific to this directive presented in the White Paper, it is indicated that: "Although some entities in Texas provided feedback that certain RCs perform functions equivalent to a TOP, the informal development group did not expand VAR-001 to give parity to TOPs and RCs." R2 as presented appears to go beyond the FERC directive that RC be included to be assigned the "monitoring responsibility" as R2 now requires the RC to "….perform assessments on their respective areas in order to ensure sufficient reactive resources are available for scheduling to maintain voltage stability under normal and contingency conditions in order to provide the voltage levels as defined in Requirement R1". The inclusion of RC in this requirement is also inconsistent with the view presented in the Informal Consideration with respect to parity between TOPs and RCs. Parts 2.1 and 2.2 stipulates a number of tasks for the TOPs with respect to operating or directing the real-time operation of devices necessary to regulate transmission voltage and reactive flow, and to ensure that sufficient reactive resources have been scheduled to meet acceptable day-ahead voltage limits identified in Requirement R1. These tasks do not involve the RC. It thus raises a question on the need for including RC in the main requirement when it is not required to take further actions to assure its assessment of "sufficient reactive resources are available for scheduling to maintain voltage stability under normal and contingency conditions" can be fulfilled in real-time operations. We believe the inclusion of RC in this requirement is inappropriate, or if there is a compelling reason to include the RC, then Parts 2.1 and 2.2 are insufficient to assure the RC's assessment can be supported in real-time operations. c. Requirement R2, Part 2.1 stipulates that: "Each Transmission Operator shall operate or direct the real-time operation of devices necessary to regulate transmission voltage and reactive flow necessary to regulate transmission voltage and reactive flow which may include…" We do not understand this requirement as it contains two sets of "necessary to regulate transmission voltage and reactive flow". If this is a typographical error, please correct it. d. We do not have any concerns or comments on R3 and R4 as presented, but suggest that their order be reversed since the exemption criteria (R3) should appear after the overarching requirements for GOs to maintain a voltage or Reactive Power schedule and tolerance band. e. R5: we suggest to change the word "know" to "monitor". This provides an active approach, which is appropriately reflected by the wording in Measure M4. f. In the Compliance Section, there is no requirement for the RC to retain evidence for Measure M2. Further, there is no requirement for the TOP to retain evidence for Measures M5 and M6. g. VSL for R1: There is no explicit requirement in R1 for the TOP to provide a copy of the assessment criteria to its RC or neighbor TOPs since the assessment criteria are supposed to be included in the policy or procedure document. The Low VSL thus serves no purpose whatsoever. Further, from the standpoint of meeting the intent of Requirement R1, there is little to no difference between having documented policies or procedures which do not include any of the elements stipulated in Parts 1.1 to 1.3, and having no documented policies or procedures at all. In the former case, the documented policies or procedures provide absolutely no value, and hence is it a total violation of the intent of R1. We suggest to remove the Low VSL and the High VSL, and keep the Moderate VSL and revise the Severe VSL to include the condition presented in the High VSL as an "OR" condition under the Severe VSL. h. VSL for R2: Throughout R2, there are not specific requirements for having policies and procedures implemented to have sufficient Mvars. R2 requires the TOP and RC to perform assessments on their respective areas in order to ensure sufficient reactive resources are available for scheduling to maintain voltage stability under normal and contingency conditions. Part 2.2 stipulates the requirements for scheduling reactive resources to meet

the reactive requirements resulting from day-ahead assessments. Part 2.1 stipulates the requirement to operate or direct the real-time operation of devices necessary to regulate transmission voltage and reactive flow. While the Moderate VSL which address non-compliance with Part 2.2 and appears to be reasonable, the Severe VSL does not correspond to how Part 2.1 is presented. Further, the condition that “A lack of real-time operations is also severe.” seems irrelevant to Part 2.1 when it comes to operating or directing the real-time operation of devices necessary to regulate transmission voltage and reactive flow. There can be no lack of real-time operations, but a TOP may totally ignore the operations or directing the operations of devices necessary to regulate transmission voltage and reactive flow. Finally, there is no VSL for the RC failing to meet R2. Hence, RC is assigned a responsibility but its compliance is not measured and there is no VSL to determine its non-compliance. i. VSL for R5: The conditions in the Moderate and High VSLs are irrelevant to the requirement. R5 requires a TOP to know (monitor) the status of all transmission Reactive Power resources, automatic voltage regulators, and power system stabilizers in their system. The Moderate VSL makes reference to a “stable area”, which is totally irrelevant and out of context of R5. In the High VSL, the TOP not knowing “the status of important equipment in weaker areas that were identified in assessments as part of R1.” are also irrelevant and out of context of R5. Finally, there is no Severe VSL. It begs the question on: what constitutes a total failure to comply with Requirement R5? j. VSL for R6: The Low VSL should have an “is”, not an “are”. Also, there is no Severe VSL and hence there is no condition to constitute a total failure to comply with Requirement R6. VAR-002-3 k. Measure M2: A good part of M2 presents the scenarios where a Generator Operator may not be able to meet voltage schedule or comply with the TOP’s directive, and how a GOP may mange the situations. The description part does not belong to a Measure, and should be moved to the Background Information Section that a Results-based standard template has made provision for. l. Measure M3: the latter part of M3 is not presented in a manner to require the evidence to demonstrate compliance. We suggest M3 be revised to: The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any of the changes identified in Requirement 3, or evidence that the status had been restored within the first 15 minutes of such change. m. For all Measures, there are no examples of evidence provided. It will be appropriate if after each of the “evidence”, additional wording “such as log, recording, or other documents” so as to be consistent with the way measures are presented in other standards. n. Evidence Retention: It will be appropriate to reference the Measure Number for the GO’s and the GOP’s data retention requirements.
No
NERC’s Reliability Issue Steering Committee (RISC) is charged to address emerging reliability issues and recommend preferred approaches to manage such issues. Whether or not the TOP/GOP voltage coordination issue should rise up to a risk level that warrants special attention by the industry, and whether the appropriate way to address this issue in a standard project will be best evaluated and determined by the RISC. We suggest that the SDT nominate this issue to the RISC for its deliberation.
Individual
Martin Kaufman
ExxonMobil Research and Engineering
No
Yes
The SDT should revisit VAR-002-3 Requirement R2 (including sub-requirements) and Measure M2. Generators should be required to operate in automatic voltage control mode and implement a setpoint consistent with the voltage target (schedule, etc.). The current requirement combined with the measure presents a framework that opens new reliability gaps. For example, in the new framework, if the voltage in a localized area goes low, the generators that notice the drop first are encouraged to deviate from actions that are predictable and take independent action to alter their control systems to provide the system more VARs. This presents three problems: 1) The ideal situation would be for the Transmission Operator to allow sufficient time for all of the generators under its control to automatically respond and then issue specific dispatch instructions to those units that are optimally able to resolve the issue: 2) When numerous generators take independent action, it’s questionable as

to whether the Transmission Operator's real-time evaluations of system contingencies are accurate b/c the assumptions related to how a generator will respond are no longer accurate and are unpredicatable due to the independent actions taken by GOPs; and 3) The generators that are slower to notice the voltage dip will likely not alter their control system parameters; allow for the automatic voltage regulator to respond (at which point adequate voltage will likely be restored); and, potentially, these units will have an economic advantage over similarly sized units because they are supplying less VARs than the units that took independent action (If you generate more VARS you can generate less Watts at maximum MVA on the generator capability curve). Additionally, Measure M2's statement "For units that monitor on the low-side/terminal voltage, Generator Operators shall provide evidence of the method of conversion from the high-side schedule to low-side monitoring" creates a hidden defacto requirement for those units that control their units based on the low-side of the GSUT. It's unclear how possession of a conversion method without any clear criteria for what should be included in the conversion method could 1) improve system reliability and 2) be evaluated by an auditor during a compliance audit. The majority of generators on the grid are controlled on the low-side of the GSUT. Under normal conditions, since generator's operation is validated when the unit is brought on-line and voltage schedules should consider N-1 and credible N-2 contingencies, the voltage drop across and losses through the GSUT should have minimal impact (on an individual generator basis) on the voltage quality of the grid. If the technical concern is based on the aggregated impact of GSUTs' voltage regulation varing with loading, then criteria for a methodology should be developed for those units that do not have the capability to monitor the high side voltage in real-time. However, industry input feedback indicates that only a minority of generation units that control on the low-side of the GSUT do not have high-side monitoring. The majority of units that control their AVR based on the low-side of the GSUT do see the high-side voltage and would notify the Transmission Operator of a deviation from the voltage schedule lasting longer than 15 minutes (VAR-002 R2), which would allow the Transmission Operator to direct the Generator Operators under their control to correct the deviation in a predictable and economic fashion AND would allow the Transmission Operator to calibrate any assumptions / variables necessary in their real-time models so that the real-time evaluations reflect accurate input data. Additionally, we would suggest that the models used by Transmission Operator to satisfy requirements R1 and R2 of the draft VAR-001 standard should account for the GSUT's voltage regulation characteristics under normal system operation in order to accurately reflect that Generators are controlling the low-side bus.
If the Transmission Operator has not reached a pre-defined system operating alarm / limit and the Generator Operator is already operating with its automatic voltage regulatory in voltage control mode, what reliability concern is alleviated by the Generator Operator notifying the Transmission Operator that the voltage on the Generator Operator is monitoring has drifted off of schedule? The majority of units on the grid are unable to move the grid voltage by themselves, which is why VAR-002 requires that the aggregate operate in voltage control mode, and the likely cause of the event is a system contingency that the Transmission Operator has: A) planned for in their development of operating limits and is still within their pre-defined operating limits; B) has not planned for and is still within their pre-defined operating limits; or C) has not planned for and is outside of their pre-defined operating limits AND should be the only one taking independent action so that the system's response to the Transmission Operator's actions is predictable.
Individual
David Jendras
Ameren
No
Yes
For the most part we agree with the GS Subcommittee comments but we also have included are our specific comments below.
Yes
(1) R2 – We request the SDT to clarify this requirement. As it is written we believe operators may be confused of knowing when the new "15 minute" time period will start. Since it seems (under the draft) to be OK, that we can drift in and out of the Voltage Schedule for several hours if the operator

thinks the machine can get back on the VS later. How will our operators know when the 15 minute report trigger has occurred? (2) R2 – We believe the 15 minute time period is too short for mandatory reporting to the TOS. We ask the SDT to consider that currently there is no specific time period, and therefore we will need to modify our procedures accordingly. (3) Whether in VAR-001 or VAR-002 temporary exemptions are not appropriate. There may be circumstances that a generator should be declared exempt consistent with VAR-001 Requirement 3. These type of exemptions should be declared and documented outside of any particular period of inability to maintain the voltage schedule. Rather than have temporary exemptions if a generator were unable to operate in AVR or if operating in AVR the generator could not operate in the band of the voltage schedule, language should reflect that the notification of the inability is made to the TOP and the TOP will provide further instruction for operation, i.e. a set VAR output, a specific power factor, to the unit D-curve, etc. This would ensure that even if a generator could not meet the voltage schedule they should be as near the voltage schedule as is possible. Being exempted might give the generator the notion, "Since I am unable to get to my voltage schedule and I am therefore exempt, it does not matter how I operate." That should never be the case. (4) Whether in VAR-001 or VAR-002 temporary exemptions are not appropriate. There may be circumstances that a generator should be declared exempt consistent with VAR-001 Requirement 3. These type of exemptions should be declared and documented outside of any particular period of inability to maintain the voltage schedule. Rather than have temporary exemptions if a generator were unable to operate in AVR or if operating in AVR the generator could not operate in the band of the voltage schedule, language should reflect that the notification of the inability is made to the TOP and the TOP will provide further instruction for operation, i.e. a set VAR output, a specific power factor, to the unit D-curve, etc. This would ensure that even if a generator could not meet the voltage schedule they should be as near the voltage schedule as is possible. Being exempted might give the generator the notion, "Since I am unable to get to my voltage schedule and I am therefore exempt, it does not matter how I operate." That should never be the case. (5) M2 – A "30 minute" time period is allowed in M2 that appears to not be included, explained or mentioned in R2, please clarify. (6) We believe the TOP should set the reporting time period and it should not be set in the Standard. Our TOP has told us is the 15 minuet reporting is excessive and not necessary for reliable operation of the transmission system. (7) M2 – The first sentence of M2 requires the GOP to "make all attempts to operate within the tolerance bands provided by the TOP". We ask the SDT to explain from a generator perspective and provide an example for how this can be proven to an auditor?
Individual
Chris de Graffenried
Consolidate Edison Co. of NY, Inc.
Agree
Northeast Power Coordinating Council (NPCC) - All comments.
Individual
David Burke
Orange and Rockland Utilities, Inc
Agree
Northeast Power Coordinating Council (NPCC) - all comments.
Group
FirstEnergy
Larry Raczkowski
No
No
Yes
FE believes that #2 of Part 2.1 of Requirement 2 needs clarity. Since both conditions of Part 2.1 must be met, there should be a time parameter associated with #2. Otherwise, unless something

catastrophic happens, #2 will always be true, ie, we expect to be back on schedule at some time. We propose the folloing for #2 of Part 2.1 of Requirement 2 2) the GOP is unable to return to its voltage or Reactive Power schedule within 30 minutes of operating outside the prescribed schedule.
Individual
Michelle R D'Antuono
Ingelside Cogeneration LP (Occidental Chemical Corporation)
Yes
Ingleside Cogeneration LP supports the changes that have been made to both VAR standards. First, we agree that the removal of FERC's two LSE-related directives can be justified using the Paragraph 81 criteria. Directive 1858, which calls for LSEs to take on Reactive Power responsibilities consistent with PSEs, can be retired (as can VAR-001-2 R5) since those actions are already governed by the OATT. Similarly, the directive that LSEs maintain power factors within a given range is a normal part of interconnection agreements. Since both the OATT and pro-forma interconnection agreements are under regulatory control, reliability requirements are an unnecessary redundancy. Secondly, we agree with the need to include precise language in the measures to assure that Compliance Enforcement Authorities are looking for situations that present true risk to the BES. For example, the measure for VAR-002-3 R2 clearly accounts for those configurations where the GOP monitors voltage and reactive power flows at the generator output instead of the interconnection. In these cases, the CEA needs to understand that a conversion mechanism is sufficient – and not insist that high-side voltage and reative power monitoring is specifically required.
Yes
In particular, Ingleside Cogeneration would like to see the changes made to VAR-002-3 R3 take effect. We agree that there needs to be a level of tolerance around the communication of an AVR outages – those that are restored within 15 minutes pose no viable threat to the BES and only serve to distract the Transmission Operator from more pressing tasks. Although it does not change our vote to approve both of the VAR standards, we would like to suggest that a referece could be added under R1 to capture the same 15 minute criteria. Otherwise it seems possible that any uncommunicated AVR outage will violate R1, even if compliant with R3.
No
Ingleside Cogeneration would hesitate to call for more standards development activity related to TOP/GOP voltage and reactive communication. In our view, the issue does not appear during normal and semi-normal operations (i.e.; the generator is able to maintain voltage and reactive power within tolerance without exceeding its Facility Ratings). It may be a different story during an event where transients driven by the external network exceed a generation facility's capabilities. Since the proper action to take relies on the character of the transient – whether it is of long-duration/short-duration – and the topology of the local system, and the availability of other nearby reactive resources, the GOP can only take best-effort steps to maintain output to the TOP's schedule. We rely on guidance from the TOP if there are actions that must be taken beyond that point. For example, if a GOP were to make a change to a voltage setpoint outside of the threshold range without the TOP's guidance, the impact to the local system may actually worsen. Ingleside understands that during an emergency, the TOP may be otherwise engaged with many other operating entities – and may need the GOP to take helpful actions to stabilize the situation without direct supervision. However, there needs to be some pre-developed universal criteria in place before we would be comfortable proceding in this direction. In our view, this is an issue best taken up in a NERC sub-committee or task force – not a SDT.
Individual
David Austin / Ed Mackowicz
NIPSCO
Yes
We would like to see this project divided into two separate projects/ ballots. We are fine with the proposed VAR-002-3, but have some concerns with VAR-001-4. Ultimately, this means we must vote

negative for both standards instead of just one.
Yes
1. VAR-001 causes concern for the uncertainty of how to come up with a basis of how we plan operations. Is our performance over the last "x" years enough to justify no change, or do we need to study for voltage and VARs for the day(s) ahead and in real time (two extremes)? 2. There are discrepancies or vagueness between interpretations in new VAR standards and other standards like TOP. Which one trumps the other? 3. In general, the individual standards can be made to work. However, the interdependencies and the ability to go off on a tangential path between VAR, TOP and other related standards is troublesome. While each standard may be good as a solo act, they do not make a symphony together. RECOMMENDATIONS: A. All of the standards should be placed on a matrix so that interdependencies are identified and coordinated in application and measurement. B. The standards need to be stable over time as opposed to new ones being voted on before the previous one is implemented. C. A multi-year process where interdependent standards are adjusted and implemented in unison will yield a productive effort by the industry towards being more reliable rather than concentrating on avoidance of violations.
No
Individual
Brett Holland
Kansas City Power & Light
No
Yes
In VAR-001-4, depending on what periodicity and type of studies required in R2, this could overly burdensome to the registered entities to show evidence of compliance.
No
We would add that any proposed improvement to the voltage coordination between the TOPs and GOPs is a suggested guidance or level of expectation.
Group
Salt River Project
Bob Steiger
No
No
No
No comments from SRP
Individual
Lynda Kupfer
Puget Sound Energy
No
Yes
VAR-001-4 Comments Requirement R2 appears to be a mix of planning and operational processes. Since the main section of the requirement only addresses the planning process, part 2.1, which

addresses operational issues, seems out of place. In addition, since part 2.2 goes back to addressing planning processes, part 2.1 also seems out of sequence. This could be addressed by revising the main section of requirement R2 to address how the planning and operational aspects interrelate and then reordering parts 2.1 and 2.2. Alternatively and preferably, part 2.1 could be a stand-alone requirement, since it also addresses complying with the limits under the processes required by requirement R1. The drafting team should consider deleting the language "and direct the Generator Operator to comply with the schedule in automatic voltage control (the AVR is in service and controlling voltage)" from part 4.1 of requirement R4. Since VAR-002 requires the GOPs to operate in AVR mode and to follow the voltage schedule, the quoted language is both redundant and administrative in nature. Minor conforming changes would be necessary in VAR-002 (replacing the phase "as directed" with "provided" where that standard references the schedule should be sufficient to address this change). The last sentence of measure M5 should be deleted since it is redundant with EOP-008-1, which requires TOPs to have backup control center functionality available to address the loss of primary control center functionality. Losing the ability to monitor voltage would be a loss of primary control center functionality that is addressed by EOP-008-1.
Yes
VAR-002-3 Comment R2.1 condition 2 is vague and unclear how this should be interpreted "…no longer able to return…" What if you knew you were going to be able to return to schedule tomorrow? Would you need to report?
Individual
Herb Schrayshuen
Self
No
Yes
VAR-002 footnote (3) on page 6 offers a definition of the phrase "voltage or Reactive Power schedule." VAR-001 does not define "voltage or Reactive Power schedule." The term "voltage or Reactive Power schedule" should be defined for both standards. The voltage and Reactive Power (VAR) output of a generator is adjusted by several methods. The requirements in the VAR-001 Standard should state in terms of an action oriented result, what is expected. In VAR-002 M2 provides situations where a Generator Operator may not be able to meet a voltage schedule or comply with the TOP's directive. The description does not belong in a Measure, and should be moved to the Background Information Section of the Results-based standard. The proposed requirements in both VAR-001 and VAR-002 should be carefully reviewed to ensure they meet the expectations of a results based standard.
No
Group
Tacoma Public Utilities
Michael Hill
Yes
Concerned about the significant overlap in these standards vs: their long term accuracy.
Yes

VAR-001: -R3, Concern over the TO setting the criteria for when an AVR may be out of service. Could look to the current exceptions table for guidence. -R4 is poorly written and needs editing. Are we to specify the schedule a the point of interconnection, GSU hi side, GSU lo side, or a combination? Also, R3 allows the TO to exempt when the AVR must be in service, but R4.1 doesn't reference this exemption. VAR-002: -R1 confilcts directly with VAR-001 R4.1. Again, I read VAR-001 R4.1 to state the TO is giving the GO a directive to always be in AVR mode. No room is given for exceptions, (could easily correct this).
No
Individual
Kayleigh Wilkerson
Lincoln Electric System
MRO NSRF
No
Yes
Although supportive of the drafting team's efforts, LES is concerned with the removal of the FERC-approved interpretation previously appended to VAR-002-2b. Per the Interpretation, the Transmission Operator is permitted the option of directing the Generator Owner to operate the AVR in the constant Pf or constant Mvar modes rather than the constant voltage mode. In consideration that Requirements R1 and R2 of VAR-002 have not changed significantly, it is difficult to discern whether or not the Interpretation still applies. To ensure clarity going forward, LES recommends the interpretation either be appended to VAR-002-3 as well or else the drafting team further modify the requirements and/or measures to allow the TOP to direct the GO to run in a mode other than constant voltage.
Group
SERC OC Review Group
Catherine Wesley
Yes
There is a general concern with this proposed standard that it will create further administrative burden for the TOP/RC as well as the back office staff. Additionally, the opportunity exists that the number of calls between the GOP and TOP will increase without materially enhancing BES reliability. Further, how would these standards be used to evaluate the compliance of a unit which has their AVR taken off auto for testing?
Yes
VAR-001-4 Comments: R1.1.2. Each Transmission Operator shall Delete: "provide a copy of these documented policies or procedures to adjacent Transmission Operators" make plans available with a written request so entities requiring documents have access. R1.1.3. Each Transmission Operator shall Delete:"provide a copy of these documented policies or procedures to its Reliability Coordinator." make plans available with a written request so entities requiring documents have access. R2. Each Transmission Operator and Reliability Coordinator shall perform assessments on their respective areas in order to ensure sufficient reactive resources are available Delete: "for scheduling" to maintain voltage stability under normal and contingency conditions in order to provide the voltage levels as defined in Requirement R1. R2.2.2. As a result of the assessments, each Transmission Operator shall ensure that sufficient reactive resources Delete: " have been scheduled" Add: "are available" to meet acceptable day-ahead voltage limits identified in Requirement R1. Sufficient reactive resources may include, but is not limited to reactive generation scheduling; transmission line and reactive resource switching; and controllable load. M2 (excerpt): During a "real-time event" where voltage must be adjusted, a Transmission Operator shall show evidence to show directions were given to adjust the operation of capacitive and inductive resources. It is requested that the SDT provide additional

clarification what is meant by “real-time event” and whether it refers to normal operations or disturbances. SDT Question: How does the SDT anticipate this measure be used to evaluate the compliance of a unit which has their AVR taken off auto for testing? M3 (excerpt): For temporary exemptions, evidence showing the exemptions were granted must be provided. If the exemptions were given verbally from the Transmission Operator, the phone recordings or emails commemorating the phone call must be provided. For temporary exemptions, the evidence of communication must also include the timeframe for how long the exemption will last. We believe that this measure will increase the administrative burden placed on the TOP/GOP in real-time. R4.4.1. The Transmission Operator shall provide the voltage or Reactive Power schedule and tolerance band to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode. Delete:”(the AVR is in service and controlling voltage).“ R5. The Transmission Operator shall know the status of Delete:”all transmission” Add: “ BES” Reactive Power resources, automatic voltage regulators, and power system stabilizers in their system. Request that the SDT review R5 to ensure that it is not a duplicative of a TOP standard. M5. The Transmission Operator shall have evidence to show Reactive Power resources are being monitored. Evidence may include, but is not limited to screen shots of EMS/SCADA data, alarms, and phone logs. In the event the monitoring system does not work, each Transmission Operator should have a protocol in place to show these resources are being monitored. Request the SDT to add further clarification for AVR and PSS. VAR-002-3 Comments: R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless Delete:”the Generator Operator has notified the Transmission Operator of one of the following: “a generator has been has been exempted from operating in the AVR voltage control mode by the Transmission Operator or the Generator Operator has notified the Transmission Operator of one of the following: M1. Add: "Unless exempted" the Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode as specified in Requirement 1. 2.1. If a GOP drifts out of schedule, each Generator Operator shall notify its associated Transmission Operator within 15 minutes when both of the following conditions are met: 1) the GOP is operating outside of the prescribed voltage or Reactive Power schedule tolerance band for Change from 15 to 30: 30 minutes; and 2) the GOP is no longer able to return to its voltage or Reactive Power schedule. M2 excerpt: 1) Communications with the TOP when the Generator Operator was operating outside of the prescribed voltage or Reactive Power schedule tolerance band for 30 minutes Delete: “or less the 30 minutes allow for 15 minutes to call and 15 minutes to be outside of the tolerance band)” AND Generator Operator is no longer able to return to its voltage or Reactive Power schedule; 2) R3. Request a threshold be defined for the term “capability change” M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any of the changes identified in Requirement 3. If the status has been restored within the first 15 minutes, no call is necessary Delete: "therefore, if a status on Reactive Power resource has changed, and that change lasts greater than 15 minutes, the GOP must notify its associated TOP within 30 minutes of when the change first occurred.”
Yes
We are unclear on how the draft time period was arrived at. Without that information it is difficult to compare time periods. The concern is the potential administrative burden placed on the TOP.
Strong communications between TOPs and GOPs is essential for reliability of the system. The concern that we have centers on the potential administrative burden that is placed on the TOPs and GOPs. The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Review Group only and should not be construed as the position of the SERC Reliability Corporation, or its board or its officers.
Group
Dominion NERC Compliance Policy
Randi Heise
No
Yes
VAR-001-4 • R1.1.2 amd R1.1.3 – Dominion suggests addition of the words ‘if requested”. This will

lessen administrative burden. • R2.1; “necessary to regulate transmission voltage and reactive flow” seems to be listed twice in this requirement, please clarify. • R3.1; Dominion suggests replacing “it” with “the Transmission Operator” • M3; Dominion suggests replacing “its” with “the Transmission Operators” • R6 - To allow for coordination of operations between Transmission Operators and Generator Operators, it is suggest the the words “that is mutually agreed” after the words “timeframe for making the changes” be added in requirement. VAR-002-3 • R1 – Dominion suggests requirement be revised to read “The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless the Generator Operator has been exempted from operating in the AVR voltage control mode by the Transmission Operator or has notified the Transmission Operator of one of the following: • M1- Dominion suggests measure be revised to read “Unless exempted the Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode as specified in Requirement 1” • R2 - We suggest inclusion of a footnote to indicate that GOP is expected to be able to maintain voltage schedule as long as doing so would not violate its reactive capability curve or power factor requirement (as prescribed in other reliability standards such as FAC-001-0,. MOD-025-2 and MOD-026-1 or agreements such as an interconnection agreement). • R2.1 – Dominion suggests deletion of the words “If a GOP drifts out of schedule” because inclusion of these words could give the impression that an intentional deviation nullifies this sub-requirement. We do not believe this is the intent and therefore suggest that the sub-requirement read “Each Generator Operator shall notify its associated Transmission Operator within 30 minutes when both of the following conditions are met: 1) the GOP is operating outside of the prescribed voltage or Reactive Power schedule tolerance band for 30 minutes; and 2) the GOP is no longer able to return to its voltage or Reactive Power schedule. • M2- Dominion does not agree with proposed language . GOP should be required to monitor and maintain voltage (high or low side of GSU) as specified by TOP in VAR-001-4@R4. • R3 & M3 - Dominion does not see value in the changes but do not oppose the revisions. In both VAR-001-4 and VAR-002-3 standards; GOP and TOP acrnomyns are used, Dominion suggests these acronyms be either spelled out or be updated to use GOP and TOP throughout the documents.
Yes
Dominion does not believe the additional granularity (15 minutes to determine and 15 to notify) is necessary or improves reliability. We believe the previous requirement (to inform within 30 minutes) is superior to the prosoed revision.
Dominion appreciates the IVG’s concentrated efforts to meet FERC Directives outlined in FERC Order No. 693 in suport of generator timeframes that ensure appropriate generation operation to maintain network voltage schedules. Dominion believes that the language and timeframe in VAR-002 provides for the generator to have adequate time to correct voltage drift and in the occasion where the cause of the voltage status change needs to be determined and then resolved, the timeframe of 30 minutes provides adequate time for the generator to notify the Transmission Operator.
Individual
John Canavan
NorthWestern Energy
Yes
It appears VAR-001-4, R5 is negated by VAR-002-3, R2 and R3. These standards should be coordinated with each other before they are submitted for a vote. Also we believe VAR-001-4, R2, requires additional clarification. Also, there are some overlaps within these new standards when compared to current NERC standards in place. For example FAC-014 and TOP-002. An overlap exists in establishing limits in accordance with the RC SOL methodology and the new RC SOL Methodology includes establishing limits for voltage stability and steady state voltage limits. TOP-002 states that the Transmission Operator shall perform seasonal, next day, and current day BES studies. Because of the overlaps we fear that entities could be subject to Double Jeopardy.

Individual
Scott Berry
Indiana Municipal Power Agency
Yes
Indiana Municipal Power Agency (IMPA) believes that there is some overlapping of requirements when comparing VAR-001-4 R1 to TOP-004-2 R6. IMPA recommends removing the common requirements (such as, monitorind and controlling voltage levels and real and reactive power flows-including additional requirements) from R1 of VAR-001-4. IMPA also believes that VAR-001-4 R5 can be deleted because TOP-006-2 R1 and R2 perform the same function. In addition
Group
Oklahoma Gas and Electric Co
Terri Pyle
Agree
Southwest Power Pool Standards Review Group.
Group
PPL NERC Registered Affiliates
Brent Ingebrigtson
No
No
These comments are submitted on behalf of the following PPL NERC Registered Affiliates (PPL): Louisville Gas and Electric Company and Kentucky Utilities Company; PPL Electric Utilities Corporation, PPL EnergyPlus, LLC; and PPL Generation, LLC, PPL Susquehanna, LLC and PPL Montana, LLC. The PPL NERC Registered Affiliates are registered in six regions (MRO, NPCC, RFC, SERC, SPP, and WECC) for one or more of the following NERC functions: BA, DP, GO, GOP, IA, LSE, PA, PSE, RP, TO, TOP, TP, and TSP. Comments: VAR-001: 1. The rationale statement for R1 of VAR-001 says that it, “will allow each Transmission Operator (TOP) to establish its own policies and procedures,” regarding voltage schedules and tolerance bands. This wording does nothing to prevent specifying an unreasonably-tight bandwidth (e.g. +/- 0.5%), as some parties are now doing. The PPL NERC-Registered Affiliates suggest that R1.1 end as follows, “…voltage schedules along with associated tolerance bands of not less than 1.5% of the schedule voltage unless technically justified.” There may be some resistance to making the standard prescriptive, but it’s not a burdensome requirement, and it would be unfortunate to update the standard without addressing known abuses of the present version. 2. The statement, “Each Transmission Operator shall specify a voltage or Reactive Power schedule and tolerance band (at either the high side or low side of the Generator Step-Up transformer at the TOP's discretion) at the interconnection point between the generator facility and the Transmission Owner's facilities,” in R4 of VAR-001 has a semantics glitch in that there is just one interconnect point. That is, mandating control at the interconnection eliminates any discretion in making the high vs. low-side selection. PPL suggests saying instead, “Each Transmission Operator shall specify a voltage or Reactive Power schedule and tolerance band, at the agreed upon metering point to which the GOP has access.” This will typically be either the transmission bus or the generator terminals. If the TOP specifies this as the TO’s “transmission bus”, the TO should be required to make the same voltage point used by the TOP available to the GOP to ensure both are seeing the exact same voltage. Additionally, there needs to be a feedback loop from the GOP to the TOP regarding the voltage schedule. This does not mean we want to spark a debate every time a schedule is provided, but simply add a step that allows a GOP to provide feedback regarding the feasibility of the schedule. A recommended R4.2: R4.2 The Generator Operator shall review the voltage or Reactive Power schedule and tolerance band provided by the Transmission Operator and inform the Transmission Operator of any conditions that would prevent the Generator Operator from complying with the

schedule or tolerance band, along with the technical basis for that determination. The question that then comes up is what does the TOP do if the GOP cannot comply with the schedule as presented? Recommended R4.3: R4.3 If the Generator Operator is unable to comply with the voltage or Reactive Power schedule or tolerance band as provided by the Transmission Operator, the Transmission Operator shall (a) modify the voltage schedule within the parameters established in the documented policies and procedures established in R1, taking into account the Generator Operator's limitations, or (b) exempt the Generator Operator from following the voltage schedule or tolerance band using the criteria established in R3. 3. PPL would like to see R6 of VAR-001 changed to, "After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes that is mutually agreed, and technical justification for these changes." That is, the change should normally wait until it can be rolled into a scheduled downtime event. VAR-002: 1. PPL suggests changing, "The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode as specified in Requirement 1," in M1 of VAR-002 to a more semantically neutral, "The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it did not operate a generator in the automatic voltage control mode." 2. PPL recommends the following changes to R2, for clarity; R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule3 (within each unit's ratings or capabilities4) as directed by the Transmission Operator. [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] 3. PPL suggests corresponding changes to R2.1. Note that the time frames are left blank in our recommendation, as there is still much discussion within the industry as to what an appropriate timeframe would be; If the system bus voltage drifts out of schedule, each Generator Operator shall notify its associated Transmission Operator within __ minutes when both of the following conditions are met: 1) the GOP has been operating outside of the prescribed voltage or Reactive Power schedule tolerance band5 for __ minutes; and 2) the GOP is no longer able to return to its voltage or Reactive Power schedule. Notification to the TOP is not required if the GOP can return to schedule. 4. In line with the recommended changes above, PPL suggests changing M2 to; Generator Operators shall operate the generators to help minimize excursions outside the established tolerance bands for the agreed-upon metering point. It is recognized that excursions may occur outside of the tolerance bands during unit start-up and shut-down, during MW and MVAR loading at a transmission bus where multiple units are connected, during time of relatively sudden transmission system loading changes, during system events and when grid conditions are beyond the capability of a generator to correct. Therefore, when the system bus voltage is out of the tolerance band, the Generator Operator will not be held in non-compliance with this requirement if the sub-requirements 2.1, 2.2, and 2.3 are met. In order to identify when a unit is deviating from its schedule, GOPs will monitor voltage at the agreed upon metering point to which the GOP has access. Therefore, GOPs have the option to operate on a voltage schedule on either the high-side or convert the high-side schedule to a low-side schedule at the GOP's discretion. For units that monitor on the low-side/terminal voltage, Generator Operators shall provide evidence of the method of conversion from the high-side schedule to low-side monitoring. GOP shall have evidence to show compliance with requirement R2 by providing 1) Communications with the TOP when the Generator Operator was operating outside of the prescribed voltage or Reactive Power schedule tolerance band for __ minutes AND Generator Operator was unable to return the generator to operation within its voltage or Reactive Power schedule tolerance bands; 2) Generator Operator implemented an alternative method to control reactive output when the AVR was out-of-service or unavailable; 3) compliance with directive to modify voltage or a notification that the directive could not be met. Evidence may include, but is not limited to Generator Operator logs, SCADA data, phone logs, and any other alarming notifications that would alert the Transmission Operator that both conditions were met. Timing for Requirement R2.1 can be crucial during system events, and Generator Operators are expected to begin timing when notified of an event by the TOP as soon as the unit is operating outside of the tolerance band. Further, voltage documentation during a system event may be requested by an auditor to show measures were taken to bring the unit back into schedule. 5. To harmonize Footnote 4 with our recommended language for R2, PPL suggests Footnote 4 be revised to state; For the operations horizon, the GOP may choose a test-based or real-time method of establishing a unit's reactive power capability. The test-based capability is that determined for compliance with MOD-025. Parameters typically monitored for determining real-time capability may include 1) generator loading (MW, MVAR, amps), temperatures, and terminal voltage; 2) GSU

loading and temperatures; 3) auxiliary bus voltages; 4) plant auxiliary equipment loadings, temperatures, and voltages; 5) Generator and GSU Volts/Hz limits; 6) excitation system and/or AVR limits. 6. If R2.1 sticks, PPL would like to see M2 clearly state that "if the GOP can return to schedule, it does not have to notify the TOP." 7. For the new footnote 6 referenced above; The TOP is to establish an official-for-compliance bus and phase voltage point for monitoring compliance of generators controlling to the high-side voltage. An excursion begins for compliance purposes when the measured voltage exceeds the bandwidth boundary by a recognizable amount (0.5%). Multiple notifications to the TOP need not be made when the system voltage wanders back and forth across the bandwidth boundary. The system voltage must be back within the boundary for one hour before the next excursion counts as a separate event. 8. VAR-002, R2.2 should read, "When a generator's automatic voltage regulator is out-of-service, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator, unless the TOP grants an exemption." The purpose of this change is to reference the process established in R3 of VAR-001. 9. VAR-002, R4.1 should be revised to state; "For generator step-up and auxiliary transformers with nominal primary voltages equal to the generator terminal voltage:" This is to clarify that R4 is N/A to startup transformers and other station auxiliary transformers connected to a HV bus at a plant. 10. VAR-002, R5 should read, "after consultation with the Transmission Operator and agreement on a schedule regarding necessary step-up transformer tap changes…'" for the reason stated under comment 3 above. Regarding the Technical Whitepaper; 1. The statement on p.7 that, "the more VARs produced at a generating facility, the fewer MWs produced," would be true only if operating to the generator OEM D-curve limit, and many generation units are instead typically limited by generator voltage limits due to variations in aux bus voltages. Under the latter situation raising and lower reactive power export or import does not affect the MW capability. 2. The statement on p.7 that "the informal development group did not want to place numerical requirements on what the proper operational limits should be for the continent," fails to consider that there are present-day abuses of the system that should be addressed in the VAR-001 update. Self-policing isn't working, hence our comment #1 above. 3. Ref. "unit drifts out of schedule," on p.9 it is the system that is drifting, not generation units. 4. The statement on p.10, "This industry divide is not addressed in the pro forma standard presented today," appears to account for some of the ambiguity discussed in the North American Generator Forum's comments. PPL believes that requirements need to be unambiguous, however, and there must also exist explicit and achievable means of achieving compliance. 5. While there is a sentence in the measure that states it is clearly the generator's discretion as to whether they monitor (presumably control) low side or high side to demonstrate compliance, we believe that there is still a substantial amount of language in the Standard and the Whitepaper that would tend to cloud that by implying that a generator should monitor high side for compliance if you have high side equipment installed; in other words, the monitoring/control point is based on current installed equipment. 6. Additionally, the Whitepaper does nothing to shed light on whether generators should make manual moves to reactive output (by changing the AVR low side set-point) without explicit direction form the TOP which leaves the compliance application open for interpretation.

Yes

1. In order 693 Page 488 the FERC "directive" for VAR-002 stated, "Dynegy has suggested an improvement to Reliability Standard VAR-002-1, and NERC should consider this in its Reliability Standards development process." Dynegy's concern stated, "VAR-002-1 should be modified to require more detailed and definitive requirements when defining the time frame associated with an 'incident' of noncompliance." Dynegy offered two alternatives to address their concern: "…[1] either more detail should be added to the Reliability Standard to cure this omission, Or [2] the Reliability Standard should require the transmission operator to have a technical basis for setting the time frame that takes into account system needs and any limitations of the generator." Their reasoning: "… this approach will eliminate the potential for undue discrimination and the imposition of overly conservative or excessively wide time frame requirements, both of which could be detrimental to grid reliability." Note that voltage tolerance band is not mentioned. 2. Going from NERC "should consider" Dynegy's suggested improvements to a very prescriptive time requirement (embedded in a VSL) in the current version of VAR-002 was a big step from the generation perspective. Also, it appears that Dynegy's second alternative was ignored during this step. 3. In the 2013 FERC Order approving VAR-002-2b (current version which became effective on July 1, 2013): PPL presented valid arguments against the "zero tolerance" time frame deviation introduced in the VSLs from the generator operator perspective (see Paragraphs 15 and 16). Both NERC and FERC rejected PPL's arguments. Paragraph

17 states, “NERC argues that the proposed modification would allow for a deviation in system voltage for up to 30 minutes to allow for time to correct an excursion and that such deviations from a voltage and reactive schedule is inappropriate because a deviation even up to a few minutes can negatively impact reliability.” Paragraph 18 goes on to say, “NERC maintains that significant voltage deviations for extended periods of time may lead to voltage collapse and can increase the potential for a wide-area impact to the reliability of the Bulk-Power System, and as such PPL Companies’ proposed modification to the VSL language should be rejected.” The context of the NERC and FERC discussions and agreement on the rigid time requirement apparently assumes all TOP’s voltage schedule tolerance bands are reasonable and “reliability based”. Also, there seems to be an absence of discussion on Dynegy’s 2nd alternative for the “the transmission operator to have a technical basis for setting the time frame that takes into account system needs and any limitations of the generator.” However, the Pro Forma VAR R1 will require each TOP to have documented policies or procedures used to “establish, monitor, and controls voltage levels and Reactive Power flows within limits as defined below: R1.1 These documented policies or procedures shall include criteria used in system assessments. The criteria for the assessments shall include established steady-state limits, voltage stability limits and associated operating margins, and voltage schedules along with associated tolerance bands.” Thus, a fair question on the Pro Forma standards follows: If VAR-001 R1.1 is met; can GOPs conclude that each TOP’s tolerance bands have a documented technical basis? If not, what mechanism will allow GOPs to question extremely narrow voltage or reactive power schedule tolerance bands that make compliance with VAR-002 R2.1 difficult or impossible? Note the Background discussions in the White Paper (see Pages 7 – 10). The discussion for VAR-001 R4 states, “The informal development group is cognizant of the fact that the nature of reactive power on the network varies depending on local conditions. Thus, the group focused on the process that the requirements would detail, not the proper numbers a TOP should enforce in the standard. For VAR-001, the group would not put operational limits on how a TOP should manage voltage stability for its regions; more specifically, the informal development group did not want to place numerical requirements on what the proper operational limits should be for the continent. Operating margins vary due to specific system characteristics as well as the operating conditions.” This begs the question: Why was this same rationale not applied in addressing the time frame? 4. The published reasons for the changes to VAR-002 include 1) eliminating nuisance calls and mitigating compliance issues for generators (i.e. non-reliability gap reducing violations), and 2) addressing the FERC directive to NERC to "consider a timeframe" for allowing a generator to be out of schedule before having to make a notification to its TOP. It could be argued that imposition of a very prescriptive time frame alone does not fully address the FERC “directive” language and the first Pro Forma objective of reducing nuisance calls (GOP to TOP), especially if the voltage tolerance bands are extremely tight or do not have a technical basis.
See responses to question 2 above.
Individual
Anthony Jablonski
ReliabilityFirst
Yes
ReliabilityFirst has a fundamental overarching concern with the two proposed standards and believe the two standards in their draft state have major flaws. The two drafts are completely dependent on each other and when implemented individually do not make sense and actually conflict with each other. This interdependency on each other may cause serious issues and potential issues within compliance space and overall reliability. For example, Requirement R5 in VAR-001-4 requires the Transmission Operator to know the status of all transmission Reactive Power resources, automatic voltage regulators, and power system stabilizers in their system. If the Generator never supplies the status, there is a potential for a potential violation on the Transmission Operator. Another example includes Requirement R3 in VAR-001-4. If the Transmission Operator fails notify the Generator Operator that they are exempted, there is a potential for non-compliance for the Generator Operator not complying with R2 in VAR-002-3. ReliabilityFirst believes the linkage between the two standards is crucial and recommends combining the two standards to address the contradictory aspects of the two standards.
Yes

ReliabilityFirst provides the following comments related to the requirements and VSLs for the draft VAR-001-4 standard: 1. Requirement R1, Part 1.1 - ReliabilityFirst seeks further clarity on what is meant by the term “system assessments” in Requirement R1, Part 1.1. Are these “system assessments” meant to be performed in the near-term or long-term time period and what do encompass? 2. Requirement R1, Part 1.2 and Part 1.2 - There is no periodicity for when the documented policies need to be provided to the relevant entities. There is also no stipulation on whether changes to these polices need to be provided as well. ReliabilityFirst offers the following for consideration for Part 1.2: “Each Transmission Operator shall provide a copy of these documented policies or procedures to adjacent Transmission Operators [within 30 calendar days of request and within 30 calendar days of any changes]”. 3. Requirement R2 - ReliabilityFirst seeks further clarity on what is meant by the term “assessments” in Requirement R2. Are these “assessments” meant to be performed in the near-term or long-term time period and what do encompass? 4. Requirement R2, Part 2.1 and Part 2.2 - The Reliability Coordinator is an applicable entity for the parent Requirement R2 but is not listed within Part 2.1 or Part 2.2. ReliabilityFirst believes the Reliability Coordinator is relevant to both of the sub-parts and should be referenced in both sub-parts. For Part 2.1, the Reliability Coordinator can “…direct the real-time operation of devices…” and for Part 2.2, the Reliability Coordinator can help in ensuring “…that sufficient reactive resources have been scheduled…” ReliabilityFirst recommends referencing the Reliability Coordinator within Part 2.1 and Part 2.2. 5. Time Horizons Q2 - The Time Horizons within a number of the requirements (e.g., “Operations”) do not align with the five NERC defined Time Horizons (i.e., Long-term Planning, Operations Planning, Same-day Operations, Real-time Operations and Operations Assessment). ReliabilityFirst suggests the SDT review the NERC defined Time Horizons and modify the Time Horizons for all the requirements accordingly. The NERC defined Time Horizons are located at: http://www.nerc.com/pa/Stand/Resources/Documents/TimeHorizons.pdf. 6. VSL Requirement R1 - The High VSL should reference “sub-parts” rather than “sub-requirements.” NERC standards no longer include sub-requirements. 7. VSL Requirement R2 - The VSL is inconsistent with the language for Requirement R2. Based on the FERC VSL Guideline 3: “Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement.” The VSLs are missing reference to the Reliability Coordinator which is an applicable entity for Requirement R2. ReliabilityFirst recommends adding the Reliability Coordinator to the VSLs associated with Requirement R2. 8. VSL Requirement R3 - ReliabilityFirst believes there should be an associated VSL referencing sub-part 3.1. ReliabilityFirst recommends the following for consideration: "High VSL – “The TOP failed to notify the associated Generator Operator, In the event a Transmission Operator approves a generator as satisfying the exemption criteria.” 9. VSL Requirement R4 - ReliabilityFirst believes the word “some” in the high VSL is ambiguous and troublesome and ambiguous. ReliabilityFirst recommends the following for consideration: i. High VSL – The Transmission Operator specified a voltage or Reactive Power schedule and tolerance band but failed to provide the voltage or Reactive Power schedule and tolerance band to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode.” ii. Severe VSL – “The Transmission Operator failed to specify a voltage or Reactive Power schedule and tolerance band.” 10. VSL Requirement R5 - All Requirements are required to have a Severe VSL designation. Violation Severity Levels (VSLs) define the degree to which compliance with a requirement was not achieved. In cases where an entity completely failed to meet the intent of the requirement, it falls within the Severe category regardless of the risk to reliability (risk is dealt within the Violation Risk Factors). ReliabilityFirst recommends the following for consideration: i. Severe VSL – “The Transmission Operator failed to know the status of all transmission Reactive Power resources, automatic voltage regulators, and power system stabilizers in their system. 11. VSL Requirement R6 - All Requirements are required to have Severe VSL designation. Violation Severity Levels (VSLs) define the degree to which compliance with a requirement was not achieved. In cases where an entity completely failed to meet the intent of the requirement, it falls within the Severe category regardless of the risk to reliability (risk is dealt within the Violation Risk Factors). ReliabilityFirst recommends the following for consideration: i. High VSL – “The Transmission Operator failed to provide documentation to the Generator Owner specifying either the required tap changes, a timeframe for making the changes, or technical justification for these changes.” ii. Severe VSL – “The Transmission Operator failed to provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.” ReliabilityFirst provides the following comments related to the requirements and VSLs for the draft VAR-002-3 standard: 1. Requirement R2, Part 2.2 - For consistency, spell out Generator Operator rather than listing the acronym “GOP.” 2. Requirement R5 -

The parent Requirement R5 is applicable to the Generator Owner while the sub-part 5.1 specifies the Generator Owner. The same applicable entity listed in the “parent” requirement should be the same as any associated sub-parts. This inconsistency needs to be remedied. 3. VSL Requirement R2 - The VSL is inconsistent with the language for Requirement R2. Based on the FERC VSL Guideline 3: “Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement.” ReliabilityFirst recommends the following for consideration: i. Severe VSL – “The Responsible entity failed to maintain the generator voltage or Reactive Power schedule as directed by the Transmission Operator in accordance with Requirement R2, parts 2.1, 2.2 and 2.3 “ 4. VSL Requirement R3 - The VSL is inconsistent with the language for Requirement R3. Based on the FERC VSL Guideline 3: “Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement.” ReliabilityFirst recommends the following for consideration: i. Severe VSL – “The Responsible entity failed to notify its associated Transmission Operator of a status or capability change on any generator Reactive Power resource within 30 minutes of the change.” 5. VSL Requirement R4 - The VSLs for Requirement R4 are completely inconsistent with the associated Requirement R4. Requirement R4 speaks to the Generator Owner providing data to the Transmission Operator while the VSL speaks to the failure of maintaining the generator voltage or reactive power schedule. ReliabilityFirst recommends reviewing Requirement R4 and developing VSLs consistent with the requirement. 6. VSL Requirement R5 - Requirement R5 is applicable to the Generator Owner while the associated VSL refers to the Generator Operator. This inconsistency needs to be remedied.
Individual
Scott Helyer
Tenaska, Inc.
No
Yes
We appreciate the language giving GOPs the option to monitor voltage on the low-side of the step-up transformers. This is a positive step, but work is still needed on the proposed standards. One concern is that VAR-001-4 allows the TOP to set voltage/reactive power schedules with tolerance bands. However, setting a tolerance band that is too narrow will require GOPs to frequently call TOPs as required in VAR-002-3 anytime the system causes the generator to move outside the tolerance band. The drafting team should consider whether a minimum tolerance band should be included in the standard that is enough to maintain a reliability voltage, but is large enough to minimize the potential for constant communications between GOPs and TOPs. Another concern is that VAR-002-3 R2 should specifically state that a GOP shall be allowed to convert a high-side schedule and control voltage on the low-side of the step-up transformer. Otherwise, R2 and M2 do not match as M2 is the only place where this language is provided. Further, VAR-002-3 requires the GOP to inform the TOP if the voltage drifts outside the tolerance bands set by the TOP. The problem is that GOPs may frequently find themselves outside the tolerance bands as the system voltage drifts if the TOP does not set appropriate tolerance bands.
No
Group
SERC EC Generation Subcommittee
David Thompson
Yes
There is a general concern with this proposed standard that it will create further administrative burden for the GOP, TOP, and RC, as well as the back office staff. Additionally, the high probability exists that the number of calls between the GOP and TOP will increase without materially enhancing BES reliability.

Yes
VAR-002-3 Comments: R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless Delete: "the Generator Operator has notified the Transmission Operator of one of the following:" a generator has been has been exempted from operating in the AVR voltage control mode by the Transmission Operator or the Generator Operator has notified the Transmission Operator of one of the following: M1. Add words “Unless exempted” the Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it Add words: “did not” operate a generator in the automatic voltage control mode. R2. Add "Unless exempted" by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule (within Replace: “applicable Facility Ratings” with Add words: “each unit’s ratings or capabilities4”) (NOTE: Footnote 4 should be associated with R2.2, not R2.1.) as directed by the Transmission Operator. [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] 2.1. When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met. [Delete Pro Forma 2.1 and replace it with Pro Forma 2.3. See our comments below and in our response to Question 3.] 2.2. When a generator’s automatic voltage regulator is out-of-service, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator Add words: “unless the TOP grants an exemption.” Comments: We feel that approach and language in VAR-002-2.b R2.2 should be retained. This approach reflects closer alignment with VAR-001-4 and current language in the Functional Model for Generator Operator expectations and current plant design features. The GS recommends NERC vet the White Paper for this standard through formal industry review, get stakeholder input and consensus as required per the Standards Process Manual, section 11. It appears that this standard has been written with the assumption that generators can monitor and directly control transmission bus voltage (only some monitor it and almost none directly control it). With the elimination of (the 18 Jul 2013 proposed) R2.1 this measure (M2) should be rewritten. The revised M2 should not include additional requirements. Comments: The M2 information should be considered during the revision of the White Paper. R3. Each Generator Operator shall notify its associated Transmission Operator of a status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability within 30 minutes of the change. If the status has been restored within the first 15 minutes of such change, then there is no need to call the TOP. [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] Comments: The GS suggests clarifying the term “capability change” in the White Paper revision. There is considerable confusion about the time requirement and it is not clear that these are applicable to the AVR status question or the capability change question. It may make sense to separate these two requirements to allow better clarification. M3. The Generator Operator shall have evidence it notified its associated Transmission Operator Replace: “within 30 minutes of any of the changes identified” with Add words: “as required” in Requirement 3. If the status has been restored within the first 15 minutes, no call is necessary. R4. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. [Violation Risk Factor: Lower] [Time Horizon: Real-time Operations] 4.1. For generator step-up transformers and auxiliary transformers with Add words: “nominal” primary voltages equal to (Delete words “or greater than” the generator terminal voltage: Comments: (This is to clarify that R4 is N/A to startup transformers and other station auxiliary transformers connected to a HV bus at a plant.) R5. After consultation with the Transmission Operator Add words: “and agreement on schedule” regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. [Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]. Regarding the Technical Whitepaper; 1. The statement on p.7 that, “the more VARs produced at a generating facility, the fewer MWs produced,” would be true only if operating to the generator OEM D-curve limit, and many generation units are instead typically limited by generator voltage limits due to variations in aux bus voltages. Under the latter situation raising and lower reactive power export or import does not affect the MW capability. The NATF Model Practices Group has recognized that improvements in the way units are modeled for reactive power capability that respects other plant operating limitations, such as aux system voltage limits need to be investigated and have a project to review this issue. 2. The

statement on p.7 that “the informal development group did not want to place numerical requirements on what the proper operational limits should be for the continent,” fails to consider that there are present-day abuses of the system that should be addressed in the VAR-001 update. Numerical tolerance bands should be based on clear system reliability criteria and not some arbitrary tolerance band. For example, maximum voltage limits should be based on equipment ratings at that point in the system. 3. Ref. “unit drifts out of schedule,” on p.9 it is the system that is drifting, not generation units. 4. The statement on p.10, “This industry divide is not addressed in the pro forma standard presented today,”. The SDT is encouraged to follow through on AVR paragraph under the VAR-002 section by pursuing full industry review of the White Paper as required by the Standards Process Manual, section 11. 5. While there is a sentence in the measure that states it is clearly the generator’s discretion as to whether they monitor (presumably control) low side or high side to demonstrate compliance, we believe that there is still a substantial amount of language in the Standard and the Whitepaper that would tend to cloud that by implying that a generator should monitor high side for compliance if you have high side equipment installed; in other words, the monitoring/control point is based on current installed equipment. 6. Additionally, the Whitepaper does nothing to shed light on whether generators should make manual moves to reactive output (by changing the AVR low side set-point) without explicit direction from the TOP which leaves the compliance application open for interpretation.
Yes
Comments: See question 2 comments above. VAR-001-3 allows the TOP to determine the appropriate voltage schedules and tolerances for that TOP’s area for the reasons stated in the White Paper under the VAR-001 section. Why does VAR-002 not allow the TOP to determine the corresponding time requirement? We believe that the prescriptive time requirement in VAR-002 may cause conflicts with R4 of VAR-001 such that system requirements and different control areas may require different notification and therefore will be problematic for system and plant operators. The TOPs are familiar with their systems and will issue voltage tolerance bands based on their system needs. Therefore, it is appropriate for the TOPs to establish the associated time frame for their tolerance bands based on their system needs. That is, the time frame should be linked to the tolerance band. If the voltage tolerance is reliability based the TOP with the RC should be able to establish a corresponding time tolerance for deviations from the scheduled voltage. No reliability gaps should exist if both voltage tolerance band and corresponding time frame are reliability based rather than arbitrarily established. It is imperative that the TOPs provide realistic voltage tolerances and time frames that are 1) practical for both system operators and generator operators who have many duties related to system and plant reliability and safety, and 2) will not result in administrative burdens due to unnecessary notification and possible violations for deviations in voltage schedule that do not pose a BES reliability concern. Further, it appears that this standard has been written with the assumption that generators can monitor and directly control transmission bus voltage. Generation design standards have been that plant voltage regulators regulate the generator bus and having operators being able to see grid voltage has not been a standard. The responsibility for monitoring transmission class voltage has been a transmission operations function and taking action to makes changes requires a wider system view that the generation plants will ever have. This is what is reflected in version 5 of the Functional Model, which states that the GOPs in Real Time 10. Provides Real-time operating information to the Transmission Operators and the required Balancing Authority. 11. Adjusts real and reactive power as directed by the Balancing Authority and Transmission Operators.
The SDT is encouraged to follow through on AVR paragraph under VAR-002 by pursuing full industry review of the White Paper as required by the Standards Process Manual, section 11. The comments expressed herein represent a consensus of the views of the above named members of the SERC Generation Subcommittee (GS)only and should not be construed as the position of the SERC Reliability Corporation, or its board or its officers.
Group
Florida Municipal Power Agency
Frank Gaffney
No
Yes

FMPA appreciates the efforts of the ad hoc team; but, the ad hoc team missed many opportunities to reduce duplication of the VAR standards with other standards (e.g., TOP standards, FAC-011, FAC-014). Consequently, FMPA is recommending a Negative vote. VAR-001-4, R1 is Duplicative of FAC-011 and the TOP-004 Standards This requirement as drafted is duplicative of existing TOP-004-2: "R6. Transmission Operators, individually and jointly with other Transmission Operators, shall develop, maintain, and implement formal policies and procedures to provide for transmission reliability. These policies and procedures shall address the execution and coordination of activities that impact inter- and intra-Regional reliability, including: R6.1. Monitoring and controlling voltage levels and real and reactive power flows. R6.2. Switching transmission elements. R6.3. Planned outages of transmission elements. R6.4. Responding to IROL and SOL violations." The Project 2007-03 SDT that revised the TOP standards found this requirement administrative in nature and eliminated the need for policies and procedures, mapping much of this requirement to the Purpose statement of the new TOP-001-2 Standard. VAR-001-4 should at least remain consistent with Project 2007-03 SDT's intent and eliminate policies and procedures as administrative in nature. R1 as drafted is also duplicative of FAC-011, System Operating Limit Methodology in the Operating Horizon: Proposed VAR-001-4, R1, 1.1: "These documented policies or procedures shall include criteria used in system assessments. The criteria for the assessments shall include established steady-state limits, voltage stability limits and associated operating margins, and voltage schedules along with associated tolerance bands." (emphases added) Existing FAC-011-2: "R2. The Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following: R2.1. In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits … R3. The Reliability Coordinator's methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins …" (emphases added) Hence, R1 as drafted essentially requires developing and implementing policies and procedures to: a) Operate within SOLs. b) Operate to voltage schedules The only unique part of R1 that is different than FAC-011 is "voltage schedules along with associated tolerance bands". Therefore, R1 should be boiled down to just the TOP or RC establishing, and the TOP operating to "voltage schedules along with associated tolerances bands" to eliminate duplication with other standards. In addition, FMPA questions whether the RC should establish these voltage schedules instead of the TOP. If neighboring TOPs establish different, uncoordinated voltage schedules, then at the boundaries between TOPs, voltage schedules may be difficult to maintain and there will be significant VAR flow between the TOPs with significant associated losses. Coordinated voltage schedules between TOPS should be required. This can be accomplished in two ways: 1) the RC develops the voltages schedules; or 2) the word "jointly" is reintroduced to R1 (the ad hoc team chose to eliminate the word "jointly" from the existing requirement) so that neighboring TOPs "jointly" develop a coordinated voltage schedule. VAR-001-4, R2 is Duplicative of TOP-002 and TOP-001 and should be Eliminated VAR-001-4, R2 requires the TOP to perform assessments (which is duplicative of TOP-002-3, R2 to develop a plan to operate) to ensure sufficient reactive reserves to maintain voltage stability. Voltage stability is a determinant of SOLs; hence, the standards already require TOPs to develop and to operate within SOLs, including SOLs determined by voltage stability limits (FAC-011, FAC-014, TOP-001-2 R7 through R11, TOP-004-2, TOP-007-0). VAR-001-4 also requires TOPs to direct action if needed; for which they already have responsibility under TOP-001. Hence, R2 as drafted is entirely duplicative of other requirements and should be eliminated. VAR-001-4, R5 is Duplicative of TOP Standards and should be Eliminated TOP-006-2 states: "R1. Each Transmission Operator and Balancing Authority shall know the status of all generation and transmission resources available for use .... R2. Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall monitor applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, and status of rotating and static reactive resources." So, contrary to the ad hoc team's assertion, R5, which requires the TOP to know the status of all reactive power resources, AVRs and PSSs on their system, is duplicative of TOP-006-2, R1 and R2 which do include Power System Stabilizers and voltage regulators (e.g., "status of rotating … reactive resources"). The Project 2007-03 SDT mapped this to the TOP-003-2 standard, R1, which states: "Each Transmission Operator shall create a documented specification for the data necessary for it to perform its Operational Planning Analyses and Real-time monitoring." Hence, if the ad hoc team disagrees with the action of the Project 2007-03 SDT in generalizing the requirement to a generalized data request as opposed to the specificity of exactly what "data (is) necessary for it to perform its … Real-time monitoring" the ad hoc team seems to desire, then, the newly formed SDT for this VAR project should instead modify TOP-

003-2 to incorporate that specificity and not include this requirement in VAR-001-4. VAR-002-3, R2, 2.3 is Duplicative of TOP-001 and should be Eliminated The requirement is essentially for GOPs to follow a directive of the TOP; which is duplicative of TOP-001-2, R1 which states: “Each Balancing Authority, Generator Operator, Distribution Provider, and Load-Serving Entity shall comply with each Reliability Directive issued and identified as such by its Transmission Operator(s), unless such action would violate safety, equipment, regulatory, or statutory requirements.” Hence, VAR-002-3, R2, 2.3 should be eliminated. If “directed” as used in the draft VAR-002-3, 2.3 is not intended to be from a Reliability Directive, then, clarification is required as to what “directed” means. VAR-002-3, R3 is Duplicative of TOP-003 and should be Eliminated VAR-002-3, R3 as drafted requires GOPs to inform the TOP of changes in status or capability from a reactive power perspective. This is very similar in nature to the GOPs’ obligation to inform the TOP of the same from a real power perspective in TOP-002-2, R14. The Project 2007-03 SDT mapped this to TOP-003-2, R5 which states: “Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Interchange Authority, Load-Serving Entity, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall satisfy the obligations of the documented specifications for data.” It is expected that the TOP will require such data in TOP-003-2, R1, and the GOPs will need to respond in accordance with TOP-003-2, R5. If the ad hoc team disagrees with the action of the Project 2007-03 SDT in generalizing the requirement as opposed to the specificity of exactly what “data (is) necessary for it to perform its … Real-time monitoring” the ad hoc team seems to desire, then, the newly formed SDT for this VAR project should instead modify TOP-003-2 to incorporate that specificity and not include this requirement in VAR-002-3.
Individual
Kathleen Goodman
ISO New England, Inc.
Agree
IRC SRC
Individual
Nazra Gladu
Manitoba Hydro
No
Yes
(1) Manitoba Hydro believes that Power System Stabilizer (PSS) should not be included in the standard (R3) because they are not designed for, nor could they be operated in any way to maintain and/or control Network voltage (schedules). In particular: (a) PSS deals with power swings (oscillations) by adjusting the generator voltages through AVRs to add damping to the generator rotor oscillations. The outcome of this process is to provide more stable real power transfer. (b) PSS does NOT control the generator or network voltages, but instead affects them in a uncontrollable way. Moreover, PSS does not contribute to the voltage stability. (c) If PSS must be included in the scope of this standard, then Manitoba Hydro believes that other functions in the AVR such as overexcitation limit (OEL), under excitation limit (UEL) and voltage per hertz limit should be included as well since they all at some point will affect the generator voltages during periods of “normal” operation. (d) It is our experience that PSSs are sometimes out of service as a result of automatically shutting off based on design and operational criteria which may include below certain gate positions or loading levels. In modern designs, the PSSs are normally part of the excitation control system and there is no physical turn-on/off switch (even though our utility has always asked for switches for easy operation). Manitoba hydro believes that there is a lack of clarity in the standard as it pertaines to the need to/process of reporting this status, i.e. the function of PSS is automatically switched off/on (out-of or back-in-service) during normal operation. Manitoba Hydro believes that if a requirement of the PSS is to remain in the standard, then a formal interpretation on this situation is warented. (2) Please clarify that when Automatic Voltage Regulators (AVR’s) or Power System Stabilizers (PSS) come out of service, the appropriate Reliability Coordinator, Transmission Operator and neighbors are to be

notified should they be impacted. Moreover, this must be documented and posted for other Transmission Operators and RC's to view.
No
(1) Effective Dates, VAR-001-4 and VAR-002-3 - replace the words " Board of Trustees approval " with " Board of Trustees' approval " for consistency with other standards. (2) General Comment - replace " Board of Trustees " with " Board of Trustees' " throughout the applicable documents/standards for consistency with other standards.
Individual
Karen Webb
City of Tallahassee - Electric Utility
No
Yes
The standards already require coordination. If the TOP is not being provided enough "cooperation" from the GOPs in their footprint, then there is a need for stronger internal documents to achieve the necessary level of cooperation. While the standard states they must coordinate, it does not provide to what extent. One solution may be to compensate VAR output as well as MW output for the GOPs. As it pertains to VAR-002-3, the last sentence of R3, should state "…..no need to NOTIFY the TOP", in lieu of "call the TOP." This consistency would be appreciated.
No
The standards already require coordination. If the TOP is not being provided enough "cooperation" from the GOPs in their footprint, then there is a need for stronger internal documents to achieve the necessary level of cooperation. While the standard states they must coordinate, it does not provide to what extent. One solution may be to compensate VAR output as well as MW output for the GOPs.
Individual
Scott Langston
City of Tallahassee
No
No
No
The standards already require coordination. If the TOP is not being provided enough, "cooperation" from the GOPs in their footprint, then there is a need for stronger internal documents to achieve the necessary level of cooperation. While the standard states they must coordinate, it does not provide to what extent. One solution may be to compensate VAR output as well as MW output for the GOPs. As it pertains to VAR-002-3, the last sentence of R3, should state "…..no need to NOTIFY the TOP", in lieu of "call the TOP." This consistency would be appreciated.
Individual
Bill Fowler
City of Tallahassee
No
No

No
The standards already require coordination. If the TOP is not being provided enough, “cooperation” from the GOPs in their footprint, then there is a need for stronger internal documents to achieve the necessary level of cooperation. While the standard states they must coordinate, it does not provide to what extent. One solution may be to compensate VAR output as well as MW output for the GOPs. As it pertains to VAR-002-3, the last sentence of R3, should state “…..no need to NOTIFY the TOP”, in lieu of “call the TOP.” This consistency would be appreciated.
Group
Duke Energy
Michael Lowman
No
Yes
Duke Energy suggests the SDT consider using the NERC defined terms of Operating Plan, Operating Process or Operating Procedure instead of “policies or procedures” in Requirement 1 to provide clarity and consistency. R1.2 and R1.3 should be revised and consolidated to read, “ Upon request, the TOP shall provide a copy of these documented Operating Plans, Operating Processes, or Operating Procedures to adjacent Transmission Operators and its Reliability Coordinator. “ Duke Energy recommends the SDT determine the correct NERC defined Time Horizon necessary for all requirements in VAR-001-4 as “Operations” is not considered a valid NERC defined time horizon. Measure 1 would have to be modified if “Upon request” is accepted by the SDT. Duke Energy suggests the following for Requirement 2 1. R2 should be changed to, “Each Transmission Operator and Reliability Coordinator shall perform assessments on their respective areas in order to ensure sufficient reactive resources are available for scheduling to maintain voltage stability under normal and contingency conditions in order to provide the voltage levels as defined in Requirement R1. 2. R2.2 should be changed to, “As a result of the assessments, each Transmission Operator shall ensure that sufficient reactive resources have been scheduled are available to meet acceptable day-ahead voltage limits identified in Requirement R1. Sufficient reactive resources may include, but is not limited to reactive generation scheduling; transmission line and reactive resource switching; and controllable load. Duke Energy seeks clarification on the term “real-time event” used in M2. What was the criterion considered to constitute a “real-time event”? The concern is that an auditor could consider a 1kV voltage deviation a “real-time event”. This type of voltage deviation has no impact to the reliability of the BES. The SDT should consider using alternative language that is more specific. Duke Energy suggests alternative language for VAR-001-04 R4.1 and VAR-002-3 R.1. Per the NERC Compliance Analysis Report of the VAR-002, it is stated that there are three widely-used AVR modes for generators: AVR- automatic controlling voltage mode, AVR-VAR mode, and AVR-power factor mode. Duke Energy is aware of a number of generating facilities that are not equipped with an automatic voltage regulator, thus the pro-forma standard should be revised to include other known AVR modes. Duke Energy suggests the following language: VAR-001-4 R4.1 should read: 4.1. The Transmission Operator shall provide the voltage or Reactive Power schedule and tolerance band to the associated Generator Operator and direct the Generator Operator to comply with the schedule in one of three AVR modes (AVR-automatic controlling voltage mode, AVR-power factor control mode, or AVR-VAR control mode) as determined to be appropriate by the TOP. R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in one of three AVR control modes specified by the Transmission Operator (AVR-automatic controlling voltage mode, AVR-power factor control mode, or AVR-VAR control mode)unless the Generator Operator has notified the Transmission Operator of one of the following: [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] • That the generator is being operated in start-up1 or shutdown2 • That the generator is not being operated in the TOP-directed AVR control mode for a reason other than start-up or shutdown. In VAR-002-3 R4, Duke Energy suggests removing auxiliary transformers from the standard. Auxiliary transformers are not used to control MVars for reliability purposes. In VAR-002-3 R5, Duke Energy suggests inserting the phrase “mutual assent” into the language of R5. The standard language should read as follows: R5. “After consultation and mutual assent with the Transmission Operator regarding necessary step-up transformer tap changes, …”

Yes
Duke Energy suggests extending the timeframe a GOP must notify its TOP of schedule drift to 30 minutes to allow time for recognition of the problem, assessing corrective action needed, and contacting the TOP when required. Regarding VAR-002-3 R2.1, the start time that a generator “drifts out of schedule” (i.e. is considered to have drifted out of schedule), is dependent upon the method used for monitoring the voltage. Does the clock start based upon the first scan that the generator is outside the voltage schedule, and stop upon the first scan that the generator is back within the voltage schedule? If not, how long of a period must a generator be back within schedule to reset the clock? Can the Transmission Operator define the criteria for measurement when the voltage schedules are provided? For example, can the TOP indicate that a generator is considered outside its voltage schedule when the clock-minute average voltage is outside the schedule? No matter of the data used for measuring voltage against the voltage schedule (scan-rate, clock-minute, rolling ten-minute average), is a generator considered back within its voltage schedule (clock stops) based on the same measurement to contact the TOP? Duke Energy suggests clarifying the term “capability change” in the White Paper revision. There is considerable confusion about the time requirement and it is not clear that these are applicable to the AVR status question or the capability change question. It may make sense to separate these two requirements to allow better clarification. Duke Energy suggest adding the words “or maintain any documentation” after TOP in the R3 sentence. The rewording should read as follows: “If the status has been restored within the first 15 minutes of such change, then there is no need to call the TOP or maintain any documentation” Duke Energy suggests rewording Measure 3 as follows: “The Generator Operator shall have evidence it notified its associated Transmission Operator as required in Requirement 3. If the status has been restored within the first 15 minutes, no call is necessary.”
Individual
John Bee
Exelon and its' affiliates
Yes
As NERC representatives pointed out in recent webinars, one goal of many of the existing standard development projects is to seek a steady state for applicable standards. In order to avoid iterative development projects, the SARs should accommodate all known issues and/or recommendations. The recently issued Independent Experts Review Project cites some requirements within VAR-001 and VAR-002 for attention. The scope of the SAR should include assessment and resolution of the Independent Expert Review Report recommendations. Additionally, to the extent related, the recently submitted risk assessment by the RISC should be considered when developing the scope of SARs. Question 4 below requests input on specific issues acknowledged are not currently included in this project. More detail is below, but Exelon supports addressing all known issues, not just the FERC directives, at this time. In addition, Exelon supports the concept of developing Compliance Guidance concurrently with the Standard development because it makes sense to develop audit explanations and tools while the intent and information is fresh and under development. In addition, this is very useful for Registered Entities to understand how compliance will be judged. However, it is not clear how development of Compliance Input is to be conducted. The Compliance Input should evolve as the Standard language evolves through the standards development process and must ultimately reflect the actual language in the final, approved standard. Understanding that no ballot is associated with Compliance Input, it would be very useful for NERC to post Compliance Input with a separate comment form for stakeholder input. Some of the project SARs cite development of an RSAW. Stakeholder Review and comment on RSAWs and Compliance Input prior to the final ballot of a proposed standard will be mutually beneficial.
Yes
The VAR white paper discusses VAR-002 Requirement R2 and provides a discussion on notifications regarding adherence to a voltage schedule. Specifically, this paper mentions instances where the unit may not be able to return to schedule when it has encountered an operating limit, or when a system event is pulling the unit out of schedule; however, this project does not address issues where the TOP (as may be delegated to the TO) provides an unrealistic voltage schedule that is difficult if at all possible to maintain by the Generator Operator. The white paper evaluates the need for the TOP and

GOP to agree to a voltage schedule but dismisses that concept as it could create “disputes between the parties as to what the appropriate voltage schedule should be for a unit”. In our opinion, VAR-002 should provide a vehicle for a GOP to challenge what they may perceive as an unrealistic schedule if that schedule is unmanageable or challenges the physical operating capability of the generating unit. Exelon suggests that a formal notification to the TOP/TO with a technical justification be required to ensure that this challenge not be abused by the GOP. We believe it is reasonable to allow the generator to monitor the high side or the low side of the generator step up transformer; however, the TOP should align their voltage schedule to match the GOP chosen monitoring equipment or agree on the conversion factor. There is not a one for one conversion between grid voltage and terminal voltage and both parties should agree on the conversion to avoid any future audit or implementation issues. Further to the the specific language in proposed VAR-002, R2, the statements do not seem to track with the stated intent. It appears that a GOP is to notify a TOP within 15 minutes concurrently with being out of the schedule for 15 minutes. Should the language read: “…each Generator Operator shall notify its associated Transmission Operator within 30 minutes when both of the following conditions are met: …” VAR-002, R2.3. When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met. Suggest that “the schedule” be replaced with “the modified Voltage Level” since a request to move Voltage is not really a new “schedule” it is just a temporary change. The Implementation Plan for VAR-001-4 and VAR-002-3 requires the new Standard revisions to be implemented the first day of the first calendar quarter after applicable regulatory approval. This is not sufficient time to allow generating units to implement training of operators and procedural changes necessary to implement the proposed changes to notification requirements. Suggest at least a 6 month implementation period following regulatory approval. Note that as written in the proposed implementation plan, the “first calendar quarter following approval” does not guarantee even the cited timeframe of 3 months (i.e. if approved in March 2014, it becomes effective April 1, 2014). To accommodate a six month implementation period the language must mark time in months. For example the language should read: “this standard shall become effective on the first day of the seventh month after applicable regulatory approval…” The current draft does not have any tolerance at all and starts a time requirement regardless of the deviation from the voltage band. Why is this Standard requiring a time requirement for notification to the TOP when each voltage schedule, tolerance, and voltage band is different for each generator based on size, location, impact to the system and the TOPs preference for operating its system?. The voltage schedule, tolerance band, and notification requirements should be left to the discretion of the TOP. The revised Standard VSL should include a percentage value associated with an excursion outside of the voltage schedule. If the Standard moves forward without any evaluation of the magnitude of deviation from the voltage schedule, then there should be some consideration of this in the associated VSLs. Finally Exelon suggests that the Compliance Section 1.2 Evidence Retention for VAR-002-3 should read the same as for VAR-001-4.

Yes

If the operator takes the time to trouble shoot, make repairs or makes attempts to get the AVR or If the operator takes the time to trouble shoot, make repairs or makes attempts to get the AVR or PSS back to automatic, the operator limits the time available to notify the TOP that the AVR or PSS is not in auto. Exelon recommends that the time for notification be increased to allow for the operator to trouble shoot and make a determination that the AVR/PSS cannot be put back in auto. Additionally, Exelon would like the standard to specify that AVR/PSS status indication, if installed, via SCADA will satify the notification requirement.

As stated above, this project does not address issues where the TOP (as may be delegated to the TO) provides an unrealistic voltage schedule that is difficult if at all possible to maintain by the Generator Operator. Throughout the white paper and this comment form there is the common theme of addressing a “reliability gap”. In the cases of generator who are given an almost impossible job of attempting to adhere to an unrealistic voltage schedule, there is frustration on the operator’s part or constant attempts to adjust voltage that has little or any impact on the system. In the technical white paper this is classified as a “minority issue” however in our opinion this is an issue that definitely warrants attention therefore Exelon feels that it is appropriate to expand the scope of this project to address this and all known issues relevant to the Standards.

Individual

dmason

HHWP

No
Yes
"The Transmission Operator shall know the status of all transmission Reactive Power resources, automatic voltage regulators, and power system stabilizers in their system. [Violation Risk Factor: Medium] [Time Horizon: Operations]" does not allow for a TOP to specify its own information requirements for ensuring that its portion of the BES is operated reliably.
No
Yes it is appropriate to address the coordination between GOP and TOP in this project
Group
ACES Standards Collaborators
Jason Marshall
Yes
(1) We are concerned that the informal development process that was originally contemplated has gone off course. The original plan that was announced to industry was to have an informal development team create a proposal for a standard, which would then pass the preliminary work to a formal standard drafting team to continue the development process. This is not what has occurred. The informal development process should not circumvent the NERC Rules of Procedure. (2) We question the value in posting the draft standard with the SAR. What good is the SAR posting if a standard has already been developed? This gives the impression that the Standards Committee has already determined the need for the standard and eliminated the opportunity for industry stakeholders to provide feedback. It seems unnecessary to comment on the SAR at this point because it appears that it was drafted in tandem with the pro forma standard. We urge NERC to pay close attention to its Rules of Procedure and the Standard Process Manual to avoid deviations and setting precedent that could be challenged in the future. (3) We are also concerned that the standards process manual was not followed correctly regarding the selection of the drafting team. The nomination period began after the draft standard was posted, which clearly shows the ad hoc team developed the draft standard instead of satisfying the activities it was charged with by vetting the issues of the VAR standards with industry. The initial draft standard should be the work of the appointed standards drafting team. We doubt that there was sufficient time for the new drafting team members to thoroughly review and agree with the language in the initial posting. The method of developing the initial draft should comply with the NERC Rules of Procedure and we are concerned that a bad precedent is being set.
Yes
(1) Requirement VAR-001-4 R1 is redundant with FAC-011-2 and FAC-014-2 and, thus, meets paragraph 81 criteria. FAC-014-2 R2 requires each TOP to establish SOLs for its transmission system that is consistent with the RC SOL methodology. FAC-011-2 R2 compels the RC to develop a SOL methodology that requires SOLs to consider voltage, thermal, and stability limits (including voltage) and demonstrate that the BES remains stable (transient, dynamic and voltage) during pre-contingent (R2.1) and post-contingent (R2.2) conditions. FAC-014-2 R6 compels the Planning Coordinator to identify which Category C (multiple) contingencies from TPL-003 that result in stability limits (including voltage) and to communicate the list of Category C (multiple) contingencies along with the stability limits to the RC. FAC-011-2 further compels the RC to establish a process for identifying which stability limits associated with multiple contingencies identified by the Planning Coordinator are applicable in the operating horizon within its SOL methodology. FAC-014-2 R5.2 compels the TOP to communicate its SOLs to its RC and TSP and FAC-014-2 R5.1 compels the RC to communicate the SOLs to neighboring RCs and other TOPs among a list of other entities. Finally, existing TOP-002-2.1b R10 and proposed TOP-002-3 R2 require the TOP to operate within SOLs. Thus, the combination of FAC-011-2 and FAC-014-2 compel the establishment and communication of SOLs within the TOP footprint that already consider the items such as steady-state voltage limits and voltage stability limits compelled in proposed VAR-001-4 R1 and its subparts and TOP-002 compels the TOP to operate within those SOLs. Please strike R1 in its entirety since it is clearly redundant. If the drafting team

does not strike the requirement, we ask that technical justification be provided to explain why the requirement should remain and why the redundancy is necessary. (2) If the standards development team determines there is a technical distinction that would justify why requirement VAR-001-4 R1 remains in the standard, we suggest combining parts 1.2 and 1.3 for simplicity since they both are about providing documentation. (3) We are concerned with the statement in the rationale box for R1 that this "requirement will allow each Transmission Operator (TOP) to establish its own policies and procedures". This statement implies that the TOP cannot create its own voltage policies and procedures without this requirement. This is simply not the case. All TOPs already have their own policies and procedures for voltage so the requirement is not necessary to "allow". Since there is not a specific requirement to have such policies and procedures, some may not be documented to the level necessary to demonstrate compliance but they do exist. Please modify the rationale box to state that it will "compel" or "require" and not "allow" policies and procedures. (4) While we believe VAR-001-4 R1 is redundant with other standards as stated above, we recommend removing "establish" and "Reactive Power flow (Mvar flows)" in R1 if the requirement persists. Both are redundant and, thus, superfluous. First, you cannot monitor "voltage levels… within limits" without establishing such limits. Furthermore, the requirement to establish limits is clear in Part 1.1. Second, you cannot control voltage levels with controlling Reactive Power flows. Thus, it is redundant in the requirement. (5) If VAR-001-4 R persists, please change "Mvar" to "MVAr" in requirement R1. It is actually the correct way to document megavolt amperes reactive. (6) VAR-001-4 M1: The measure contradicts itself. It states web postings as valid evidence but then states that posting a copy of the policy or procedure on a public website is not sufficient. Is it valid evidence or not? (7) VAR-001-4 R2 is redundant with currently enforceable TOP-002-2.1b R10 and R11. R11 already requires the TOP conduct seasonal, next-day, and current-day studies or assessments to determine SOLs and R10 requires the TOP to operate within those SOLs. Remember from our response in bullet (1) that FAC-011-2 and FAC-014-2 collectively require those SOLs defined by the TOP to consider pre-contingent and post-contingent voltages and voltage stability per the RC SOL methodology. Furthermore, some of the contingencies must include Category C contingencies that cause stability issues. There are similar requirements in the proposed TOP-002-3 to perform an assessment and operate within SOLs. We suggest revising R2 to remove this overlap. (8) We disagree with including the list of reactive devices in VAR-001-4 R2. It is simply not needed and is not complete either. If a TOP is not aware of the types of tools and equipment it has available to control voltage, there are more serious issues surrounding the TOP's certification. Furthermore, it might create the unintended consequence of compelling load shedding to maintain a steady-state voltage limit. If the TOP must follow its plan in R1 to operate within steady-state voltage limits by operating "voltage regulation devices" (which includes load shed) in R2, wouldn't the literal interpretation mean that load would have to be shed because a steady-state 94% voltage was below the typical 95% steady-state limit. Obviously, this would be bad for reliability. A registered entity should never be put in a position of having to choose between compliance and reliability. (9) VAR-001-4 M2 refers to studies while VAR-001-4 R2 refers to assessments. If this requirement should persist contrary to our arguments presented in point (7), we suggest using NERC Glossary Term Operational Planning Analysis (OPA). An assessment is a vague term that has several meanings and no time boundaries associated with it. For example, "assessment" is used in the TPL standards, which mean it could go out 10 years. While we understand there would be no reasonable expectation for a TOP to perform an assessment 10 years out, there could be inconsistent compliance applications because one auditor believes an assessment should cover the next day and another believes it should cover the next week. OPA is specific and bounded by time. Furthermore, use of this term would make the standard consistent with IRO-005-4, IRO-008-1, IRO-010-1a, TOP-001-2, TOP-002-3, and TOP-003-2. (10) VAR-001-4 R3 should be modified to state the TOP shall specify the criteria that will exempt generators from maintaining the voltage schedule. The TOP is not the enforcement authority and cannot exempt another responsible entity from compliance. We are concerned the language used will not be approved by FERC and result in a subsequent directive. (11) Part 3.1 of VAR-001-4 would appear to meet the paragraph 81 criterion on reporting. The criterion states that the requirement should be retired if it "obligates responsible entities to report to a Regional Entity, NERC, or another party or entity". Clearly, the GOP would be "another party or entity". The GOP should be able to simply self-determine from the criteria provided by the GOP that it satisfies the criteria. The TOP will be able to see if the GOP is following the voltage schedule from the telemetry. If there is a question, the TOP would call the GOP. (12) While the language in VAR-001-4 R4 is clear that the TOP must have criteria for granting exemptions, the associated language in VAR-001-4 Measure M4 states that the "temporary exemptions may be

provided". Please modify the language in the measure to be clear that the temporary exemptions will be provided if the criteria are met. Otherwise, the measure sounds like the TOP has discretion in granting the temporary exemptions. (13) VAR-001-4 R4 should be modified to require the TOP to only provide a voltage schedule to generators that are capable of controlling voltage. As it literally reads now, the TOP must provide a voltage schedule "to be maintained by each generator". This would include even small generators that simply do not have the size to control voltage. As an example, a 1 MVA generator connected to a 138 kV bus should not be expected to control to a voltage schedule because it simply will never be able to maintain the voltage schedule. One potential solution to address this problem is to insert BES before generator in the requirement. Once the new definition is in effect, it would be clearer that voltage schedules must be provided only to generating units 20 MVA or greater in size and or aggregate generating plants 75 MVA or greater in size. (14) It is unnecessary to require the TOP to direct the Generator Operator to comply with the voltage schedule with the AVR in voltage control mode in VAR-001-4 Part 4.1. It is redundant with VAR-002-3 R2 which compels the GOP to follow the voltage schedule. If drafting team feels the "directive" language is necessary in VAR-001-4 Part 4.1, then VAR-002-3 R2 should be removed because it would be redundant with TOP-001-1a R3 (existing) and TOP-001-2 R1 (pending regulatory approval). Both require the GOP to follow the directives of its TOP. (15) Contrary to the rationale box for VAR-001-4 R5, this requirement is clearly redundant with TOP-006-2 R1 which requires the TOP to know the status of all generation and transmission resources available for use and VAR-002-3 R3 which requires that GOP to notify the TOP of a change in the status of the automatic voltage regulator (AVR) and power system stabilizer (PSS). Since voltage control is one of the primary responsibilities of the TOP, it can be safely assumed that a transmission resource would have to include reactive power resources. Thus, the VAR-001-4 R5 is at least partially redundant with TOP-006-2 R1. How would a generation resource not include the status of the AVR and PSS? The drafting team appears to be interpreting TOP-006-2 R1 outside of the standards development process since interpretation of TOP-006-2 R1 was not included in the scope. If the drafting team does not believe an AVR or PSS is covered in TOP-006-2 R1, the appropriate course of action would be to submit a request for interpretation of TOP-006-2 R1 to verify the interpretation. If industry would disagree through the ballot process, then the interpretation would clearly obviate the need for the requirement for the remaining parts of the requirement. Finally, we can understand why the drafting team may want to emphasize reporting changes in status of the PSS and AVR but VAR-002-3 R3 compels the GOP to report the changes to the TOP already. Please strike VAR-001-4 R5 since it clearly meets the P81 criteria regarding redundancies. (16) Please clarify VAR-001-4 R6 that the TOP must consider the safety, equipment, statutory, and regulatory requirements on the GOP when specifying GSU transformer tap changes. (17) The compliance section needs significant revision. This section does not look like a final standard and is missing much of the boiler plate language. (18) VAR-001-4 VSLs: Overall the VSLs need significant work and do not look like final VSLs. For example, the Severe VSL for R2 mentions that the TOP does not perform assessments and, therefore, does not have policies and procedures implemented. R2 does not require policies and procedures. R1 does. The same Severe VSL also has a vague statement at the end stating "a lack of real-time operation," which is also classified as Severe. How does this relate to the requirement? The VSLs for R4 are inconsistent. One mentions tolerance bands and the other does not. Furthermore, failure to provide a voltage schedule to a 1000 MVA generator on a 500 kV voltage constrained line has a much greater impact on reliability than failing to provide a voltage schedule to 25 MVA generator on a 138 kV line. The former would miss more of the requirement than the latter. The bottom line is that there is an opportunity to provide more graduated VSLs than two levels. Four should be provided for R4. (19) VAR-002-3 R2 will be problematic for some GOPs because it does not reflect the characteristics of the voltage schedule provided by some TOPs. For example, some TOPs provide an hourly average voltage schedule to avoid the need for notification for every time the GOP drifts out of schedule. How would R2 be applicable in this situation? Would it only apply for the first 15 minutes of each hour looking back at the last hour? Please modify the requirement accordingly to address this issue. (20) The VSLs for VAR-002-3 R2 are too severe. Failure to provide an explanation to the TOP for failure to provide an explanation to modify voltage per Part 2.3 should be a Lower VSL not a Severe VSL. The TOP will have telemetered voltage values and will be able to see that voltage has not been modified. Thus, the TOP will be aware of the issue and will be able to call the GOP to find out what is happening or make other arrangements to modify voltage. (21) We suggest that the VAR-002-3 R2 should use different language than "as directed by the Transmission Operator". Compliance personnel may read this to mean this is a directive. If this is directive, then TOP-001-1a R3 would also apply. In essence, the language creates the opportunity for double jeopardy because failure to follow the voltage schedule

would be a violation of VAR-002-3 R2 and could be viewed as a violation of TOP-001-1a R3 for failure to follow the directive. Similar issues exist in the subparts of the requirement. (22) The VSLs for VAR-002-3 R4 appear to be intended for VAR-002-3 R2. (23) The VSL for VAR-002-3 R5 states that a technical justification must be provided for why the GOP did not implement that tap changes. No such requirement exists in the standard. The GOP could provide a safety or statutory reason for not changing the tap which are not technical justifications. Please revise the VSL accordingly.

Yes

We believe the notification should not be required until one hour after the generator has drifted from the voltage schedule or the PSS or AVR has changed status. This will give ample time for the generator to make adjustments to return to the voltage schedules, return the PSS or AVR to service or determine that it will be unable to return the voltage schedule or return the PSS or AVR to service. Then the GOP can notify the TOP. Furthermore, the TOP will be monitoring voltage and can call the GOP in the interim if they need an update on why the voltage schedule has drifted. This will also allow ample time for the TOP to switch reactive devices should they be needed which will help return the generator to voltage schedule and increase its dynamic reactive reserve.

We have no specific additional recommendations beyond those provided in earlier questions. Thank you for the opportunity to comment.

Individual

Andrew Z. Pusztai

American Transmission Company, LLC

No

ATC doesn't have any recommended changes to VAR-001 R1. However, VAR-001-4, M1 states "the policies and procedures must detail how criteria for steady-state and voltage stability limits are used in the [TOP's] assessments …" [emphasis added]. This language should be modified to reflect the wording of the requirement, which only requires that the TOP's policies and procedures specify the criteria, not the manner in which the criteria is used in an assessment. A suggested change is: "the policies and procedures must detail the steady-state and voltage stability limits criteria to be used in the [TOP's] assessments of the system." VAR-001-4, R2 and its sub-requirements are duplicative of approved future standards TOP-001-2 R7 though R11 and TOP-002-3 R1 and R2. TOP-001-2 requires the TOP to identify and operate within SOLs and covers VAR-001-4, R2.1. The NERC definition of SOL includes both voltage stability and steady-state voltage limits. The argument that R2.1 is focused on directing reactive resources misses the point that the requirement is designed to ensure that the system is operated within SOLs. VAR-001-4 R2.1 specifies in detail what the TOP will be doing to ensure compliance with TOP-001-2 R9 through R11. TOPs should not be subjected to potentially violating two standards that cover the same ground. Similarly, TOP-002-3 R1 requires TOPs to have next-day assessments and TOP-002-3 R2 requires the TOP to develop a plan to operate within SOLs. The plan under TOP-002-3 R2 would, by necessity, include scheduling reactive resources, when necessary, to ensure SOLs will not be violated. If the comment above regarding VAR-001-4 R2 is not accepted by the ad-hoc team, the following comments on VAR-001-4 R2 should be considered: VAR-001-4, R2 does not specify "real-time and day-ahead assessments" as noted in the R2 rationale statement. The word "assessments" in R2 is not modified by any accompanying descriptor. R2 should be edited to add "real-time and day-ahead" prior to "assessments". VAR-001-4, R2.2 states that the list of options "is not limited to" the methods mentioned. However, given R2.1 specifically calls out load shedding and R2.2 does not specifically state this, it is likely that a future auditor will note this difference and state that load shedding is not acceptable under R2.2. Therefore, R2.2 should explicitly include load shedding, if necessary, as another acceptable tool in the day-ahead plan. VAR-001-4 R3.1 states that the TOP "shall notify the associated Generator Operator" but M3 states that the TOP is to have evidence showing that it notified "the associated Generator Owner". This discrepancy should be corrected. VAR-001-4 M3 places too high of a burden on the TOP for a GOP AVR issue. Specifically, the TOP is made accountable for tracking temporary exemptions granted to a GOP when the GOP calls to state that their AVR is no longer in automatic mode or is no longer controlling voltage. Since no standing exemption has been granted to the GOP (hence the phone call), the compliance obligation to show that an exemption was granted should rest on the GOP through VAR-002-3 R1 and/or R2. VAR-001-4 R4 seems to have a potential inconsistency between the

parenthetical statement and the balance of the requirement. It is suggested that R4 be rewritten and simplified as follows: “Each Transmission Operator shall specify a voltage or Reactive Power schedule and tolerance band at the interconnection point between the generator facility and the Transmission Owner’s facilities, or at either the high side or low side of the Generator Step-Up transformer at the TOP's discretion, to be maintained by each generator.” Other than our comments on VAR-001-4 R4 noted in the preceding paragraph, we agree with and fully support the current wording of VAR-001-4 R4. VAR-001-4 R5 conflicts with VAR-002-3 R3/M3 because VAR-001-4 obligates the TOP to know the status of all AVRs and PSSs but VAR-002-3 does not obligate the GOP to report status or capability changes of AVRs and PSSs if the duration of change is less than 15 minutes. VAR-001-4 R5 should be clarified to state that the TOP is dependent on the GOP to report status of AVRs and PSSs. Suggested edits are as follows: “R5. The Transmission Operator shall know the status of: 1) all transmission Reactive Power resources in its system, and 2) automatic voltage regulators and power system stabilizers as communicated by the Generator Operators in its system.” VAR-001-4 M5 should read: “The Transmission Operator shall have evidence to show transmission Reactive Power resources are being monitored” since that is the language of the requirement.
Yes
See comment in response to question #2 above where 15 minute window in VAR-002-3 R3 conflicts with VAR-001-4 R5.
ATC believes a standard is not required to address this issue.
Group
DTE Electric
Kathi Black
No
No Comments
No
No Comments
No
No Comments
It is our opinion that any communication and coordination between the TOPs and GOPs that affects reliability should be included in the standard.
Individual
Andrew Z. Pusztai
American Transmission Company
Yes
ATC does not believe that placing both VAR Standards on one ballot is a good practice, and in fact, only VAR-001 is applicable to ATC as a TO/TOP. For future postings, please post as two separate balloted Standards. This can also create a conflict such that an entity can support one and not the other, resulting in a dilema as to vote affirmative or negative that would affect one or the other Standard negatively.
Individual
Brian Shanahan
National Grid Transmission Operations
Agree
NPCC Regional Standards Committee
Individual
Catherine Wesley
PJM Interconnection

No
Yes
Specific to VAR-001-4, PJM questions why the RC is included in the standard since the responsibilities to comply with all the requirements are with the TOPs actions. If there are no actions for the RC, PJM supports the RC being removed from the standard. Included in R1 is use of the term 'establish' specific to policies and procedures that are required to be implemented. PJM supports deletion of that specific word because there are several other standards which specifically address establishing methodologies, in turn, procedures and processes, that define voltage levels, reactive power flow, steady state limits and voltage stability limits. Those standards included TPL-001, 002 (footnote a, Table1), FAC-010-2.1 and FAC-011-2 (R1, R2, R2.2) and FAC-014-2 (R1, R2, R3, R4).
No
Individual
Diane Barney
New York State Dept of Public Service
Yes
It is premature to be voting at all for the standard at this point in the process. Two major pieces of information are missing. First, the SAR has not been adopted, so we do not know if the proposed standard conforms to an adopted SAR. Second, the proposed standard was drafted by a small team of subject matter experts and has not yet been subject to a NERC wide critical review. Therefore, we do not yet know if there is a fatal flaw in the standard for some system(s) across NERC not represented by the SMEs, or if there is an outstanding idea to improve the draft standard.
Individual
John Brockhan
CenterPoint Energy Houston Electric LLC.
No
Yes
CenterPoint Energy appreciates the efforts of the informal development team in providing the industry the proposed language changes to the VAR Standards incorporating the remainng FERC Directives. CenterPoint Energy offers the following comments and proposed changes for consideration and discussion to better align the standard language to the functions of Transmission Operator and Reliability Coordinator as described in the NERC Reliability Functional Model Technical Document Version 5 in relation to the coordination and control of voltage. The Transmission Operator has policies to monitor and control static reactive devices under its range of vision and control only. The Transmission Operator also has policies for requesting reactive output from generation units already online for voltage control; however, the redispatching of generation for reliability purposes is the responsibility of the Reliability Coordinator. Since the Transmission Operator cannot control all of the generation, then the Transmission Operator is unable to perform a complete or valid Operational Planning Analysis and modify generation dispatch to maintain operational limits both steady state and dynamic. Furthermore, any maintenance outages on static reactive devices need to be reviewed and approved by the Reliability Coordinator. Also, it is unclear to the industry what kind of action is expected from the Transmission Operator based on the status of the reactive power resources since the Transmission Operator cannot dispatch other units to make up for lack of AVR or frequency control in a generator. It would seem to be crtitical for the Balancing Authority and Reliability

Coordinator to be notified of status or capability change on any generator Reactive Power resource. CenterPoint Energy recommends the requirements be modified as follows: VAR-001-4 R1. Each Transmission Operator shall have documented policies or procedures that are implemented to monitor voltage levels and reactive power flows (MVAR flows) and maintain the voltage within limits by controlling reactive devices under its purview or by directing online generation. R1.3 Each Transmission Operator shall provide a copy of its local documented policies or procedures to its Reliability Coordinator. R2. Each Reliability Coodinator shall perform assessments… R3. The Reliability Coordinator shall specify criteria… R3.1 In the event a Reliability Coordinator approves a generator as satisfying the criteria, it shall notify the associated Transmission and Generator Operator. R4. Each Transmission Operator, in coordination with the Reliability Coordinator, shall specify a voltage or Reactive Power schedule and tolerance band at the interconnection point between the generator facility and the Transmission Owner's facilities to be maintained by each generator. R4.1 The Reliability Coordinator shall provide the voltage or Reactive Power schedule to the associated Generator Operator. The Transmission Operator shall direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage). R5. The Balancing Authority and the Reliability Coordinator shall know the status of all transmission Reactive Power resources, including the status of voltage regulators and power system stabilizers. R6. After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Owner, in coordination with the Reliability Coordinator, shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes. VAR-002 R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless the Generator Operator has notified the Reliability Coordinator of one of the following…
No
Individual
Steven Mavis
Southern California Edison
Yes
SCE commends the drafting team on the work that it has done to address the FERC Order 693 Directives to modify VAR-001 and VAR-002. The draft standards are productive starting points for further clarification and refinement. Additional clarification is required before SCE can support the standards, for example, in VAR-001-4, Requirement 1.1, the use of the term "system assessment" is vague and ambiguous. The standards drafting team should provide further precision in explaining the intended meaning of this term.
Yes
The draft standards are productive starting points for further clarification and refinement. Additional clarification is required before SCE can support the standards, for example, in VAR-001-4, Requirement 1.1, the use of the term "system assessment" is vague and ambiguous. The standards drafting team should provide further precision in explaining the intended meaning of this term.
No
SCE commends the drafting team on the work that it has done to address the FERC Order 693 Directives to modify VAR-001 and VAR-002. The draft standards are productive starting points for further clarification and refinement. Additional clarification is required before SCE can support the standards, for example, in VAR-001-4, Requirement 1.1, the use of the term "system assessment" is vague and ambiguous. The standards drafting team should provide further precision in explaining the intended meaning of this term.
Group
IRC/Standards Review Committee
Gregory Campoli

Yes
We do not think the proposed requirement in VAR-001-4 which now includes RC as a Responsible Entity adequately addresses the directives. Please see our comments (b) under Q2.
Yes
VAR-001-4 a. It is unclear on the main objective and the target reliability outcome of Requirement R1, and the intent of the proposed changes in relation to the directive in P. 1868 in Order 693. We interpret R1 to require a TOP to have documented policies or procedures in place that can be implemented to establish, monitor, and control voltage levels and Reactive Power flows (Mvar flows) within limits as defined in Parts 1.1 to 1.3. However, Part 1.1 requires that the policy/procedure shall include criteria used in system assessments. It is unclear as to what "system assessments" means? Does it mean assessments of the TOP area's reliability performance with respect to the voltage levels and Mvar flows and any limits (SOLs, IROLs, reactive capability)? Or does it mean the system assessment that yields the "limits" (SOLs, IROLs, reactive requirements, etc.) which provide the target and guideline for the establishment, monitoring, and control of voltage levels and Mvar flows? It is also unclear as to what the "criteria of the assessments" means in the second sentence of Part 1.1, especially in relation to "established steady-state limits, voltage stability limits, etc. if the answer to the above question is that the assessments were meant to yield the "limits", then there is a confusion as to what limits are intended to be developed in relation to the "established" limits. In Order 693, P. 1868, FERC directs the ERO to modify VAR-001-1 to include more detailed and definitive requirements on "established limits". However, it is unclear what this directive really means. Does it mean more details and definitive requirement on stipulating voltage and reactive requirements with respect to established limits (SOLs, IROLs, voltage level, etc.) or does it mean more details on limits (boundaries) of the interconnection voltages as implied by Requirement R8 of the existing VAR-001 standard? Requirement R1 does not provide this clarity since Part 1.1. refers to "established steady-state limits, voltage stability limits", which is different than the "established limits" presented in the R8 of the existing VAR-001 standard. It is our understanding that as a general practice, a TOP will assess if there exists any reliability concerns that can be caused by voltage levels and instability to develop operating limits (SOLs or IROLs) to ensure reliable operations. The operating limits may be expressed in voltage level, pre and post-contingency power flow level, reactive support requirements or any combination of the above. The operating limits so established will provide a linkage between the SOL, voltage level and reactive power capability/reserve requirement either explicitly or implicitly. System Operators will monitor the key parameters including voltage level, power flow level and reactive power flow/reserve/capability to meet the SOL boundary conditions. Requirement R1 as presented does not provide any clarity as to what is it that in the practice that a TOP is required to meet. Requirement R1 as presented is unclear on its objective and the exact actions required of the Responsible Entity as there are a number of "criteria" and "limits" in the main requirement and its Part 1.1 that are confusing and subject to different interpretation. R1 as presented will leave a Responsible Entity not knowing what it needs to do to meet Requirement and its reliability objectives. We suggest the SDT to revise R1 and its parts to clarify its intent, especially on the who, the specific actions and expected outcome according to the results-based principle and guideline. Note that with respect to Part 1.1, Measure M1 asks for evidence that proves voltage is currently being monitored. Such evidence may include, but is not limited to: 1) proof that points are telemetered, 2) alarms are functioning, and 3) during events of low or high voltage the policies and procedures are being followed to respond to control voltage levels. These examples of evidence do not reflect the scope and depth of R1 and Parts 1.1 (the criteria and the assessment parts). We also suggest the drafting team review TOP-002 Rquirements R1, R8 and R10 as they relate to voltage limits. R1 obligates us to have plans to meet system conditions, similar to the VAR-001 R1. R8 requires us to meet voltage and reactive limits, R10 requires us to meet all SOL's and IROL's which are inclusive of voltage steady state and stability limits. The drafting team also needs to resolve the use of the term 'establish' as it relates to FAC-014 which requires us to establish SOL/IROL's that include voltage limits. b. FERC directive 1855 directs NERC to include Reliability Coordinator as applicable entities and include a new requirement(s) that identifies the reliability coordinator's monitoring responsibilities. In the Informal Consideration specific to this directive presented in the White Paper, it is indicated that: "Although some entities in Texas provided feedback that certain RCs perform functions equivalent to a TOP, the informal development group did not expand VAR-001 to give parity to TOPs and RCs." R2 as presented appears to go beyond the FERC directive that RC be

included to be assigned the "monitoring responsibility" as R2 now requires the RC to "….perform assessments on their respective areas in order to ensure sufficient reactive resources are available for scheduling to maintain voltage stability under normal and contingency conditions in order to provide the voltage levels as defined in Requirement R1". The inclusion of RC in this requirement is also inconsistent with the view presented in the Informal Consideration with respect to parity between TOPs and RCs. Parts 2.1 and 2.2 stipulates a number of tasks for the TOPs with respect to operating or directing the real-time operation of devices necessary to regulate transmission voltage and reactive flow, and to ensure that sufficient reactive resources have been scheduled to meet acceptable day-ahead voltage limits identified in Requirement R1. These tasks do not involve the RC. It thus raises a question on the need for including RC in the main requirement when it is not required to take further actions to assure its assessment of "sufficient reactive resources are available for scheduling to maintain voltage stability under normal and contingency conditions" can be fulfilled in real-time operations. We believe the inclusion of RC in this requirement is inappropriate, or if there is a compelling reason to include the RC, then Parts 2.1 and 2.2 are insufficient to assure the RC's assessment can be supported in real-time operations. c. Requirement R2, Part 2.1 stipulates that: "Each Transmission Operator shall operate or direct the real-time operation of devices necessary to regulate transmission voltage and reactive flow necessary to regulate transmission voltage and reactive flow which may include…" We do not understand this requirement as it contains two sets of "necessary to regulate transmission voltage and reactive flow". If this is a typographical error, please correct it. d. We do not have any concerns or comments on R3 and R4 as presented, but suggest that their order be reversed since the exemption criteria (R3) should appear after the overarching requirements for GOs to maintain a voltage or Reactive Power schedule and tolerance band. e. R5: we suggest to change the word "know" to "monitor". This provides an active approach, which is appropriately reflected by the wording in Measure M4. f. In the Compliance Section, there is no requirement for the RC to retain evidence for Measure M2. Further, there is no requirement for the TOP to retain evidence for Measures M5 and M6. g. VSL for R1: There is no explicit requirement in R1 for the TOP to provide a copy of the assessment criteria to its RC or neighbor TOPs since the assessment criteria are supposed to be included in the policy or procedure document. The Low VSL thus serves no purpose whatsoever. Further, from the standpoint of meeting the intent of Requirement R1, there is little to no difference between having documented policies or procedures which do not include any of the elements stipulated in Parts 1.1 to 1.3, and having no documented policies or procedures at all. In the former case, the documented policies or procedures provide absolutely no value, and hence is it a total violation of the intent of R1. We suggest to remove the Low VSL and the High VSL, and keep the Moderate VSL and revise the Severe VSL to include the condition presented in the High VSL as an "OR" condition under the Severe VSL. h. VSL for R2: Throughout R2, there are not specific requirements for having policies and procedures implemented to have sufficient Mvars. R2 requires the TOP and RC to perform assessments on their respective areas in order to ensure sufficient reactive resources are available for scheduling to maintain voltage stability under normal and contingency conditions. Part 2.2 stipulates the requirements for scheduling reactive resources to meet the reactive requirements resulting from day-ahead assessments. Part 2.1 stipulates the requirement to operate or direct the real-time operation of devices necessary to regulate transmission voltage and reactive flow. While the Moderate VSL which address non-compliance with Part 2.2 and appears to be reasonable, the Severe VSL does not correspond to how Part 2.1 is presented. Further, the condition that "A lack of real-time operations is also severe." seems irrelevant to Part 2.1 when it comes to operating or directing the real-time operation of devices necessary to regulate transmission voltage and reactive flow. There can be no lack of real-time operations, but a TOP may totally ignore the operations or directing the operations of devices necessary to regulate transmission voltage and reactive flow. Finally, there is no VSL for the RC failing to meet R2. Hence, RC is assigned a responsibility but its compliance is not measured and there is no VSL to determine its non-compliance. i. VSL for R5: The conditions in the Moderate and High VSLs are irrelevant to the requirement. R5 requires a TOP to know (monitor) the status of all transmission Reactive Power resources, automatic voltage regulators, and power system stabilizers in their system. The Moderate VSL makes reference to a "stable area", which is totally irrelevant and out of context of R5. In the High VSL, the TOP not knowing "the status of important equipment in weaker areas that were identified in assessments as part of R1." are also irrelevant and out of context of R5. Finally, there is no Severe VSL. It begs the question on: what constitutes a total failure to comply with Requirement R5? j. VSL for R6: The Low VSL should have an "is", not an "are". Also, there is no Severe VSL and hence there is no condition to constitute a total failure to comply with Requirement

R6. VAR-002-3 k. Measure M2: A good part of M2 presents the scenarios where a Generator Operator may not be able to meet voltage schedule or comply with the TOP's directive, and how a GOP may mange the situations. The description part does not belong to a Measure, and should be moved to the Background Information Section that a Results-based standard template has made provision for. l. Measure M3: the latter part of M3 is not presented in a manner to require the evidence to demonstrate compliance. We suggest M3 be revised to: The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any of the changes identified in Requirement 3, or evidence that the status had been restored within the first 15 minutes of such change. m. For all Measures, there are no examples of evidence provided. It will be appropriate if after each of the "evidence", additional wording "such as log, recording, or other documents" so as to be consistent with the way measures are presented in other standards. n. Evidence Retention: It will be appropriate to reference the Measure Number for the GO's and the GOP's data retention requirements.
No
NERC's Reliability Issue Steering Committee (RISC) is charged to address emerging reliability issues and recommend preferred approaches to manage such issues. Whether or not the TOP/GOP voltage coordination issue should rise up to a risk level that warrants special attention by the industry, and whether the appropriate way to address this issue in a standard project will be best evaluated and determined by the RISC. We suggest that the SDT nominate this issue to the RISC for its deliberation.
Individual
Clay Young
SCE&G
Yes
1. There is a general concern with this proposed standard that it will create further administrative burden for the TOP/RC as well as the back office staff. Additionally, the opportunity exists that the number of calls between the GOP and TOP will increase without materially enhancing BES reliability. Further, how would these standards be used to evaluate the compliance of a unit which has their AVR taken off auto for testing? 2. VAR-001-4 Comments: R1.1.2. Each Transmission Operator shall Delete: "provide a copy of these Comment Form-2013-04 VAR-001-4/VAR-002-3 July 2013 Page 2 of 5 https://www.nerc.net/nercsurvey/Survey.aspx?s=c645f86a592f47c9ae532b7c11d92eb1&Re... 9/3/2013 documented policies or procedures to adjacent Transmission Operators" make plans available with a written request so entities requiring documents have access. R1.1.3. Each Transmission Operator shall Delete:"provide a copy of these documented policies or procedures to its Reliability Coordinator." make plans available with a written request so entities requiring documents have access. R2. Each Transmission Operator and Reliability Coordinator shall perform assessments on their respective areas in order to ensure sufficient reactive resources are available Delete: "for scheduling" to maintain voltage stability under normal and contingency conditions in order to provide the voltage levels as defined in Requirement R1. R2.2.2. As a result of the assessments, each Transmission Operator shall ensure that sufficient reactive resources Delete: " have been scheduled" Add: "are available" to meet acceptable day-ahead voltage limits identified in Requirement R1. Sufficient reactive resources may include, but is not limited to reactive generation scheduling; transmission line and reactive resource switching; and controllable load. R5. The Transmission Operator shall know the status of Delete:"all transmission" Add: " BES" Reactive Power resources, automatic voltage regulators, and power system stabilizers in their system. Request that the SDT review R5 to ensure that it is not a duplicative of a TOP standard. M5. The Transmission Operator shall have evidence to show Reactive Power resources are being monitored. Evidence may include, but is not limited to screen shots of EMS/SCADA data, alarms, and phone logs. In the event the monitoring system does not work, each Transmission Operator should have a protocol in place to show these resources are being monitored. Request the SDT to add further clarification for AVR and PSS.
Yes
See answer to question 1.
Yes

See answer to question 1.
Group
Santee Cooper
S. Tom Abrams
No
No
We agree with the SERC Generation Subcommittee comments.
Individual
Thomas Hanzlik
SCE&G
Yes
1. There is a general concern with this proposed standard that it will create further administrative burden for the TOP/RC as well as the back office staff. Additionally, the opportunity exists that the number of calls between the GOP and TOP will increase without materially enhancing BES reliability. Further, how would these standards be used to evaluate the compliance of a unit which has their AVR taken off auto for testing?
Yes
R1.1.2. Each Transmission Operator shall Delete: “provide a copy of these Comment Form-2013-04 VAR-001-4/VAR-002-3 July 2013 Page 2 of 5 https://www.nerc.net/nercsurvey/Survey.aspx?s=c645f86a592f47c9ae532b7c11d92eb1&Re... 9/3/2013 documented policies or procedures to adjacent Transmission Operators” make plans available with a written request so entities requiring documents have access. R1.1.3. Each Transmission Operator shall Delete:“provide a copy of these documented policies or procedures to its Reliability Coordinator.” make plans available with a written request so entities requiring documents have access. R2. Each Transmission Operator and Reliability Coordinator shall perform assessments on their respective areas in order to ensure sufficient reactive resources are available Delete: “for scheduling” to maintain voltage stability under normal and contingency conditions in order to provide the voltage levels as defined in Requirement R1. R2.2.2. As a result of the assessments, each Transmission Operator shall ensure that sufficient reactive resources Delete: “ have been scheduled” Add: “are available” to meet acceptable day-ahead voltage limits identified in Requirement R1. Sufficient reactive resources may include, but is not limited to reactive generation scheduling; transmission line and reactive resource switching; and controllable load. R5. The Transmission Operator shall know the status of Delete:”all transmission” Add: “ BES” Reactive Power resources, automatic voltage regulators, and power system stabilizers in their system. Request that the SDT review R5 to ensure that it is not a duplicative of a TOP standard. M5. The Transmission Operator shall have evidence to show Reactive Power resources are being monitored. Evidence may include, but is not limited to screen shots of EMS/SCADA data, alarms, and phone logs. In the event the monitoring system does not work, each Transmission Operator should have a protocol in place to show these resources are being monitored. Request the SDT to add further clarification for AVR and PSS.
No
Individual
Laurie Williams
PNM Resources, Inc.

No
Yes
PNM disagrees and cast a negative ballot vote due exclusively with the implementation timeframe of one calendar quater. One calendar quater does not appear to be enough time to prepare a documented policy or procedure for assessments that is required of Transmission Operators nor does it allow sufficient time for the newly applicable RC function to prepare its compliance documentation as well as ensure processes/procedures are established and working well prior to the effective date. Finally, Transmission Operators t which were not previously providing voltage/reactive tolerance bands will need additional time to establish this exchange with Generator Operators. PNMR suggests a minimum of 2 calendar quarters for implementation to ensure registered entities are not forced to self report non-compliance due to the extraordinarily short implementation schedule. PNMR has no issues with the wording in the standards and is otherwise in favor of the new proposed standards.
No
None.
Individual
Andrew Gallo
City of Austin dba Austin Energy
No
Yes
For requirement R1, Austin Energy proposes that the standard include generator “testing mode” in the exemption criteria. Austin Energy proposes the following for R1-first bullet item: ”That the generator is being operated in start-up, shutdown or testing mode pursuant to a Real-Time communication or a …….”
Yes
Austin Energy believes Requirement 2.1 is not focusing on the most useful metric for Transmission voltage stability. In the ERCOT Region, the Transmission Operators (Local Control Centers) monitor voltage on their Facilities and, when necessary, control the voltage by operating or directing the operation of reactive devices including reactive generation scheduling. The Generator Operator responds to requests from the Local Control Center for voltage support and notifies the Local Control Center if it is unable to provide voltage support. Asking the GOP to monitor voltage at the GSU and notify the TOP of certain deviations is somewhat redundant and not useful because the Local Control Center already monitors voltage at the system level and directs the Generator to alter MVAR output. Typically, in the ERCOT Region, the Generator and Generator Operator have no visibility into the larger system voltage and operate in a responsive mode. Generator equipment settings (Tap Settings & MVAR Settings) are set to meet the assigned voltage schedule under normal operating conditions and are adjusted only when a request for voltage support is received. Therefore, Austin Energy recommends altering the requirement to read “If the GOP is unable to meet the reactive support requested by the TOP due to equipment limitations it shall notify the Transmission Operator”, as already required in R2.3.
These comments apply to the VSLs (you did not provide an opportunity to do so elsewhere in this comment form): It looks like the VSLs for R2 show up for R4 and vice versa. R4 is merely a requirement to provide data, yet the VSLs address failing to maintain voltage schedules. On the other hand, the VSL for R2 has only a "severe" entry and penalizes the Registered Entity only if it fails to perform ANY sub-requirement (there are three). That doesn't seem correct. Finally, the VSL for R5 applies only if the Registered Entity does not perform BOTH requirements. That also appears incorrect.
Group
SPP Standards Review Group
Robert Rhodes

No
Yes
VAR-001-4 Replace ‘real time’ with ‘Real-time’ in the Purpose and throughout the standard. It is a NERC defined term. R1 requires the TOP to have policies and procedures that establish, monitor and control voltage levels and Reactive Power flows in the Operations timeframe. Is the requirement stating that the Transmission Operator must develop the voltage and reactive schedules in Real-time? This function is typically performed behind the scenes by Transmission Planners or other support staff. We suggest that the wording be changed by deleting ‘establish’. Additionally, the white paper states that the Operations timeframe is from Real-time up to one year in the future. Real-time, according to NERC Time Horizons document, is within one hour or less while Operations Planning is from day-ahead to up and including seasonal. We suggest this be revised to state the Real-time Operations thru Operations Planning time horizons. R1.2 and R1.3 are redundant with TOP-004-2, R6 and do not need to be repeated in this standard. We recommend deleting these two sub-requirements. In M1 insert ‘and controlled’ in the 6th line after ‘monitored’ such that the sentence states ‘…is currently being monitored and controlled.’ Also inisert ‘adjacent’ in front of Transmission Operator and add an ‘s’ to Operator in the next to last line. R2 requires voltage stablility assessments to be conducted by the TOP but no direction is given on how often these assessments must be performed. While we’re not asking the drafting team to place specific time limits on when assessments must be performed we would like to know what conditions would drive the need for performing a new voltage assessment. This should then be incorporated into the requirement. Also, are references to online assessments referring to Real-time snapshots for input into steady state voltage analysis or are they referring to dynamic voltage stability assessments? Given that it is stated in the Rationale Box for R2 that online assessments are not being specifically required in this standard, what kind of assurances does a TOP have that an audit team won’t expect the TOP to have such functionality available on the control room floor? The word ‘switching’ is left by itself in the listing of resources in M2. We’re not real sure what it refers to but would suggest that we delete capacitor banks and switching and replace it with transmission line and reactive resource switching. This recognizes that switching out a transmission line or a reactor bank serves the same purpose as switching in a capacitor bank. Also, delete the 2nd ‘provide’ in the next to last line of M2. R3 exempts GOPs from R4 but GOPs are not required to do anything in R4. The exemption should apply to VAR-002-3, R2. This is stated in the white paper on Page 8 in the first line under Requirement 3. In the 4th line of M3 ‘maybe’ should be ‘may be’. R4 requires the TOP to direct the GOP to follow the voltage schedule the TOP provided to the GOP. R2 of VAR-002-3 requires the GOP to maintain its assigned voltage schedule and the TOP does not need to direct the GOP to follow it also. This is redundant and should be removed. For consistency with the Measure, delete last sentence of M3. We recommend retiring R6 because it is simply a mechanism for adhering to the requirements in R4. R4 is more of a results-based requirement – follow the provided schedule. R6 is providing one option to assist in following R4. It should be deleted. The VSLs for R2 do not match the requirement. In fact, they add requirements which are not included in the standard. We recommend deleting the Moderate VSL for R2 and revising the Severe VSL to read The Transmission Operator does not perform assessments of their area. Unless the VSLs for R4 are spread out among all categories; did not provide to one GOP for Low, two GOPs for Moderate, three GOPs for High and four or more GOPs for Severe, we would suggest simply deleting the existing High VSL, leaving only the Severe VSL. The VRF shown in R5 does not match the VRF in the VSL table. One is Medium and the other is Lower. Which is it? The justification for the inclusion of power system stabiliizers in R5 is weak to say the least. Why does this equipment need to be highlighted and other equipment, such as capacitor banks and reactors, not? TOP-006-3 R1 requires the TOP to know the status of all generation and transmission resources within its area. R2 goes on to specifically include static and rotating reactive resources. It would appear that R5 is then duplicative with these requirements and therefore could be retired. If AVRs and PSSs need to be highlighted, they should be highlighted in TOP-006 and not in this standard. VAR-002-3 We have a concern that the use of Generator Operator in this standard appears as an attempt to change the definition of GOP to the operator inside the plant control room. Some of the functionality referred to in the standard specifically points to the plant personnel rather than the NERC defined Generator Operator. For example, controlling the AVR. This is something that a plant operator would do not the Generator Operator consolidating several plants at some remote location. This would be similar to field support personnel in a transmission setting. We suggest changing the responsibility to plant

personnel. We recommend replacing ‘directed’ with ’provided‘ in R2 and R2.2. The way the timing logic is written in R2.1 if a GOP is outside the tolerance band for longer than 15 minutes and the GOP has the capability to return to control, the GOP does not have to notify its TOP. Either the ‘and’ needs to be changed to an ‘or’ or the sub-requirement needs to be totally rewritten. Delete ‘associated’ when referring to TOPs in R3, M3 and R5. We recommend moving the VSLs from R4 to R2 with the following changes: LOW – When unable to maintain voltage or reactive power schedule the Generator Operator notified its TOP in more than 30 minutes but within 45 minutes. MODERATE – When unable to maintain voltage or reactive power schedule the Generator Operator notified its TOP in more than 45 minutes but within 60 minutes. HIGH – When unable to maintain voltage or reactive power schedule the Generator Operator notified its TOP in more than 60 minutes but within 75 minutes. SEVERE – When unable to maintain voltage or reactive power schedule the Generator Operator notified its TOP in more than 75 minutes or did not notify its TOP at all. We recommend changing the Severe VSL in R3 to: The responsible entity did not notify its TOP of a status or capability change as specified in R3. The provided VSLs for R4 probably belong to R2 and could be used there if the drafting team chooses to dispurse the severity of the violations across the VSL spectrum. We recommend the following for the VSLs for R4. LOW – The Generator Operator provided the data requested in R4 in more than 30 days but within 45 days. MODERATE – The Generator Operator provided the data requested in R4 in more than 45 days but within 60 days. HIGH – The Generator Operator provided the data requested in R4 in more than 60 days but within 75 days. SEVERE – The Generator Operator provided the data requested in R4 in more than 75 days or the Generator Operator did not provide the data at all. We recommend changing the Severe VSL in R5 to: The responsible entity did not perform the specified tap change and failed to provide the technical justification to its TOP as to why it did not comply with the request as required in R5.
Yes
Please see our comment in Question 2.
The information provided is not sufficient to make this determination. Additional, specific information regarding precisely what the issues are is needed.
Group
Bonneville Power Administration
Jamison Dye
No
Yes
BPA considers the impact of large renewable generation projects (asynchronous machines) in our interconnection requirements and recognizes the ability of these machines or their auxiliary devices to support voltage. BPA recommends the drafting team address renewable resource voltage control in VAR-002-3. BPA believes that VAR-001-4, Requirements R1.1 and R2 are redundant as they appear to overlap with existing Mandatory standards. FAC-011-2, Requirements R1, R2 and R3 establish that the RC Methodology includes process and pre/post contingency performance, including margins. FAC-014-2, R2 instruct the TOP to establish SOL’s in accordance with the RC Methodology. Because of this, BPA believes that VAR-001-4, R1.1 is already established in these FAC standard requirements. Additionally TOP-002, R11 requires the TOP to perform seasonal, next day and current day studies to determine SOL’s. Because of this, BPA believes that VAR-001-4, R2 appears to be redundant. BPA recommends the elimination of R1.1 and R2 of VAR-001-4 to remove this redundancy.
No
Group
PacifiCorp
Kelly Cumiskey
No

Yes
PacifiCorp would like to point out that there is no uniform method with which voltage schedules are established in R1 of VAR-001-4. If there isn't anything specific that a TOP is expected to look at or address when drafting the procedures or policies for establishing voltage schedules, it is not clear to PacifiCorp how the policies and procedures will be measured. Moreover, if the policies and procedures only include a TOP's own criteria for the studies used to establish voltage schedules, how does requiring a documented policy and procedure in the reliability standard (referenced on page 7 of the NERC White Paper) "remove the opportunity for auditors or other parties to scrutinize a TOP's own system studies"? Additionally, PacifiCorp would like more clarity with respect to how real-time reactive deficiencies are expected to be identified in R2 of VAR-001-4. The rationale for R2 states that the informal development team believed the requirement should not require a utility to purchase new online simulation tools but in the absence of such tools, it is not clear to PacifiCorp how real-time reactive deficiencies can be captured.
No
Individual
Ryan Walter
Tri-State Generation and Transmission Association, Inc.
No
Yes
In the draft of VAR-001-4 R2 the use of the word 'schedule' when referring to all reactive resources is unclear. This is in conjunction with the Compliance response to question 2 part 2, "…provide the documentation for the day ahead scheduling in addition to documentation supporting that it was scheduled…" found in the NERC document Draft Reliability Standard Compliance Guidance for VAR-001 and VAR-002 dated July 8, 2013. Is it the ad hoc group's intent to have a schedule for all reactive resources including capacitors, reactors, Static var Compensators and generators? Is the schedule meant to be similar to that of a generator (i.e. Insert capacitors at 1.0pu and remove at 1.05) or on a time base? Is schedule just supposed to take into account availability of all reactive resources? For VAR-001-4 R4 Tri-State Generation and Transmission Association, Inc. (TSGT) believes it would be beneficial to include a feedback loop from the GOP to the TOP when there are generator capability concerns with regards to the TOP's supplied voltage schedule. Also TSGT believes the statement "(at either the high or low side of the Generator Step-Up transformer at the TOP's discretion)" currently in VAR-001-4 R4 to should be changed to "(at an agreed upon metering point to which the GOP has direct access)." For VAR-001-4 R6 why did the ad hoc group not change the consultation requirement from GO to GOP? Tri-State believes that this information would better serve the GOP function particularly at Co-Owned facilities. This change would not have a negative effect on the reliability of the BES would reduce duplicative notification to be administered by the TOP. TSGT suggests the ad hoc group add the statement "Notification to the TOP is not required if the GOP can return to schedule" to the end of VAR-002-3 R2.1 to provide further clarification when notification is needed. For VAR-002-3 R5 TSGT believes the TOP should consult with the GOP rather than the GO to better align requirement R5 with its subrequirement R5.1.
No
TSGT does think a feedback loop would be beneficial for VAR-001-4 R4 as noted in our comment to question 2.
Individual
Denise Yaffe
Southern California Edison
No

No

No

SCE commends the drafting team on the work that it has done to address the FERC directives in Order 693 to modify VAR-001. The draft standard is an excellent baseline/ starting point to accomplish this endeavor the draft VAR-001-4 standard, currently out for comment and balloting, still needs additional clarity and refinement before it can be moved forward and go into effect. An example of the need for clarity can be found in the Requirement 1.1, and the use of the term "system assessment". The drafting team should better describe this term as it is somewhat ambiguous in nature.

Group

NAGF Standards Review Team

Patrick Brown

Yes

VAR-001: 1. The rationale statement for R1 of VAR-001 says that it, “will allow each Transmission Operator (TOP) to establish its own policies and procedures,” regarding voltage schedules and tolerance bands. This wording does nothing to prevent specifying an unreasonably-tight bandwidth (e.g. +/- 0.5%), as some parties are now doing. We suggest that R1.1 end as follows, “…voltage schedules along with associated tolerance bands of not less than 1.5% of the schedule voltage unless technically justified.” There may be some resistance to making the standard prescriptive, but it’s not a burdensome requirement, and it would be unfortunate to update the standard without addressing known abuses of the present version. 2. The statement, “Each Transmission Operator shall specify a voltage or Reactive Power schedule and tolerance band (at either the high side or low side of the Generator Step-Up transformer at the TOP's discretion) at the interconnection point between the generator facility and the Transmission Owner's facilities,” in R4 of VAR-001 has a semantics glitch in that there is just one interconnect point. That is, mandating control at the interconnection eliminates any discretion in making the high vs. low-side selection. We suggest saying instead, “Each Transmission Operator shall specify a voltage or Reactive Power schedule and tolerance band, at the agreed upon metering point to which the GOP has access.” This will typically be either the transmission bus or the generator terminals. If the TOP specifies this as the TO’s “transmission bus”, the TO should be required to make the same voltage point used by the TOP available to the GOP to ensure both are seeing the exact same voltage. Additionally, there needs to be a feedback loop from the GOP to the TOP regarding the voltage schedule. This does not mean we want to spark a debate every time a schedule is provided, but simply add a step that allows a GOP to provide feedback regarding the feasability of the schedule. A recommended R4.2: R4.2 The Generator Operator shall review the voltage or Reactive Power schedule and tolerance band provided by the Transmission Operator and inform the Transmission Operator of any conditions that would prevent the Generator Operator from complying with the schedule or tolerance band, along with the technical basis for that determination. The question that then comes up is, what does the TOP do if the GOP cannot comply with the schedule as presented? Recommended R4.3: R4.3 If the Generator Operator is unable to comply with the voltage or Reactive Power schedule or tolerance band as provided by the Transmission Operator, the Transmission Operator shall (a) modify the voltage schedule within the parameters established in the documented policies and procedures established in R1, taking into account the Generator Operator’s limitations, or (b) exempt the Generator Operator from following the voltage schedule or tolerance band using the criteria established in R3. 3. We’d like to see R6 of VAR-001 changed to, “After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes that is mutually agreed, and technical justification for these changes.” That is, the change should normally wait until it can be rolled into a scheduled downtime event. We sometimes get people studying things for numerous months, then when finally reaching a decision wanting to know why we can’t make the change in the next day or two. VAR-002: 1. We suggest changing, “The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to

operate a generator in the automatic voltage control mode as specified in Requirement 1," in M1 of VAR-002 to a more semantically neutral, "The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it did not operate a generator in the automatic voltage control mode." 2. The SRT recommends the following changes to R2, for clarity; R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule3 (within each unit's ratings or capabilities4) as directed by the Transmission Operator. [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] 3. We suggest corresponding changes to R2.1. Note that the time frames are left blank in our recommendation, as there is still much discussion within the industry as to what an approporitate timeframe would be; If the system bus voltage drifts out of schedule, each Generator Operator shall notify its associated Transmission Operator within __ minutes when both of the following conditions are met: 1) the GOP has been operating outside of the prescribed voltage or Reactive Power schedule tolerance band5 for __ minutes; and 2) the GOP is no longer able to return to its voltage or Reactive Power schedule. Notification to the TOP is not required if the GOP can return to schedule. 4. In line with the recommended changes above, we suggest changing M2 to; Generator Operators shall operate the generators to help minimize excursions outside the established tolerance bands for the agreed-upon metering point. It is recognized that excursions may occur outside of the tolerance bands during unit start-up and shut-down, during MW and MVAR loading at a transmission bus where multiple units are connected, during time of relatively sudden transmission system loading changes, during system events and when grid conditions are beyond the capability of a generator to correct. Therefore, when the system bus voltage is out of the tolerance band, the Generator Operator will not be held in non-compliance with this requirement if the sub-requirements 2.1, 2.2, and 2.3 are met. In order to identify when a unit is deviating from its schedule, GOPs will monitor voltage at the agreed upon metering point to which the GOP has access. Therefore, GOPs have the option to operate on a voltage schedule on either the high-side or convert the high-side schedule to a low-side schedule at the GOP's discretion. For units that monitor on the low-side/terminal voltage, Generator Operators shall provide evidence of the method of conversion from the high-side schedule to low-side monitoring. GOP shall have evidence to show compliance with requirement R2 by providing 1) Communications with the TOP when the Generator Operator was operating outside of the prescribed voltage or Reactive Power schedule tolerance band for __ minutes AND Generator Operator was unable to return the generator to operation within its voltage or Reactive Power schedule tolerance bands; 2) Generator Operator implemented an alternative method to control reactive output when the AVR was out-of-service or unavailable; 3) compliance with directive to modify voltage or a notification that the directive could not be met. Evidence may include, but is not limited to Generator Operator logs, SCADA data, phone logs, and any other alarming notifications that would alert the Transmission Operator that both conditions were met. Timing for Requirement R2.1 can be crucial during system events, and Generator Operators are expected to begin timing when notified of an event by the TOP as soon as the unit is operating outside of the tolerance band. Further, voltage documentation during a system event may be requested by an auditor to show measures were taken to bring the unit back into schedule. 5. To harmonize Footnote 4 with our recommended language for R2, we suggest Footnote 4 be revised to state; For the operations horizon, the GOP may choose a test-based or real-time method of establishing a unit's reactive power capability. The test-based capability is that determined for compliance with MOD-025. Parameters typically monitored for determining real-time capability may include 1) generator loading (MW, MVAR, amps), temperatures, and terminal voltage; 2) GSU loading and temperatures; 3) auxiliary bus voltages; 4) plant auxiliary equipment loadings, temperatures, and voltages; 5) Generator and GSU Volts/Hz limits; 6) excitation system and/or AVR limits. 6. If R2.1 sticks, we would like to see M2 clearly state that "if the GOP can return to schedule, he does not have to notify the TOP." 7. For the new footnote 6 referenced above; The TOP is to establish an official-for-compliance bus and phase voltage point for monitoring compliance of generators controlling to the high-side voltage. An excursion begins for compliance purposes when the measured voltage exceeds the bandwidth boundary by a recognizable amount (0.5%). Multiple notifications to the TOP need not be made when the system voltage wanders back and forth across the bandwidth boundary. The system voltage must be back within the boundary for one hour before the next excursion counts as a separate event. 8. VAR-002, R2.2 should read, "When a generator's automatic voltage regulator is out-of-service, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator, unless the TOP grants an exemption." The purpose of this change is to reference the process established in R3 of VAR-001. 9. VAR-002, R4 should be revised to state; "For

generator step-up and auxiliary transformers with nominal primary voltages equal to the generator terminal voltage:" This is to clarify that R4 is N/A to startup transformers and other station auxiliary transformers connected to a HV bus at a plant. 10. VAR-002, R5 should read, "after consultation with the Transmission Operator and agreement on schedule regarding necessary step-up transformer tap changes…'" for the reason stated under comment 3 above. Regarding the Technical Whitepaper; 1. The statement on p.7 that, "the more VARs produced at a generating facility, the fewer MWs produced," would be true only if operating to the generator OEM D-curve limit, and many generation units are instead typically limited by generator voltage limits due to variations in aux bus voltages. Under the latter situation raising and lower reactive power export or import does not affect the MW capability. 2. The statement on p.7 that "the informal development group did not want to place numerical requirements on what the proper operational limits should be for the continent," fails to consider that there are present-day abuses of the system that should be addressed in the VAR-001 update. Self-policing isn't working, hence our comment #1 above. 3. Ref. "unit drifts out of schedule," on p.9 it is the system that is drifting, not generation units. 4. The statement on p.10, "This industry divide is not addressed in the pro forma standard presented today," appears to account for some of the ambiguity discussed in the NAGF's comments. We believe that requirements need to be unambiguous, however, and there must also exist explicit and achievable means of achieving compliance. 5. While there is a sentence in the measure that states it is clearly the generator's discretion as to whether they monitor (presumably control) low side or high side to demonstrate compliance, we believe that there is still a substantial amount of language in the Standard and the Whitepaper that would tend to cloud that by implying that a generator should monitor high side for compliance if you have high side equipment installed; in other words, the monitoring/control point is based on current installed equipment. 6. Additionally, the Whitepaper does nothing to shed light on whether generators should make manual moves to reactive output (by changing the AVR low side set-point) without explicit direction form the TOP which leaves the compliance application open for interpretation.

Yes

1. In order 693 Page 488 the FERC "directive" for VAR-002 stated, "Dynegy has suggested an improvement to Reliability Standard VAR-002-1, and NERC should consider this in its Reliability Standards development process." Dynegy's concern stated, "VAR-002-1 should be modified to require more detailed and definitive requirements when defining the time frame associated with an 'incident' of non compliance." Dynegy offered two alternatives to address their concern: "…[1] either more detail should be added to the Reliability Standard to cure this omission, Or [2] the Reliability Standard should require the transmission operator to have a technical basis for setting the time frame that takes into account system needs and any limitations of the generator." Their reasoning: "… this approach will eliminate the potential for undue discrimination and the imposition of overly conservative or excessively wide time frame requirements, both of which could be detrimental to grid reliability." Note that voltage tolerance band is not mentioned. 2. Going from NERC "should consider" Dynegy's suggested improvements to a very prescriptive time requirement (embedded in a VSL) in the current version of VAR-002 was a big step from the generation perspective. Also, it appears that Dynegy's second alternative was ignored during this step. 3. In the 2013 FERC Order approving VAR-002-2b (current version which became effective on July 1, 2013): PPL presented valid arguments against the "zero tolerance" time frame deviation introduced in the VSLs from the generator operator perspective (see Paragraphs 15 and 16). Both NERC and FERC rejected PPL's arguments. Paragraph 17 states, "NERC argues that the proposed modification would allow for a deviation in system voltage for up to 30 minutes to allow for time to correct an excursion and that such deviations from a voltage and reactive schedule is inappropriate because a deviation even up to a few minutes can negatively impact reliability." Paragraph 18 goes on to say, "NERC maintains that significant voltage deviations for extended periods of time may lead to voltage collapse and can increase the potential for a wide-area impact to the reliability of the Bulk-Power System, and as such PPL Companies' proposed modification to the VSL language should be rejected." The context of the NERC and FERC discussions and agreement on the rigid time requirement apparently assumes all TOP's voltage schedule tolerance bands are reasonable and "reliability based". Also, there seems to be an absence of discussion on Dynegy's 2nd alternative for the "the transmission operator to have a technical basis for setting the time frame that takes into account system needs and any limitations of the generator." However, the Pro Forma VAR R1 will require each TOP to have documented policies or procedures used to "establish, monitor, and controls voltage levels and Reactive Power flows within limits as defined below: R1.1 These documented policies or procedures shall include criteria used in system

assessments. The criteria for the assessments shall include established steady-state limits, voltage stability limits and associated operating margins, and voltage schedules along with associated tolerance bands." Thus, a fair question on the Pro Forma standards follows: If VAR-001 R1.1 is met, can GOPs conclude that each TOP's tolerance bands have a documented technical basis? If not, what mechanism will allow GOPs to question extremely narrow voltage or reactive power schedule tolerance bands that make compliance with VAR-002 R2.1 difficult or impossible? Note the Background discussions in the White Paper (see Pages 7 – 10). The discussion for VAR-001 R4 states, "The informal development group is cognizant of the fact that the nature of reactive power on the network varies depending on local conditions. Thus, the group focused on the process that the requirements would detail, not the proper numbers a TOP should enforce in the standard. For VAR-001, the group would not put operational limits on how a TOP should manage voltage stability for its regions; more specifically, the informal development group did not want to place numerical requirements on what the proper operational limits should be for the continent. Operating margins vary due to specific system characteristics as well as the operating conditions." This begs the question: Why was this same rationale not applied in addressing the time frame? 4. The published reasons for the changes to VAR-002 include 1) eliminating nuisance calls and mitigating compliance issues for generators (i.e. non-reliability gap reducing violations), and 2) addressing the FERC directive to NERC to "consider a timeframe" for allowing a generator to be out of schedule before having to make a notification to its TOP. It could be argued that imposition of a very prescriptive time frame alone does not fully address the FERC "directive" language and the first Pro Forma objective of reducing nuisance calls (GOP to TOP), especially if the voltage tolerance bands are extremely tight or do not have a technical basis.
Individual
Texas Reliability Entity
Texas Reliability Entity
Yes
VAR-001----R1 is too vague and general and nature. It does not establish a time period for compliance, and it does not provide sufficient criteria to allow an entity or an auditor to determine whether the "policies and procedures" are effective and adequate to satisfy the standard.
Yes
***VAR-001---- (1) R2.2 refers to "day-ahead voltage limits identified in Requirement R1," but R1 does not have a timeframe associated with it, and it does not expressly require identification of "day-ahead voltage limits." (2) The Measures include many details that appear to be intended to flesh out the requirements, not just to explain what will be expected to demonstrate compliance with the requirements. For example, most of M3 deals with "temporary exemptions," but there is no mention of "temporary exemptions" in R3. (3) In R4, is the specified voltage and tolerance band at the GSU or at the interconnection point (which in many cases is not the GSU)? In a world with long lead lines, setting a definite unique location for a voltage point and associated tolerance is required. ***VAR-002---- (1) Actions necessary to maintain a voltage or Reactive Power schedule are needed to prevent drift. As written the GOP would only have to be within its voltage or Reactive Power schedule for 2 minutes of a given hour and never notify its TOP. Is that what is intended? (2) Measure M2 contains an enormous amount of information that appears intended to modify the requirement – that is not the purpose of a measure. The requirement should be written to capture all of the elements of and exceptions to the requirement. (3) R3 ignores the requirement for the TOP in VAR-001-4 to know the status of "all transmission Reactive Power resources, automatic voltage regulators, and power system stabilizers in their system" as defined in VAR-001-4 R5. (4) In R5, there is a disconnect between actions by a GO in R5 and actions by a GOP in R5.1. (5) The VSL for R2 should be reconsidered. This does not appear to be a binary requirement, as multiple levels of non-compliance could be identified. Also, does the VSL require ALL sub-requirements to not be met before a non-compliance occurs—the language used is ambiguous. (6) The VSL for R4 does not correspond to the language of R4 (R4-data within 30 days of a request---VSL talks about timeframes of not meeting a schedule). (7) The VSL for R5 fails to recognize the role of a GO as stated in the requirement.
Yes
As written the GOP would only have to be within its voltage or Reactive Power schedule for 2 minutes

of a given hour and never notify its TOP. Is that what is intended?
Group
Western Electricity Coordinating Council
Steve Rueckert
Yes
WECC notes that Requirement R3.2 has been deleted from the proposed standard. The proposed R3 in VAR-002-3 still requires the GOP to notify its associated TOP of a status or capbility change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer (old R3.1) but the requirement for the GOP to notify its associated TOP of a status or capbility change on any other Reactive Power resource under the GOP's control (old R3.2) is no longer included in the proposed VAR-002-3. What is the purpose of removing this requirement?
No
Individual
Richard Vine
California Independent System Operator
Agree
IRC/Standards Review Committee
Individual
David Wang
SDG&E
San Diego Gas and Electric
No
Yes
R.1. This requirement is very unclear and the objective is undefined for the Transmission Operator in establishing the criteria for the system assessments that are to be included in the required policy. TOPs establish their operating limits (SOLs and IROLs) based on NERC and WECC RC (in the west) criteria. Would this established criteria (in the west) be the intended 'criteria' that should be used in a TOP's system assessment in the WECC region for this requirement or are there other minimum criteria that are expected to be included to meet compliance with this requirement? When establishing these operating limits, voltage and reactive requirements are captured when the WECC RC criteria is applied as required as part of the compliance with FAC-014-2 R2 for TOP entities in the WECC region. Does the establishment of this requirement create an unintended duplication of the reliability standards? These studies follow a specific methodology and criteria established and used, but requirement 1.1 refers to a criteria that is not entirely clear on what the TOP should be using.
No
Group
Southern Company: Southern Company Services, Inc.; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing
Pamela Hunter
No

Yes
On VAR-001 and VAR-002 regarding voltage schedule and compliance: The published reasons for the changes to these standards are 1) to eliminate nuisance calls and non-reliability gap reducing violations, and 2) to address the FERC directive to NERC to "consider a timeframe" for allowing a generator to be out of schedule before having to make a notification to its TOP. The changes to the standards do not fully address the first objective of reducing nuisance calls (GOP to TOP) regarding being off schedule. In addition, we have considered the idea of notification timeframes and do not suggest including such GOP notifications in the revised VAR-002. Currently, GOPs are required to maintain generator voltage or Reactive Power Schedules as directed by the TOP. If the GOP experiences problems maintaining voltage schedules, the TOPs, if warranted, will notify the GOP to either maintain or modify their voltage schedule as needed to maintain reliability of the TOP area. This existing construct has proved to work well and a new notification requirement is unnecessary. VAR-001-4 R1 Comments: Regarding R1 Part 1.1, the language addressing the specification for the criteria for the assessments needs refining. Regarding the verbiage specifying the inclusion of “estabilished steady-state limits”, while one would assume that means voltage level steady state limits, this needs to be clarified. Otherwise, it could be mis-interpreted to include steady state Mvar flows or other power system quantities. Also, the inclusion of voltage stability limits and operating margins is not applicable to all TOP footprints. Voltage stability limits manifests as the potential limiting phenomena in systems with high transfers or dense loads served over high nominal voltage kV transmission lines. Transmissions systems that are predominately load serving by local generation over lower nominal kV transmission lines are often shown, through off-line studies, to be limited by thermal and/or voltage level limits far in advance of voltage stability limits. Given that voltage stability analysis is not trival, this verbiage is burdensome and would require subject matter expertise that is not widely available for no reliability gain. Would suggest chaning the verbiage to “…..for systems where voltage stability limits are potentially the limiting phenomiena, the criteria for the assessment should also inlcude voltage stability limits and associated …….” Finally, need to include that voltage stability limits can be identified in off-line studies. VAR-001-4 R2 Comments: Modify R2 from…..”….are available for scheduling to maintain voltage stability under normal and contingency conditions conditions in order to provide the voltage levels as defined in Requirement R1” to ….”….are available to provide the voltage levels as defined in Requirement R1”. If the voltage limits found in R1 are honored, inheritently, any voltage stability limit will also be honored. Note for voltage stability limits associated with high transfer over EHV corridors, the corresponding pre-contingency voltage level limit may be near levels which are normally considered acceptable. In addition, VAR-001-4 R2 is redundant with several existing and future enforceable standards: TOP Requirements TOP-002 R10 and R11 & TOP-003 R1 and 2: The proposed VAR-001-4 R2 is redundant with the existing TOP-002 Requirements 10 and 11 that require operational assessments so that TOPs can plan to meet all SOLs and IROLs which include voltage limits. TOP-002 R10 and R11 will be replaced with TOP-003 Requirements 1 and 2 when the “Real Time Operations” project is approved by FERC. TOP-003 R1 and R2 require operational assessments to be able to operate within SOLs and IROLs as well. TOP-004-2 R6: VAR-001-4 R2 is also redundant with TOP-004-2 R6. The Real Time Operations SDT recognized that TOP-004-2 R6 was covered by TOP-001-2 which requires TOPs to operate within SOLs and IROLs. TOPs must perform assessments to be able to operate within such limits; therefore, the proposed VAR-001-4 R2 is redundant with TOP-004-2 R6 and TOP-001-2 when approved by FERC. RC Requirements FAC-011-2: The purpose of FAC-011-2 states, “To ensure that System Operating Limits (SOLs) used in the reliable operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.” Since this requires documented methodology for SOLs, which includes voltage and stability limits, VAR-001-4 R2 is redundant with FAC-011-2. FAC-014-2: The purpose of FAC-014-2 states, “To ensure that System Operating Limits (SOLs) used in the reliable planning and operation of the Bulk Electric System (BES) are determined based on an established methodology or methodologies.” Since this standard requires establishment of SOLs and IROLs, which include voltage and stability limits, VAR-001-4 R2 is redundant with FAC-014-2. IRO-008-1 R1: VAR-001-4 R2 is also redundant with IRO-008-1 R1 that requires RCs to perform assessments to ensure they do not exceed IROLs. IRO-005-3a : The proposed VAR-001-4 R2 is redundant with the existing IRO-005-3a R1 and its sub-requiremetns. It has been proposed to retire IRO-005-3a R1 and its sub-requirements with the SDTs rationale of “monitoring capability can be objectively measured and is essential to real-time operations – however real-time monitoring is a supporting activity and is only one of several processes used to support operation within defined parameters. Monitoring capability should be assessed during certification of an RC and not as a

requirement. " Given the IRO-005 SDT's rationale, the fact that the NERC BOT approved IRO-005-4, and the fact that assessments are already required in other existing Reliability Standards, VAR-001-4 R2 should be deleted. VAR-001-4 R4: The statement, "Each Transmission Operator shall specify a voltage or Reactive Power schedule and tolerance band (at either the high side or low side of the Generator Step-Up transformer at the TOP's discretion) at the interconnection point between the generator facility and the Transmission Owner's facilities has a semantics glitch in that there is just one interconnect point. That is, mandating control at the interconnection eliminates any discretion in making the high vs. low-side selection. We suggest saying instead, "Each Transmission Operator shall specify a voltage or Reactive Power schedule and tolerance band, at the agreed upon metering point to which the GOP has access." This will typically be either the transmission bus or the generator terminals. If the TOP specifies this as the TO's "transmission bus", the TO should be required to make the same voltage point used by the TOP available to the GOP to ensure both are seeing the exact same voltage. VAR-001-4 R5 is redundant with the existing TOP-006-2 (R1 and R2), which states the following, and with the proposed TOP-003-2 that requires TOPs to specify and entities to provide data necessary for it to perform its required Operational Planning Analyses and Real-time monitoring. R1. Each Transmission Operator and Balancing Authority shall know the status of all generation and transmission resources available for use. R1.1. Each Generator Operator shall inform its Host Balancing Authority and the Transmission Operator of all generation resources available for use. R1.2. Each Transmission Operator and Balancing Authority shall inform the Reliability Coordinator and other affected Balancing Authorities and Transmission Operators of all generation and transmission resources available for use. R2. Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall monitor applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, and status of rotating and static reactive resources. VAR-001-4 R5 is redundant with the existing TOP-006-2 R5 because it also requires TOPs to know the status of resources to bring to the attention of operating personnel important deviations in operating conditions and to indicate, if appropriate, the need for corrective action. The Real Time Operations SDT proposed to delete this requirement as it should be covered in the certification process for RCs, TOPs, and BAs. The SDT also noted that this requirement was covered by over enforceable reliability standards (BAL-005, TOP-001, and IRO-008); thus the proposed VAR-001-4 R5 is redundant and should be deleted. In addition, the reactive resources are the generator and not the ancillary resources such as AVR and PSS. VAR-001 R6: Generators should be allowed to make these changes during a scheduled unit downtime as long as the time is within a reasonable period of time. We suggest the time be within 12 months and propose the following rewording fo this requirement: "After consultation with the Generator Owner regarding necessary step-up transformer tap changes, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes that is mutually agreed and no longer than 12 months, and technical justification for these changes." On VAR-002, R2: We recommend eliminating "Facility Ratings" in R2 and in the footnote of VAR-002 R2 footnote 4. Use of the NERC-defined term "Facility Ratings" presents a problem, because only occasionally do equipment ratings define the amount of reactive power that a generating unit can import or export. We suggest using the term "unit capabilities" in lieu of the term "Facility Ratings." The clarification in footnote 4, "When a Generator is operating in manual control, reactive power capability may change based on stability considerations and this may lead to a change in the associated Facility Ratings," only further confuses the issue. R2 should read, "Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule (within each unit's capabilities) as directed by the Transmission Operator." Footnote 4 should be moved to R2.2 and changed to "When a Generator is operating in manual control, reactive power capability may change based on stability considerations." On VAR-002, M2: a) remove "all" from "all attempts" and ; b) the documentation requirements listed in the measure are excessive and unreasonable and unduly burdensome. We recommend, alternatively (or in addition), a statement from the TOP is acceptable evidence of GOP compliance with R2 (the voltage support performance). On VAR-002, R4: This requirement should be revised to state; "For generator step-up and auxiliary transformers with nominal primary voltages equal to the generator terminal voltage:" This will clarify that R4 is N/A to startup transformers and other station auxiliary transformers connected to a HV bus at a plant. On VAR-002, R5 rational: We suggest modifying the rationale for R5, second sentence to read " If the tap setting is not properly set, then the VAR capability of a unit can be affected."

Yes

As previously stated in our response from Question #2: On VAR-001 and VAR-002 regarding voltage

schedule and compliance: The published reasons for the changes to these standards are 1) to eliminate nuisance calls and non-reliability gap reducing violations, and 2) to address the FERC directive to NERC to "consider a timeframe" for allowing a generator to be out of schedule before having to make a notification to its TOP. The changes to the standards do not fully address the first objective of reducing nuisance calls (GOP to TOP) regarding being off schedule. In addition, we have considered the idea of notification timeframes and do not suggest including such GOP notifications in the revised VAR-002. Currently, GOPs are required to maintain generator voltage or Reactive Power Schedules as directed by the TOP. If the GOP experiences problems maintaining voltage schedules, the TOPs, if warranted, will notify the GOP to either maintain or modify their voltage schedule as needed to maintain reliability of the TOP area. This existing construct has proved to work well and a new notification requirement is unnecessary.
We fully support the need for coordination between the TOP/GOP regarding the establishment of voltage schedules. We suggest that a joint tap coordination study be performed. VAR-002 R5 alludes to this need for coordination. This process should help identify any transmission system and generating unit limitations with respect to var limitations and voltage support.
Group
Western Area Power Administration
Lloyd A. Linke
Agree
US Bureau of Reclamation, except for requiring the drafting team from explaining why the WECC variation should be applied outside of WECC.
Individual
Alice Ireland
Xcel Energy
No
Yes
1) VAR-001-4, R1 -- Although a good results-based reliability requirement, there is significant overlap with FAC-014 with regards to establishing SOL and IROL. The FAC-14 requires TOP to establish steady-state and stability-limited SOLs in accordance to its RC SOL methodology. For example, in the WECC RC SOL methodology, the RC states criteria for steady-state limit, voltage stability, and operating margins (in accordance with FAC-011 requirements) which apply to each TOP. Having these criteria to be established again in VAR-001-4 creates an issue of “Double Jeopardy” with FAC-014 and FAC-011 since system assessment done for establishing SOLs is fundamentally no different than described in this R1. 2) VAR-001-4, R2 -- Although a good results-based reliability requirement, there is significant overlap with TOP-002 enforceable standard. The TOP-002 R11 that states “The Transmission Operator shall perform seasonal, next-day, and current-day Bulk Electric System studies to determine SOLs”. Here the definition of SOLs already includes the steady state limits, voltage stability limit. So again, this creates a “Double Jeopardy” issue. It may be argued that TOP-002-3 has been approved by NERC BOD (but not by FERC yet) which may eliminate this issue. But even in the new TOP-002-3, R1 states “Each Transmission Operator shall have an Operational Planning Analysis that represents projected System conditions that will allow it to assess whether the planned operations for the next day within its Transmission Operator Area will exceed any of its Facility Ratings or Stability Limits during anticipated normal and Contingency event conditions” So even in this situation, the TOP already needs to have operating planning analysis... which is no different than performing assessment. 3) VAR-001-4, R2 addresses assessments for scheduling purposes while R2.1 mostly addresses real-time operation of devices. This seems inappropriate and we recommend moving R2.1 out to its own requirement. We believe that this requirement should include the RC as well as the TOP. The RC is required to do the assessment for scheduling in R2, but is not required to take any action to actually schedule the generation like the TOP is required to under R2.2. For example In the MISO region, the RC has more direct control over the generation dispatch than its members so I believe that they should also be subject to responsibility in R2.2. 4) VAR-002-3, Recommend firming up the language, such as “A Generator Operator shall notify its associated Transmission Operator…”. Also a timeframe needs to be applied to the second requirement to not

allow a GOP an infinite amount of time to return its voltage to the schedule. The M2 measure suggests that the reason the generator can't return to its schedule is because of a limiting factor. If that is the intent of the requirement, it should be stated in the requirement and not the measure. Part of the M2 measures seems to contradict statements made in the VAR-001-4 standard. M2 of VAR-002-3 states that the GOP has the "option to operate on a voltage schedule on either the high-side or convert the high-side schedule to a low-side schedule at the GOP's discretion" while R4 of VAR-001-4 states "Each Transmission Operator shall specify a voltage or Reactive Power schedule and tolerance band (at either the high side or low side of the Generator Step-Up transformer at the TOP's discretion)". This is confusing at best and contradictory at worse. Language in both standards should be cleaned up to clearly identify who has authority to determine where a voltage schedule is defined. 5) VAR-002-3, R2.1: Some vertically integrated utilities may have voltage monitoring systems managed by the TOP. In this case the notification would be done by the TOP to the GOP and the corrective actions jointly developed. Therefore, we suggest rewording R2.1 to something like this: [2.1. If a generating unit drifts out of the prescribed voltage or Reactive Power Schedule3 (within applicable Facility Ratings4) tolerance bands, the GOP and TOP shall have a process established to return the generator to the schedule or an acceptable alternative within 30 minutes.]
Individual
Roger Dufresne
Hydro-Québec Production
No
No
No
VAR-002-3 Regarding Measure M2, M2 presents the scenarios where a Generator Operator may not be able to meet a voltage schedule or comply with the TOP's directive, and how a GOP may manage the situations. The description part does not belong in a Measure, and should be moved to the Background Information Section that a Results-based standard template has made provision for. Regarding Measure M3, the latter part of M3 is not presented in a manner to require the evidence to demonstrate compliance. Suggest revising M3 to read: The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any of the changes identified in Requirement 3, or evidence that the status had been restored within the first 15 minutes of such change. For all Measures, there are no examples of evidence provided. It would be appropriate if after each of the "evidence", additional wording "such as log, recording, or other documents" so as to be consistent with the way Measures are presented in other standards. Regarding Evidence Retention, it would be appropriate to reference the Measure Number for the GO's and the GOP's data retention requirements
Group
Electric Power Supply Association
Jack Cashin
Yes
EPSA believes that simultaneous processing of the SAR and the standard, as was done in this instance puts them at cross-purpose with one another. This risks a situation where if a SAR needs changes, stakeholder comments on standard will be based on a defective SAR that needs work and becomes an inefficient use of stakeholder resources. The SAR scope for proposed VAR-002-2 has not considered all the aspects that can ensure that the Standard will reach a steady state. Since its issuance in June of 2013, NERC and Stakeholders have recognized that the "Standards Independent Experts Review Project" provides a global assessment of Standards including VAR-002-2. The Independent Experts recommend that requirements that are part of VAR-002-2 are duplicative and covered under other

standards or covered by tariff requirements. To avoid duplication or conflating reliability and market issues the SAR scope would benefit from including the recommendations of the Independent Experts in the current VAR-002-2 project. This will avoid expending resources on the Independent Experts recommendations in the future.
No
No
Individual
Russ Schneider
Flathead Electric Cooperative
Yes
Overall, the implementaiton of this requirement seems paperwork heavy for Transmission Operators and seems to single out generators in the western interconnection.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments Summary

Project 2013-04 Voltage and Reactive Control

February 27, 2014

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Table of Contents 2
Introduction 4
Consideration of Comments 5
Purpose 5
Duplication 5
AVR Modes 5
ERCOT RC Functions 5
Deviations from Voltage Schedule 5
Exemptions 5
Dispersed Generation 6
Implementation/Effective Date 6
Changing 15 minutes to 30 minutes in Requirements R3 and R4 6
Requirement R6 Functional Entity 6
VSL 6
Telemetering/Notifications 6
Compliance Input 6
Attachment A – SDT Members Contact Information 7

Introduction

The Project 2013-04 standard drafting team (SDT) thanks all commenters who submitted comments on the draft VAR-002-3 standard. This standard was originally posted with VAR-001-4 for a 45-day public comment period from August 23, 2013 through September 3, 2013. Both proposed standards were revised and re-posted for a successive ballot from October 11, 2013 to November 26, 2013. VAR-001-4 received the necessary approval and went forward to a final ballot. However, VAR-002-3 only received 66.09% of the weighted segment vote. A total of 58 sets of comments were received during the second 45-day public comment period. This document will present a summary of the comments considers by the SDT after the most recent comment period for VAR-002-3.

All comments submitted may be reviewed in their original format on the standard's project page.[1]

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[2]

[1] The project page is available here: http://www.nerc.com/pa/Stand/Pages/Project2013-04VoltageReactiveControl.aspx.
[2] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Consideration of Comments

Purpose

The VAR SDT appreciates the comments from industry regarding the VAR-002-3 standard. All comments were reviewed carefully by the SDT and changes were made to the standard accordingly. While all comments were reviewed, the new Standards Process Manual (SPM) does not require responses to each individual comment when a successive ballot is needed. However, this document provides a summary of responses to comments. The following pages will provide a summary of the comments received and how the comments were addressed by the VAR SDT. If a specific comment was not addressed in the summary of comments, please contact the NERC Standards Developer or one of the SDT members to discuss.

Duplication

Several commenters suggested that VAR-002-3 duplicated requirements in the TOP and MOD standards, namely TOP-001, TOP-003, and MOD-032. The VAR SDT is very mindful that the TOP-001 and TOP-003 on file with FERC are currently being re-evaluated in a separate project, and the Commission recently recommended a full remand of those standards. There is also an on-going effort to review the TOP/IRO standards, and until those standards have been finalized and approved, the SDT could not rely on those standards as a premise to remove requirements from VAR-002-3. Further, the MOD-032 standard does not apply to Transmission Operators (the entity making the data requests that would precipitate VAR-002 compliance), and the operating horizons are different from the VAR standards. Therefore, the SDT could not remove requirements based on MOD-032 overlap.

A commenter recommended removing Requirement R2 as duplicative of the TOP standards, but as explained above, that was not possible since the TOP standards are currently being reviewed. Further subpart 2.2 requires an explanation for why a voltage schedule cannot be met, and no other standard covers that. In addition, subpart 2.3 provides a caveat that a conversion methodology maybe provided during an audit, and auditor should not use the VAR standard to require high-side monitoring for GOPs. This is also not duplicated in any other standard.

AVR Modes

Some commenters recommended revisions to the standard to allow for multiple voltage control modes. The SDT agreed, and Requirement R1 was revised to allow GOPs to operate with the AVR in-service and in a mode different from “voltage controlling” if instructed by the TOP.

ERCOT RC Functions

Some commenters asked that the standard account for ERCOT nuances where the RC functions like a TOP in other areas. The VAR SDT determined the standard did not need to be modified because in ERCOT, RCs and TOPs have already determined their roles through contractual arrangements.

Deviations from Voltage Schedule

Some commenters recommended providing a minimum threshold for notifications when deviations to voltage schedules occur. The time-frames recommended were rolling averages (30 or 60 minutes), but the VAR SDT could not make these modifications. A smaller window was proposed in the last unsuccessful draft of VAR-002-3, and the industry could not reach a consensus on the right window for the entire continent. Thus, VAR-001-4 was modified to allow the TOPs to set notification timeframes based on the system needs. Also, NERC staff opposed creating too large of non-compliance window due to Reliability concerns.

Exemptions

Some commenters asked for more clarity on what qualifies as an exemption. In VAR-001-4 the TOP may set the exemption criteria for GOPs. TOPs must notify the GOPs when the exemption criteria has been met by the GOPs.

Dispersed Generation

Some commenters asked that VAR-002-3 be amended to account for dispersed generation. However, the VAR SDT is deferring to the Dispersed Generation team currently evaluating standards that would need certain updates. The VAR SDT has provided a copy of the proposed VAR-002 changes to the Dispersed Generation team.

Implementation/Effective Date

One commenter was concerned about the effective date being too soon; however, that commenter did not realize the standard will not go into effect in the United States until the first quarter after regulatory approval. The standard will not go into effect immediately after the approval by the NERC Board of Trustees.

Changing 15 minutes to 30 minutes in Requirements R3 and R4

Some commenters recommended allowing GOPs to have the full 30 minutes to correct a status or reactive capability change, and the VAR SDT agreed that this change will simplify the standard and maintain reliability. Therefore, Requirements R3 and R4 have been amended to allow the full 30 minutes to correct an issue before notifying the TOP.

One commenter also questioned the need for certain status changes. The VAR SDT re-affirmed the need for status change notifications, and the TOPs on the drafting team confirmed they should be notified when an AVR is in service and when it comes back on after an issue in order to know what resources are available in an area.

Requirement R6 Functional Entity

Some commenters questioned why Requirement R6 applies to GOs, while subpart R6.1 applies to GOPs. The VAR SDT agreed and determined that GOs are the appropriate entity for coordinating when a unit is taken offline to make the tap changes. Therefore, subpart R6.1 has been modified to apply to GOs.

VSL

Some commenters recommended changes to the VSLs to add back in time gradations for violations. However, the VAR SDT removed many of the time elements from the VSLs because those timing elements did not have a technical basis and appeared arbitrary.

Telemetering/Notifications

Some commenters asked that telemetering count for compliance purposes when making notifications to the TOP. The notification requirements are set in VAR-001-4, but the standard does not preclude telemetering in any form.

Compliance Input

Comments were received regarding the timing of the posting of a Reliability Standards Audit Worksheet (RSAW). NERC is providing a draft RSAW that will address compliance assessment questions for the draft standard within fifteen days of posting a revised VAR-002-3.

Attachment A – SDT Members Contact Information

	Participant	Entity
Chair	Bill Harm	PJM
Member	Stephen Hitchens	Bonneville Power Authority
Member	Sharma Kolluri	Entergy
Member	Hari Singh	Xcel
Member	Joshua Pierce	Southern Company
Member	Hamid Zakery	Calpine
Observer	Joe Seabrook	Puget Sound Energy
Observer	Scott Berry	Indiana Municipal Power Authority
Observer	Brian Buckley	Tampa Electric Company
Observer	Mike Swearingen	Tri-County Electric Cooperative

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments Summary

Project 2013-04 Voltage and Reactive Control

October 11, 2013

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326

Table of Contents

Table of Contents 2
Introduction 3
Consideration of Comments 4
Purpose 4
Process Comments 4
Separate Postings/Merging Standards 4
WECC Variance 4
VAR-001 Comments 4
VAR-002 Comments 5
Compliance Input 6
Attachment A – SDT Members Contact Information 7

Introduction

The Project 2013-04 standard drafting team (SDT) thanks all commenters who submitted comments on the draft VAR-001-4 and VAR-002-3 standards. These standards were posted for a 45-day public comment period from August 23, 2013 through September 3, 2013. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 78 sets of responses, including comments from approximately 211 different people from approximately 124 companies representing all 10 Industry Segments.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Consideration of Comments

Purpose

The VAR SDT appreciates the comments from industry regarding the VAR-001-4 and VAR-002-3 standards. All comments were reviewed carefully by the SDT and changes were made to the standard accordingly. While all comments were reviewed, the new Standards Process Manual (SPM) does not require responses to each individual comment when a successive ballot is needed. However, this document provides a summary of responses to comments. The following pages will provide a summary of the comments received and how the comments were addressed by the VAR SDT. If a specific comment was not addressed in the summary of comments, please contact the NERC Standards Developer or one of the SDT members to discuss.

Process Comments

Several commenters expressed concern that the simultaneous posting of the Standards Authorization Request (SAR) and the pro forma standard for initial comment and ballot was outside the scope of the Standards Process Manual (SPM). The SDT notes that, although this action was authorized by the NERC Standards Committee, NERC received an appeal of the SPM, which has been resolved. The SDT notes the process issue is outside the purview of the SDT.

Separate Postings / Merging Standards

Some commenters suggested merging the VAR standards or balloting the standards separately. Based on industry feedback and the difference in the timing of audits, the VAR SDT decided to keep the standards separate. However, the team agreed that it would be beneficial to ballot the standards separately.

WECC Variance

Some commenters were confused because the applicability section includes Generator Operators (GOP) within the Western Interconnection. This is necessary because the WECC variance in VAR-001-3 is being retained.

VAR-001 Comments

Reliability Coordinator

- Several commenters objected to adding Reliability Coordinators (RC) to the VAR-001 standard. In order to clarify the role of the RC, the VAR SDT is not going to add RCs to the standard at this time because the issue of RC monitoring is presently before FERC in another filing. Therefore, the VAR SDT will address this directive at a later time, pending a FERC order on the Interconnection Reliability Operations and Coordination (IRO) standards.

Administrative Burden

- Several commenters were concerned that there would be an administrative burden for Transmission Operators (TOPs) and RCs with the new standard. However, the new standard is intended to provide a vehicle for more efficiency and better communication once the VAR-001-4 standard is implemented; for example, fewer unnecessary phone calls/notifications will be made to the TOP once the TOP provides notification requirements to the GOPs. In addition, the standard has been modified to provide schedules to adjacent TOPs and RCs only upon request. This should alleviate some of the administrative burden involved with communicating schedules. Also, the SDT has opted to not add RCs to the standard at this time. The directive regarding RC monitoring will be addressed after order on the pending IRO standards has been issued.

Vagueness of VAR-001

- Several commenters said that several aspects of VAR-001-4 were “vague.” It was not clear to many what an “assessment” entailed and how compliance would be evaluated for many of the VAR-001-4

requirements. The revised VAR-001-4 is simplified and has clarified the standard by removing terms like "assessment," "implement," and "policies and procedures."

Duplication of Other Standards

- Several commenters stated the VAR-001-4 requirements were duplicative of several other standards. The VAR SDT determined that there is some overlap, particularly with regard to Requirements R1 and R5 of the initial posting. Requirement R5 of the initial posting has been removed, and Requirement R1 has been revised to simply require the TOP to specify voltage schedules. However, in order to show that System Operating Limits (SOLs) will encompass the details for voltage limits, both SOLs and Interconnection Reliability Operating Limits (IROLs) are referenced.

Interconnection Point

- Some commenters took issue with the phrase "at the interconnection point between the generator facility and Transmission Owner's facility." In order to allow the TOP the discretion for how to provide a voltage schedule, the phrase has been removed.

Technically Justified Schedules/Tolerance Bands

- Several commenters expressed concern because the standards did not require technically justified schedules or tolerance bands. In order to the balance the needs for maintaining a TOP's ability to monitor its system, the SDT did not add language requiring a "technically justified" schedule. Instead, the TOPs are now required under VAR-001-4 to provide the criteria to the GOPs for how the schedules were determined. This would provide GOPs with the ability to review technical documentation for schedules and tolerance bands, and this would prevent a TOP from having to dispute all of its schedules.

Power System Stabilizer

- Some commenters requested that the requirement for knowing the status of Power System Stabilizers (PSS) is a duplicate of the TOP standards. The VAR SDT determined that the importance of PSS monitoring varies by region and entity, and this requirement was removed because the TOP standards allow for the monitoring of certain data specifications. This allows the areas that require monitoring of the PSS to have this action included in the TOP data specifications, but for areas that do not need to monitor for reliability, the PSS will not have to be included. PSS equipment has not been removed from VAR-002-3 notification requirements because that equipment is part of the automatic voltage regulator (AVR).

Tap Setting Changes

- Many entities commented that the tap setting changes should have an "agreed upon" timeframe for making those changes. In order to maintain the TOPs authority, the VAR SDT only modified VAR-001-4 to require TOPs to include an implementation schedule as part of the tap setting consultation. However, the standard was not modified to require a particular timeframe for when a unit must be taken off line to make a tap setting change.

VAR-002 Comments

Testing

- Some commenters suggested modifying VAR-002-3 Requirement R1 to allow for testing of a unit. The revised standard now lists testing as a time when the unit does not have to be in AVR.

Multiple AVR Settings

- A commenter requested that the standard be updated to allow for multiple AVR settings if necessary for reliability purposes. The VAR-001-4 standard has been updated to allow for the TOPs to provide very

flexible exemptions based on system needs. These exemptions encompass being in various AVR settings based on the TOP's exemption criteria.

Timeframes for Notifications

- Many commenters questioned the timeframes proposed as a non-compliance window. It was very difficult to set a minimum notification requirement for the entire continent, particularly for being out of schedule, so the SDT opted to allow the TOPs to tailor when it should be notified by GOPs. Therefore, VAR-001-4 has a requirement to provide GOPs with their notification requirements for being out of schedule or tolerance based on system needs.

Monitoring and Conversion of a High-Side Schedule

- Although the VAR SDT initially added that the conversion of a high-side voltage schedule was acceptable in the measures for VAR-002-3, there were numerous comments that this needed to be a requirement. Thus, the VAR SDT added the requirement to provide conversion methodology for those units that do not have high-side monitoring capability.

Facility Ratings

- Some commenters suggested changing "Facility Ratings" to capability. The VAR SDT adopted this change.

VRFs/VSLs

- Some commenters recommended changes to the VRFs/VSLs for VAR-002-3 because they can be interpreted as being too severe with little to no reliability benefit. The VSLs have been simplified, and the VAR SDT modified the VRFs/VSLs significantly by removing several time constraints. The team reviewed the revised VSLs against the FERC order regarding VSL guidelines (123 FERC ¶ 61284).

Generator Owner

- One commenter suggested that the tap setting changes requirement should not include both the Generator Owner (GO) and GOP. However, both entities should be included. Several GOs are impacted when a unit has to come off-line, but the GOP is the one that will usually performs the actual changes.

Compliance Input

Comments were received regarding the posting of a Reliability Standards Audit Worksheet (RSAW). NERC is providing a Compliance Input document that acts as a draft RSAW and addresses compliance assessment questions for the draft standard.

Attachment A – SDT Members Contact Information

	Participant	Entity
Chair	Bill Harm	PJM
Vice Chair	Martin Kaufman	ExxonMobil Research and Engineering
Member	Stephen Hitchens	Bonneville Power Authority
Member	Sharma Kolluri	Entergy
Member	Hari Singh	Xcel
Member	Joshua Pierce	Southern Company
Member	Joe Seabrook	Puget Sound Energy
Member	Scott Berry	Indiana Municipal Power Authority
Member	Brian Buckley	Tampa Electric Company
Member	Mike Swearingen	Tri-County Electric Cooperative
Member	Hamid Zakery	Calpine

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR and supporting package posted for comment on July 19, 2013.
2. Draft standard posted for initial comments and ballot from July 19, 2013 to September 3, 2013.

Description of Current Draft

This is the second posting of the proposed draft standard. This proposed draft standard will be posted for a 45-day formal comment period and parallel ballot.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period with Ballot	October/November 2013
Final Ballot	December 2013
NERC Board of Trustees Adoption	December 2013
Filing to Applicable Regulatory Authorities	December 2013

Version History

Version	Date	Action	Change Tracking
1	6/18/2007	Initial Standard is FERC approved	
2	1/10/2011	FERC approved added LSEs and Controllable Load to the standard.	
3	6/20/2013	WECC Variance is approved by FERC	

Definitions of Terms Used in the Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None.

A. Introduction

1. **Title:** Voltage and Reactive Control

2. **Number:** VAR-001-4

3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real time to protect equipment and the reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators

   4.2. Generator Operators within the Western Interconnection (for the WECC Variance)

5. **Effective Date:**

   5.1. The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

Rationale for R1: P 1868 of Order No. 693 requires NERC to add more "detailed and definitive requirements on “established limits” and “sufficient reactive resources”, and identify acceptable margins (i.e. voltage and/or reactive power margins)." Since Order No. 693 was issued, several FAC and TOP standards have become enforceable to add more requirements around voltage limits. More specifically, FAC-011 and FAC-014 require that System Operating Limits (“SOLs”) and reliability margins are established. The definition of SOLs must include both: 1) Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) and *2)* System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits). Therefore, for reliability reasons Requirement R1 now requires a Transmission Operator (TOP) to set voltage or Reactive Power schedules with associated tolerance bands. Further, since neighboring areas can affect each other greatly, each TOP must also provide a copy of these schedules to its Reliability Coordinator (RC) and adjacent TOP upon request.

R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits. *[Violation Risk Factor: High] [Time Horizon: Operational Planning]*

1.1. Each Transmission Operator shall provide a copy of the voltage schedules and associated tolerance bands to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.

M1. The Transmission Operator shall have evidence that it specified system voltage schedules using either a range or a target value with an associated tolerance band.

For part 1.1, the Transmission Operator shall have evidence that the voltage schedules were provided to its Reliability Coordinator and adjacent Transmission Operators within 30 days of a request. Evidence may include, but is not limited to, emails, website postings, and meeting minutes.

Rationale for R2:

P 1875 from Order No. 693 directed NERC to include requirements to run voltage stability analysis periodically, using online techniques where commercially available and offline tools when online tools are not available. This standard does not require the periodic voltage stability analysis because such analysis is now required pursuant to the SOL methodology in the FAC standards. TOP standards also require the TOP to operate within SOLs and Interconnection Reliability Operating Limits ("IROL"). The VAR standard drafting team ("SDT") and industry participants also concluded that the best models and tools are the ones that have been proven and the standard should not add a requirement for a responsible entity to purchase new online simulations tools. Thus, the VAR SDT simplified the requirements to ensuring sufficient reactive resources are online or scheduled. Controllable load is specifically included to answer FERC's directive in Order No. 693 at P 1879.

R2. Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operational Planning]*

M2. Each Transmission Operator shall have evidence of scheduling sufficient reactive resources based on their assessments of the system. For the operational planning time horizon, Transmission Operators shall provide copies of assessments used as the basis for how resources were scheduled.

Rationale for R3:

Similar to Requirement R2, the VAR SDT determined that for reliability purposes, the TOP must ensure sufficient voltage support is provided in Real-time in order to operate within an SOL.

R3. Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operational Planning]*

M3. Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as needed in Real-time. This may include directions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments.

Rationale for R4:

The VAR SDT received significant feedback on instances when a TOP would need the flexibility for defining exemptions for generators. These exemptions can be tailored as the TOP deems necessary for the specific area's needs. The goal of this requirement is to provide a TOP the ability to exempt a Generator Operator (GOP) from: 1) a voltage or Reactive Power schedule, 2) a setting on the AVR, or 3) any VAR-002 notifications based on the TOP's criteria. Feedback from the industry detailed many system events that would require these types of exemptions which included, but are not limited to: 1) maintenance during shoulder months, 2) scenarios where two units are located within close proximity and both cannot be in voltage control mode, and 3) large system voltage swings where it would harm reliability if all GOP were to notify their respective TOP of deviations at one time. Also, in an effort to improve the requirement, the sub-requirements containing an exemption list were removed from the currently enforceable standard because this created more compliance issues with regard to how often the list would be updated and maintained.

R4. The Transmission Operator shall specify the criteria that will exempt generators from compliance with the requirements defined in Requirement R5, part 5.1, and any associated notification requirements. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

4.1 If a Transmission Operator determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.

M4. Each Transmission Operator shall have evidence of the documented criteria for generator exemptions.

For part 4.1, the Transmission Operator shall also have evidence to show that, for each generating unit in its area that is exempt from: 1) following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any notifications, the associated Generator Operator was notified of this exemption.

Rationale for R5:

The new requirement provides transparency regarding the criteria used by the TOP to establish the voltage schedule. This requirement also provides a vehicle for the TOP to use appropriate granularity when setting notification requirements for deviation from the voltage or Reactive Power schedule. Additionally, this requirement provides clarity regarding a "tolerance band" as specified in the voltage schedule and the control dead-band in the generator's excitation system.

Voltage Schedule tolerances are the bandwidth that accompanies the voltage target in a voltage schedule, should reflect the anticipated fluctuation in voltage at the Generation Operator's facility during normal operations, and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a Generation Operator's automatic voltage regulator's control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the Generator Step-Up transformer at the Transmission Operator's discretion. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **5.1.** The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).
- **5.2.** The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule.
- **5.3.** The Transmission Operator shall provide the criteria used to develop voltage schedules and associated tolerance bands to the Generator Operator within 30 days of receiving a request.

M5. The Transmission Operator shall have evidence of a documented voltage or Reactive Power Schedule and tolerance band.

For part 5.1, the Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule and tolerance band to the applicable Generator Operators, and that the Generator Operator was directed to comply with the schedule in automatic voltage control mode, unless exempted. The evidence shall include written records, email, or voice recordings.

For part 5.2, the Transmission Operator shall have evidence it provided notification requirements for deviations from the voltage or Reactive Power schedule and associated tolerance band. The evidence shall include written records, email, or voice recordings.

For part 5.3, the Transmission Operator shall have evidence it provided the criteria used to develop voltage schedules and associated tolerance bands within 30 days of receiving a request by a Generator Operator.

Rationale for R6:

Although tap settings are first established prior to interconnection, this requirement could not be deleted because no other standard addresses when a tap setting must be adjusted. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

R6. After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with the requirement and that it consulted with the Generator Owner.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Transmission Operator shall retain evidence for Measures 1 through 4 for 12 months. The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operational Planning**	**High**	N/A	N/A	N/A	The Transmission Operator has not specified a system voltage.
R2	**Real-time Operations, Same-day Operations, and Operational Planning**	**High**	N/A	N/A	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an SOL.	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an IROL.
R3	**Real-time Operations, Same-day Operations, and Operational Planning**	**High**	N/A	N/A	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an SOL.	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an IROL.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Operations Planning**	**Lower**	N/A	N/A	The Transmission Operator has exemption criteria and notified the Generator Operator, but the Transmission Operator does not have evidence of the notification.	The Transmission Operator does not have exemption criteria.
R5	**Operations Planning**	**Medium**	N/A	The Transmission Operator provides the criteria for voltage schedules after 30 days of request.	The Transmission Operator provides voltage or Reactive Power schedules to some, but not all, Generator Operators.	The Transmission Operator does not provide voltage or Reactive Power. Or The Transmission Operator did not provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule.
R6	**Operations Planning**	**Lower**	Either the technical justification or timeframe are not provided.	N/A	N/A	Neither the technical justification nor the timeframe are provided.

D. Regional Variances

The following Interconnection-wide variance shall be applicable in the Western Electricity Coordinating Council (WECC) and replaces, in their entirety, Requirements R3 and R4. Please note that Requirement R3 is deleted and R4 is replaced with the following requirements.

Requirements

E.A.13 Each Transmission Operator shall issue any one of the following types of voltage schedules to the Generator Operators for each of their generation resources that are on-line and part of the Bulk Electric System within the Transmission Operator Area: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- A voltage set point with a voltage tolerance band and a specified period.
- An initial volt-ampere reactive output or initial power factor output with a voltage tolerance band for a specified period that the Generator Operator uses to establish a generator bus voltage set point.
- A voltage band for a specified period.

E.A.14 Each Transmission Operator shall provide one of the following voltage schedule reference points for each generation resource in its Area to the Generator Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- The generator terminals.
- The high side of the generator step-up transformer.
- The point of interconnection.
- A location designated by mutual agreement between the Transmission Operator and Generator Operator.

E.A.15 Each Generator Operator shall convert each voltage schedule specified in Requirement E.A.13 into the voltage set point for the generator excitation system. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

E.A.16 Each Generator Operator shall provide its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals within 30 calendar days of request by its Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

E.A.17 Each Transmission Operator shall provide to the Generator Operator, within 30 calendar days of a request for data by the Generator Operator, its transmission equipment data and operating data that supports development of the voltage set point conversion methodology. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

E.A.18 Each Generator Operator shall meet the following control loop specifications if the Generator Operator uses control loops external to the Automatic Voltage Regulators (AVR) to manage MVar loading: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

E.A.18.1. Each control loop's design incorporates the AVR's automatic voltage controlled response to voltage deviations during System Disturbances.

E.A.18.2. Each control loop is only used by mutual agreement between the Generator Operator and the Transmission Operator affected by the control loop.

Measures[1]

M.A.13 Each Transmission Operator shall have and provide upon request, evidence that it provided the voltage schedules to the Generator Operator. Dated spreadsheets, reports, voice recordings, or other documentation containing the voltage schedule including set points, tolerance bands, and specified periods as required in Requirement E.A.13 are acceptable as evidence.

M.A.14 The Transmission Operator shall have and provide upon request, evidence that it provided one of the voltage schedule reference points in Requirement E.A.14 for each generation resource in its Area to the Generator Operator. Dated letters, e-mail, or other documentation that contains notification to the Generator Operator of the voltage schedule reference point for each generation resource are acceptable as evidence.

M.A.15 Each Generator Operator shall have and provide upon request, evidence that it converted a voltage schedule as described in Requirement E.A.13 into a voltage set point for the AVR. Dated spreadsheets, logs, reports, or other documentation are acceptable as evidence.

M.A.16 The Generator Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Transmission Operator it provided its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.A.17 The Transmission Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Generator Operator it provided data to support development of the voltage set point conversion methodology. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.A.18 If the Generator Operator uses outside control loops to manage MVar loading, the Generator Operator shall have and provide upon request, evidence that it met the control loop specifications in sub-parts E.A.18.1 through E.A.18.2. Design specifications with identified agreed-upon control loops, system reports, or other dated documentation are acceptable as evidence.

[1] The number for each measure corresponds with the number for each requirement, i.e. M.E.A.13 means the measure for Requirement E.A.13.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR and supporting package posted for comment on July 19, 2013.
2. Draft standard posted for initial comments and ballot from July 19, 2013 to September 3, 2013.

Description of Current Draft

This is the second posting of the proposed draft standard. This proposed draft standard will be posted for a 45-day formal comment period and parallel ballot.~~This draft standard is concluding informal development and will move to formal development when authorized by the Standards Committee.~~

Anticipated Actions	Anticipated Date
~~SAR Authorized by the Standards Committee~~	~~July~~
Additional 45--Day ~~SAR~~ Comment Period with~~and Initial~~ Ballot ~~Open~~	October/November 2013~~July~~
~~Nomination Period Opens~~	~~July~~
~~Standard Drafting Team Appointed~~	~~July~~
~~Initial Comment and Initial Ballot Closes~~	~~August~~
Final Ballot ~~Opens~~	December 2013~~October~~
~~Final Ballot Closes~~	~~October~~
NERC Board of Trustees~~BOT~~ Adoption	December 2013~~November~~
Filing to Applicable Regulatory Authorities	December 2013

~~Effective Dates~~

~~In those jurisdictions where regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter after applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities. In those jurisdictions where no regulatory approval is required, this standard~~

~~shall become effective on the first day of the first calendar quarter after Board of Trustees approval.~~

Version History

Version	Date	Action	Change Tracking
1	6/18/2007	Initial Standard is FERC approved	
2	1/10/2011	FERC approved added LSEs and Controllable Load to the standard.	
3	6/20/2013	WECC Variance is approved by FERC	

Definitions of Terms Used in the Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None.

A. Introduction

1. **Title:** Voltage and Reactive Control

2. **Number:** VAR-001-4

3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in real time to protect equipment and the reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators

   ~~**4.2.** Reliability Coordinators~~

   ~~4.3.~~4.2. Generator Operators within the Western Interconnection (for the WECC Variance)

5. **Effective Date:**

   5.1. The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Requirements and Measures

~~**Rationale for R1:** This requirement will allow each Transmission Operator (TOP) to establish its own policies and procedures, and the criteria for periodic updates will be individualized based on the stability of each TOP's regions. The language is refined to show that coordination with neighboring TOPs is required. It also states TOP shall provide data to the Reliability Coordinator (RC) for its monitoring functions to respond to address the FERC directive in P 1855 of Order No. 693, which directed NERC to add RC monitoring to the VAR standards. P 1868 requires NERC to add more "detailed and definitive requirements to include more detailed and definitive requirements on "established limits" and "sufficient reactive resources" and identify acceptable margins (i.e. voltage and/or reactive power margins)."~~

Rationale for R1: P 1868 of Order No. 693 requires NERC to add more "detailed and definitive requirements on "established limits" and "sufficient reactive resources", and identify acceptable margins (i.e. voltage and/or reactive power margins)." Since Order No. 693 was issued, several FAC and TOP standards have become enforceable to add more requirements around voltage limits. More specifically, FAC-011 and FAC-014 require that System Operating Limits ("SOLs") and reliability margins are established. The definition of SOLs must include both: 1) Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) and *2)* System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits). Therefore, for reliability reasons Requirement R1 now requires a Transmission Operator (TOP) to set voltage or Reactive Power schedules with associated tolerance bands. Further, since neighboring areas can affect each other greatly, each TOP must also provide a copy of these schedules to its Reliability Coordinator (RC) and adjacent TOP upon request.

R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits~~have documented policies or procedures that are implemented to establish, monitor, and control voltage levels and Reactive Power flows (Mvar flows) within limits as defined below~~. *[Violation Risk Factor: High] [Time Horizon: Operational Planning~~Operations~~]*

~~**1.1.** These documented policies or procedures shall include criteria used in system assessments. The criteria for the assessments shall include established steady-state limits, voltage stability limits and associated operating margins, and voltage schedules along with associated tolerance bands.~~

1.1. Each Transmission Operator shall provide a copy of the voltage schedules and associated tolerance bands to its Reliability Coordinator and ~~these documented policies or procedures to~~ adjacent Transmission Operators within 30 calendar days of a request.

~~**1.2.** Each Transmission Operator shall provide a copy of these documented policies or procedures to its Reliability Coordinator.~~

M1. The Transmission Operator shall have evidence that it specified system voltage schedules using either a range or a target value with an associated tolerance band.

~~The Transmission Operator shall have evidence of documented voltage schedules and associated tolerance bands.~~

For part~~policies or procedures as specified in Requirement~~ 1.1~~ As stated in R1~~, the Transmission Operator shall have~~policies and procedures must detail how criteria for steady state and voltage stability limits are used in the Transmission Operator's assessments of the system. In order to demonstrate the Transmission Operator is implementing the policies or procedures, the Transmission Operator must be able to provide~~ evidence that the~~proves~~ voltage schedules~~ and associated tolerance bands~~is currently being monitored. Such evidence may include, but is not limited to: 1) proof that points are telemetered, 2) alarms are functioning, and 3) during events of low or high voltage the policies and procedures are being followed to respond to control voltage levels. The Transmission Operator must also provide evidence that the policies or procedures~~ were provided to its Reliability Coordinator and ~~communicated to~~ adjacent Transmission Operators within 30 days of a request.~~and to its Reliability Coordinator.~~ Evidence may include, but is not limited to, emails, website postings, and meeting minutes.~~ Simply posting a copy of the policies or procedure on a public website is not sufficient if the Transmission Operator and Reliability Coordinator were not notified as to where to find the policies or procedures.~~

~~Rationale for R2:~~

~~P 1875 from Order No. 693 directed NERC to include requirements to run voltage stability analysis periodically. The informal ad hoc group and industry participants concluded that the best models and tools are the ones that have been proven over time, and that the requirement should not require any utility to purchase new online simulations tools. Therefore, the new requirement does not specify when to use online tools. The sub-requirements detail the real-time and day-ahead assessments necessary under R1. The existing VAR-001 also requires a list of sufficient reactive resources; this was retained in the proposed requirement as FERC determined in a letter order that this list answered the directive in P 1868 to detail the list of "sufficient reactive resources." Controllable load is specifically included to answer FERC's directive in P 1879.~~

Rationale for R2:

P 1875 from Order No. 693 directed NERC to include requirements to run voltage stability analysis periodically, using online techniques where commercially available and offline tools when online tools are not available. This standard does not require the periodic voltage stability analysis because such analysis is now required pursuant to the SOL methodology in the FAC standards. TOP standards also require the TOP to operate within SOLs and Interconnection Reliability Operating Limits ("IROL"). The VAR standard drafting team ("SDT") and industry participants also concluded that the best models and tools are the ones that have been proven and the standard should not add a requirement for a responsible entity to purchase new online simulations tools. Thus, the VAR SDT simplified the requirements to ensuring sufficient reactive resources are online or scheduled. Controllable load is specifically included to answer FERC's directive in Order No. 693 at P 1879.

R2. Each Transmission Operator ~~and Reliability Coordinator~~ shall schedule~~perform assessments on their respective areas in order to ensure~~ sufficient reactive resources ~~are available for scheduling~~ to regulate~~maintain~~ voltage levels~~stability~~ under normal and Contingency~~contingency~~ conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load. ~~in order to provide the voltage levels as defined in Requirement R1.~~ *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operational Planning]*

M2. Each Transmission Operator shall have evidence of scheduling sufficient reactive resources based on their assessments of the system. For the operational planning time horizon, Transmission Operators shall provide copies of assessments used as the basis for how resources were scheduled.

Rationale for R3:

Similar to Requirement R2, the VAR SDT determined that for reliability purposes, the TOP must ensure sufficient voltage support is provided in Real-time in order to operate within an SOL.

R3. Each Transmission Operator shall operate or direct the Real~~real~~-time operation of ~~-~~devices ~~necessary~~ to regulate transmission voltage and reactive flow as necessary. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day* ~~necessary to regulate transmission voltage and reactive flow which may include, but is not limited to reactive generation scheduling; transmission line and reactive resource switching; controllable load; and, if necessary, load shedding, to maintain system voltages within established limits.~~*Operations, and Operational Planning]*

~~**3.1.** As a result of the assessments, each Transmission Operator shall ensure that sufficient reactive resources have been scheduled to meet acceptable day-ahead voltage limits identified in Requirement R1. Sufficient reactive resources may include, but is not limited to reactive generation scheduling; transmission line and reactive resource switching; and controllable load.~~

~~M1.~~M3. Each Transmission Operator ~~and Reliability Coordinator~~ shall have evidence that actions~~of current or past studies used to schedule sufficient reactive resources. Each Transmission Operator shall also provide proof that additional resources~~ were taken to operate ~~scheduled when necessary. During a real-time event where voltage must be adjusted, a Transmission Operator shall show evidence to show directions were given to adjust the operation of~~ capacitive and inductive resources as needed in Real-time. This may include directions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3)~~ operate within new tolerance bands or to~~ make manual adjustments. ~~if necessary. Transmission Operators shall also have evidence to show proof of directing new resources to come online. Those resources can include, but is not limited to capacitor banks, switching, adjusting controllable load, and when necessary load can be shed. For the day-ahead scheduling, Transmission Operators shall provide copies of provide day-ahead studies used to schedule enough resources to meet expected voltage requirements.~~

Rationale for R4:

The VAR SDT received significant feedback on instances when a TOP would need the flexibility for defining exemptions for generators. These exemptions can be tailored as the TOP deems necessary for the specific area's needs. The goal of this requirement is to provide a TOP the ability to exempt a Generator Operator (GOP) from: 1) a voltage or Reactive Power schedule, 2) a setting on the AVR, or 3) any VAR-002 notifications based on the TOP's criteria. Feedback from the industry detailed many system events that would require these types of exemptions which included, but are not limited to: 1) maintenance during shoulder months, 2) scenarios where two units are located within close proximity and both cannot be in voltage control mode, and 3) large system voltage swings where it would harm reliability if all GOP were to notify their respective TOP of deviations at one time. Also, in an effort to improve the requirement, the sub-requirements containing an exemption list were removed from the currently enforceable standard because this created more compliance issues with regard to how often the list would be updated and maintained.

~~**Rationale for R4.**~~

~~These exemptions offer TOPs the option to exempt certain generators during maintenance or system events when those units are not able to maintain voltage schedules. Sub-requirements containing an exemption list were removed from the existing standard because this created more compliance issues with regard to how often the list would be updated and maintained.~~

R4. The Transmission Operator shall specify the criteria that will exempt generators from compliance with the requirements defined in Requirement R5, part 5.1,~~4~~ and any associated notification requirements. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

If~~In the event~~ a Transmission Operator determines that~~approves~~ a generator has satisfied~~as satisfying~~ the exemption criteria, it shall notify the associated Generator Operator.

M4. Each Transmission Operator shall have evidence of the documented criteria for generator exemptions.

For part 4.1, the~~The~~ Transmission Operator shall also have evidence to show that, for each generating unit in its area that is exempt from: 1) following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any notifications, the associated Generator Operator was notified of this exemption. ~~following a voltage or Reactive Power schedule, the associated Generator Owner was notified of this exemption in accordance with Requirement 3. Temporary exemptions maybe provided to generators during scenarios where notifications/communications are not necessary due to a system event that prevents a Generator Operator from maintaining a schedule. Similarly, when an Automatic Voltage Regulator (AVR) is malfunctioning, which prevents a Generator Operator from maintaining a voltage schedule and tolerance band, temporary exemptions may be provided. For temporary exemptions, evidence showing the exemptions were granted must be provided. If the exemptions were given verbally from the Transmission Operator, the phone recordings or emails commemorating the phone~~

~~call must be provided. For temporary exemptions, the evidence of communication must also include the timeframe for how long the exemption will last.~~

Rationale for R5:

The new requirement provides transparency regarding the criteria used by the TOP to establish the voltage schedule. This requirement also provides a vehicle for the TOP to use appropriate granularity when setting notification requirements for deviation from the voltage or Reactive Power schedule. Additionally, this requirement provides clarity regarding a "tolerance band" as specified in the voltage schedule and the control dead-band in the generator's excitation system.

Voltage Schedule tolerances are the bandwidth that accompanies the voltage target in a voltage schedule, should reflect the anticipated fluctuation in voltage at the Generation Operator's facility during normal operations, and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a Generation Operator's automatic voltage regulator's control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

~~**Rationale for R5:**~~

~~The new requirement adds "tolerance band" in order to provide more detailed information when establishing limits.~~

R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range~~,~~ or a target value with an associated~~and~~ tolerance band) ~~(~~at either the high voltage side or low voltage side of the Generator Step-Up transformer at the ~~TOP's discretion) at the interconnection point between the generator facility and the~~ Transmission Operator's discretion~~Owner's facilities to be maintained by each generator~~. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

5.1. The Transmission Operator shall provide the voltage or Reactive Power schedule ~~and tolerance band~~ to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).

5.2. The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule.

5.3. The Transmission Operator shall provide the criteria used to develop voltage schedules and associated tolerance bands to the Generator Operator within 30 days of receiving a request.

M5. The Transmission Operator shall have evidence of a documented voltage or Reactive Power Schedule and tolerance band.

For part 5.1, theThe Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule and tolerance band ~~as specified in Requirement 4~~ to the applicable Generator Operators, and that the Generator Operator was directed to comply with the schedule in automatic voltage control mode, unless exempted. The~~. For real-time directives,~~ evidence shall~~may~~ include written records, email, or voice recordings. ~~recorded phone logs.~~

For part 5.2,

~~**R6.** The Transmission Operator shall know~~ the ~~status of all transmission Reactive Power resources, automatic voltage regulators, and power system stabilizers in their system. *[Violation Risk Factor: Medium] [Time Horizon: Operations]*~~

~~The~~ Transmission Operator shall have evidence it provided notification requirements for deviations from the voltage or Reactive Power schedule and associated tolerance band. The evidence shall~~to show Reactive Power resources are being monitored. Evidence may~~ include written records, email, or voice recordings~~, but is not limited to screen shots of EMS/SCADA data, alarms, and phone logs. In the event the monitoring system does not work, each Transmission Operator should have a protocol in place to show these resources are being monitored~~.

For part 5.3, the Transmission Operator shall have evidence it provided the criteria used to develop voltage schedules and associated tolerance bands within 30 days of receiving a request by a Generator Operator.

Rationale for R6:

Although tap settings are first established prior to interconnection, this requirement could not be deleted because no other standard addresses when a tap setting must be adjusted. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

~~**Rationale for R6:**~~

~~Since power system stabilizers (PSS) equipment is not highlighted in any other standard, the VAR standard is the appropriate place to ensure the equipment is being monitored. This requirement is not duplicative of the TOP standards because the voltage regulators and power system stabilizer are highlighted.~~

~~R7.~~R6. After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for

making the changes, and technical justification for these changes. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~M2.~~M6. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with the requirement and that it consulted with the Generator Owner.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to~~means~~ NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Transmission Operator shall retain evidence for Measures 1 through 4 for 12 months. The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	~~Operations~~Operational Planning	High	N/A~~The Transmission Operator has documented criteria for assessments, but has provided a copy to only one of the parties that should have received a copy (either a neighboring TOPs or its RC).~~	N/A~~The Transmission Operator has documented policies and procedures, but has not provided copies to either the neighboring TOPs or its RC.~~	N/A~~The Transmission Operator has documented policies or procedures, but none of the sub-requirements were followed.~~	The Transmission Operator has not specified a system voltage schedule.
R2	Real-time Operations, Same-day Operations, and Operational Planning	High	N/A	N/A~~The Transmission Operator only performs day-ahead assessments and only schedules day-ahead resources.~~	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an SOL.~~N/A~~	The Transmission Operator does not schedule~~perform assessments and therefore does not have policies and procedures implemented to have~~ sufficient reactive resources as necessary to avoid violating an IROL~~Mvars. A lack of real-time operations is also severe~~.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Real-time Operations, Same-day Operations, and Operational Planning	High~~Lower~~	N/A	N/A	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an SOL. ~~N/A~~	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an IROL~~have exemption criteria~~.
R4	Operations Planning	Lower~~Medium~~	N/A	N/A	The Transmission Operator has exemption criteria and notified the Generator Operator, but the Transmission Operator does not have evidence~~provides voltage or Reactive Power schedules to only some~~ of the notification~~GOPs~~.	The Transmission Operator does not have exemption criteria~~provide voltage or Reactive Power schedules and tolerance bands at all~~.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Operations Planning	Medium~~Lower~~	N/A	The Transmission Operator provides ~~is unaware of~~ the criteria for voltage schedules after 30 days of request~~status in a stable area~~.	The Transmission Operator provides voltage or Reactive Power schedules to some, but~~does~~ not all, Generator Operators~~know the status of important equipment in weaker areas that were identified in assessments as part of R1~~.	The Transmission Operator does not provide voltage or Reactive Power schedules-. Or The Transmission Operator did not provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule. ~~N/A~~
R6	Operations Planning	Lower	Either the technical justification or timeframe are not provided.	~~Neither the technical justification nor the timeframe are provided.~~N/A	N/A	~~N/A~~Neither the technical justification nor the timeframe are provided.

D. Regional Variances

The following Interconnection-wide variance shall be applicable in ~~Regional Variance for~~ the Western Electricity Coordinating Council (WECC) and replaces, in their entirety, Requirements R3 and R4. Please note that Requirement R3 is deleted and R4 is replaced with the following requirements.

Requirements

E.A.13 Each Transmission Operator shall issue any one of the following types of voltage schedules to the Generator Operators for each of their generation resources that are on-line and part of the Bulk Electric System within the Transmission Operator Area: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- A voltage set point with a voltage tolerance band and a specified period.
- An initial volt-ampere reactive output or initial power factor output with a voltage tolerance band for a specified period that the Generator Operator uses to establish a generator bus voltage set point.
- A voltage band for a specified period.

E.A.14 Each Transmission Operator shall provide one of the following voltage schedule reference points for each generation resource in its Area to the Generator Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- The generator terminals.
- The high side of the generator step-up transformer.
- The point of interconnection.
- A location designated by mutual agreement between the Transmission Operator and Generator Operator.

E.A.15 Each Generator Operator shall convert each voltage schedule specified in Requirement E.A.13 into the voltage set point for the generator excitation system. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

E.A.16 Each Generator Operator shall provide its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals within 30 calendar days of request by its Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

E.A.17 Each Transmission Operator shall provide to the Generator Operator, within 30 calendar days of a request for data by the Generator Operator, its transmission equipment data and operating data that supports development of the voltage set point conversion methodology. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

E.A.18 Each Generator Operator shall meet the following control loop specifications if the Generator Operator uses control loops external to the Automatic Voltage Regulators (AVR) to manage MVar loading: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

E.A.18.1. Each control loop's design incorporates the AVR's automatic voltage controlled response to voltage deviations during System Disturbances.

E.A.18.2. Each control loop is only used by mutual agreement between the Generator Operator and the Transmission Operator affected by the control loop.

Measures[1]

M.A.13 Each Transmission Operator shall have and provide upon request, evidence that it provided the voltage schedules to the Generator Operator. Dated spreadsheets, reports, voice recordings, or other documentation containing the voltage schedule including set points, tolerance bands, and specified periods as required in Requirement E.A.13 are acceptable as evidence.

M.A.14 The Transmission Operator shall have and provide upon request, evidence that it provided one of the voltage schedule reference points in Requirement E.A.14 for each generation resource in its Area to the Generator Operator. Dated letters, e-mail, or other documentation that contains notification to the Generator Operator of the voltage schedule reference point for each generation resource are acceptable as evidence.

M.A.15 Each Generator Operator shall have and provide upon request, evidence that it converted a voltage schedule as described in Requirement E.A.13 into a voltage set point for the AVR. Dated spreadsheets, logs, reports, or other documentation are acceptable as evidence.

M.A.16 The Generator Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Transmission Operator it provided its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.A.17 The Transmission Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Generator Operator it provided data to support development of the voltage set point conversion methodology. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

~~M.A.13~~**M.A.18** If the Generator Operator uses outside control loops to manage MVar loading, the Generator Operator shall have and provide upon request, evidence that it met the control loop specifications in sub-parts E.A.18.1 through E.A.18.2. Design specifications with identified agreed-upon control loops, system reports, or other dated documentation are acceptable as evidence~~VAR-001-3 is retained~~.

[1] The number for each measure corresponds with the number for each requirement, i.e. M.E.A.13 means the measure for Requirement E.A.13.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please review~~see~~ the rationale provided~~VAR White Paper~~ for each requirement~~further technical information~~.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR and supporting package posted for comment on July 19, 2013.
2. Draft standard posted for initial comments and ballot from July 19, 2013 to September 3, 2013.

Description of Current Draft

This is the second posting of the proposed draft standard. This proposed draft standard will be posted for a 45-day formal comment period and parallel ballot.

Anticipated Actions	Anticipated Date
Additional 45-Day SAR Comment Period with Ballot	October/November 2013
Final Ballot	December 2013
NERC Board of Trustees Adoption	December 2013
Filing to Applicable Regulatory Authorities	December 2013

Version History

Version	Date	Action	Change Tracking
1	5/1/2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and 2.4.3.	July 5, 2006
1a	12/19/2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	1/16/2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	Errata
1.1a	10/29/2008	BOT adopted errata changes; updated version number to "1.1a"	Errata
1.1b	3/3/2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	Revised
2b	4/16/2013	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4. FERC Order issued approving VAR-002-2b.	Revised

Definitions of Terms Used in the Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None.

A. Introduction

1. Title: **Generator Operation for Maintaining Network Voltage Schedules**

2. Number: VAR-002-3

3. Purpose: To ensure generators provide reactive support and voltage control, within generating Facility capabilities, in order to protect equipment and maintain reliable operation of the Interconnection.

4. Applicability:

4.1. Generator Operator

4.2. Generator Owner

5. Effective Dates

The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

Rationale for R1: This requirement has been maintained due to the importance of running a unit with its automatic voltage regulator (AVR) in service and in voltage controlling mode. However, the requirement has been modified to allow for testing, and the measure has been updated to include some of the evidence that can be used for compliance purposes.

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless the Generator Operator 1) is exempted by the Transmission Operator, or 2) has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- That the generator is being operated in start-up,[1] shutdown,[2] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in the automatic voltage control mode for a reason other than start-up, shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode. Such evidence must include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If exempted, the Generator Operator shall also have evidence that it is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.
[2] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

Rationale for R2:

Requirement R2 details how a Generator Operator (GOP) operates the system to maintain a voltage schedule and when the GOP is expected to notify the Transmission Operator (TOP). In an effort to remove prescriptive notification requirements for the entire continent, the VAR standard drafting team (SDT) opted to allow each TOP to determine the notification requirements for each of its respective GOPs based on system requirements. A new part 2.3 has been added to detail that each GOP shall monitor voltage based on its existing facility equipment.

Conversion Methodology: There are many ways to convert the voltage schedule from one voltage level to another. Some entities may choose to develop voltage regulation curves for their transformers; others may choose to do a straight ratio conversion; others may choose an entirely different methodology. All of these methods have technical challenges, but the studies performed by the TOP, which consider N-1 and credible N-2 contingencies, should compensate for the error introduced by these methodologies, and the TOP possesses the authority to direct the GOP to modify its output if its performance is not satisfactory. During a significant system event, such as a voltage collapse, even a generation unit in automatic voltage control that controls based on the low-side of the generator step-up transformer should see the event on the low-side of the generator step-up transformer and respond accordingly.

Voltage Schedule Tolerances: The bandwidth that accompanies the voltage target in a voltage schedule should reflect the anticipated fluctuation in voltage at the GOP's Facility during normal operations and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a GOP's AVR control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within each generating Facility's capabilities[4]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage schedule provided by the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.

[3] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.

[4] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a Generator is operating in manual control, reactive power capability may change based on stability considerations.

2.2. When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a unit is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage schedule.

For part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.

For part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's directions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the direction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For part 2.3, for units that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall document or be able to demonstrate the method of conversion from the voltage level monitored to the voltage level specified on the voltage schedule.

Rationale for R3:

This requirement has been modified to limit the notifications required when an AVR goes out of service and quickly comes back in service. Such notifications provided little to no benefit to reliability. Fifteen (15) minutes have been built into the requirement to allow a GOP time to resolve an issue before having to notify the TOP of a status or capability change. The requirement has also been amended to remove the sub-requirement to provide an estimate for the expected duration of the status change. The 15-minute window should resolve most issues.

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within the first 15 minutes of such change, then there is

no need to notify the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of the change identified in Requirement R3. If the status has been restored within the first 15 minutes, no notification is necessary; therefore, if a status change lasts more than 15 minutes, the GOP must notify its associated Transmission Operator within 30 minutes of when the change first occurred.

Rationale for R4:

This requirement has been bifurcated from the earlier Requirement R3. This requirement allows GOPs to report reactive capability changes after they are made aware of the change. The current standard requires notification as soon as the change occurs, but many GOPs are already in non-compliance situations by the time it is known that a reactive capability change has taken place.

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes after becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within the first 15 minutes of such change, then there is no need to notify the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of the recognition of a reactive capability change identified in Requirement R4. If the capability has been restored within the first 15 minutes, no notification is necessary; therefore, if a capability change lasts more than 15 minutes, the Generator Operator must notify its associated Transmission Operator within 30 minutes of when the change first occurred.

Rationale for R5:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected. The original sub-requirement 4.1.4 (the +/- voltage range with step-change in % for load-tap changing transformers) has been removed.

R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

5.1. For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

5.1.1. Tap settings.

5.1.2. Available fixed tap ranges.

5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirements R5 part 5.1.1 through part 5.1.3.

Rationale for R6:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

6.1. If the Generator Operator cannot comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation as identified in Requirement R6. The Generator Operator shall have evidence that it notified its associated Transmission Operator when it could not comply with the Transmission Operator's step-up transformer tap specifications as identified in Requirement R6 part 6.1.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. The Generator Operator shall maintain all other evidence for the current and previous calendar year.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Real-time Operations**	**Medium**	N/A	N/A	N/A	Unless exempted, the responsible entity did not operate each generator in the automatic voltage control mode and failed to notify the Transmission Operator as identified in Requirement R1.
R2	**Real-time Operations**	**Medium**	N/A	N/A	The responsible entity did not have conversion methodology when it monitors voltage at a location different from the schedule provided by the Transmission Operator.	The responsible entity did not maintain voltage or Reactive schedule as directed by the Transmission Operator and did not make the necessary notifications required by the Transmission Operator. OR The responsible entity did not have an operating AVR, and the responsible entity did not use an alternative method for controlling voltage. OR The responsible entity did not modify voltage when directed, and the responsible entity did not provide any explanation.
R3	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The responsible entity did not make the notification within 30 minutes.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The responsible entity did not make the notification within 30 minutes.
R5	**Real-time Operations**	**Lower**	N/A	N/A	The responsible entity failed to provide to its associated Transmission Operator and Transmission Planner one of the types of data specified in Requirements R5 parts 5.1.1 and 5.1.2 and 5.1.3.	The responsible entity failed to provide to its associated Transmission Operator and Transmission Planner two or more of the types of data specified in Requirements R5 parts 5.1.1 and 5.1.2 and 5.1.3.
R6	**Real-time Operations**	**Lower**	N/A	N/A	N/A	The Generator Owner did not ensure the tap changes were made according the Transmission Operator's specifications. OR The Generator Operator failed to perform the tap changes, and the

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Generator Operator did not provide technical justification for why it cannot comply with the Transmission Operator directive.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR and supporting package posted for comment on July 19~~XX~~, 2013.
2. Draft standard posted for initial comments and ballot from July 19, 2013 to September 3, 2013.

Description of Current Draft

This is the second posting of the proposed draft standard. This proposed draft standard will be posted for a 45-day formal comment period and parallel ballot.~~This draft standard is concluding informal development and will move to formal development when authorized by the Standards Committee.~~

Anticipated Actions	Anticipated Date
~~SAR Authorized by the Standards Committee~~	~~July~~
Additional 45-~~-~~Day SAR Comment Period with~~and Initial~~ Ballot ~~Open~~	October/November 2013~~July~~
~~Nomination Period Opens~~	~~July~~
~~Standard Drafting Team Appointed~~	~~July~~
~~Initial Comment and Initial Ballot Closes~~	~~August~~
Final Ballot ~~Opens~~	December 2013~~October~~
~~Final Ballot Closes~~	~~October~~
NERC Board of Trustees~~BOT~~ Adoption	December 2013~~November~~
Filing to Applicable Regulatory Authorities	December 2013

~~Effective Dates~~

~~In those jurisdictions where regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter after applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter after Board of Trustees approval.~~

Version History

Version	Date	Action	Change Tracking
1	5/1/2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and 2.4.3.	July 5, 2006
1a	12/19/2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	1/16/2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	Errata
1.1a	10/29/2008	BOT adopted errata changes; updated version number to "1.1a"	Errata
1.1b	3/3/2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	Revised
2b	4/16/2013	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4. FERC Order issued approving VAR-002-2b.	Revised

Definitions of Terms Used in the Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None.

A. Introduction

1. Title: **Generator Operation for Maintaining Network Voltage Schedules**

2. Number: VAR-002-3

3. Purpose: To ensure generators provide reactive support and voltage control, ~~necessary to ensure voltage levels, reactive flows, and reactive resources are maintained~~ within generating~~applicable~~ Facility capabilities, in order~~Ratings~~ to protect equipment and maintain~~the~~ reliable operation of the Interconnection.

4. Applicability:

4.1. Generator Operator

4.2. Generator Owner

5. Effective Dates

~~All requirements~~The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

Rationale for R1: This requirement has been maintained due to the importance of running a unit with its automatic voltage regulator (AVR) in service and in voltage controlling mode. However, the requirement has been modified to allow for testing, and the measure has been updated to include some of the evidence that can be used for compliance purposes.

~~**Rationale for R1:** This requirement has been maintained due to the importance of running a unit with its automatic voltage regulator (AVR) in service and in voltage controlling mode. The measure has been updated include some of the evidence that can be used for Compliance purposes.~~

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless the Generator Operator 1) is exempted by the Transmission Operator, or 2) has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- That the generator is being operated in start-up,[1] ~~or~~ shutdown,[3] or testing[4] mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in the automatic voltage control mode for a reason other than start-up, ~~or~~ shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode as specified in Requirement R1~~1~~. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR~~automatic voltage regulator~~ status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode. Such evidence must include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If exempted, the Generator Operator shall also have evidence that it is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.

~~[2] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.~~

[3] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

Rationale for R2:

Requirement R2 details how a Generator Operator (GOP) operates the system to maintain a voltage schedule and when the GOP is expected to notify the Transmission Operator (TOP). In an effort to remove prescriptive notification requirements for the entire continent, the VAR standard drafting team (SDT) opted to allow each TOP to determine the notification requirements for each of its respective GOPs based on system requirements. A new part 2.3 has been added to detail that each GOP shall monitor voltage based on its existing facility equipment.

Conversion Methodology: There are many ways to convert the voltage schedule from one voltage level to another. Some entities may choose to develop voltage regulation curves for their transformers; others may choose to do a straight ratio conversion; others may choose an entirely different methodology. All of these methods have technical challenges, but the studies performed by the TOP, which consider N-1 and credible N-2 contingencies, should compensate for the error introduced by these methodologies, and the TOP possesses the authority to direct the GOP to modify its output if its performance is not satisfactory. During a significant system event, such as a voltage collapse, even a generation unit in automatic voltage control that controls based on the low-side of the generator step-up transformer should see the event on the low-side of the generator step-up transformer and respond accordingly.

Voltage Schedule Tolerances: The bandwidth that accompanies the voltage target in a voltage schedule should reflect the anticipated fluctuation in voltage at the GOP's Facility during normal operations and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a GOP's AVR control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

~~**Rationale for R2:**~~

~~R2 details how a Generator Operator (GOP) operates the system to a maintain voltage schedule and when the GOP is expected to notify the Transmission Operator (TOP). Sub-requirement 2.1 provides guidance on a non-compliance window in the event a unit is deviating from schedule, and the GOP must notify the TOP if it is unable to return to schedule. Thus, the non-compliance window allows for notifications when a unit is unable to provide additional VAR support (e.g., when hitting an operational limit) or when the unit is too small to raise voltage. In both instances, the TOP may then provide some type of temporary exemption as outlined in VAR-001.~~

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[5] (within each generating Facility's capabilities[6]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage schedule provided by the Transmission Operator.~~applicable Facility Ratings[7]) as directed by the Transmission Operator.~~ *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

~~**2.1.** If a GOP drifts out of schedule, each Generator Operator shall notify its associated Transmission Operator within 15 minutes when both of the following conditions are met: 1) the GOP is operating outside of the prescribed voltage or Reactive Power schedule tolerance band[8] for 15 minutes; and 2) the GOP is no longer able to return to its voltage or Reactive Power schedule.~~

~~2.2.~~2.1. When a generator's AVR~~automatic voltage regulator~~ is out ~~-~~of ~~-~~service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.

~~2.3.~~2.2. When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a unit is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage schedule.

For part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.

---

[5] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator~~ establishing a tolerance band within which the target value is to be maintained during a specified period~~.

[6] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a Generator is operating in manual control, reactive power capability may change based on stability considerations.

~~[7] When a Generator is operating in manual control, reactive power capability may change based on stability considerations and this may lead to a change in the associated Facility Ratings.~~

~~[8] GOPs monitor and control voltage based on their equipment limitations. GOPs will monitor their voltage or Reactive Power schedule tolerance bands either at the high side or low side/terminal voltage.~~

For part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's directions to modify its voltage or provided an explanation of why the Generator Operator was unable to comply with the direction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

~~**M2.**~~ For part 2.3, for units that do not monitor the voltage at the location specified on the voltage schedule the Generator Operator shall document or be able to demonstrate the method of conversion from the voltage level monitored to the voltage level specified on the voltage schedule.~~Generator Operators will still make all attempts to operate within the tolerance bands provided by the TOP, but natural drifting may occur. In instances where there is an event occurring to pull a unit out of the tolerance band, the Generator Operator will not be held in non-compliance with this requirement if the sub-requirements 2.1, 2.2, and 2.3 are met. In order to identify when a unit is deviating from its schedule, GOPs will monitor voltage based on existing equipment at its facility. Therefore, GOPs have the option to operate on a voltage schedule on either the high-side or convert the high-side schedule to a low-side schedule at the GOP's discretion. For units that monitor on the low-side/terminal voltage, Generator Operators shall provide evidence of the method of conversion from the high-side schedule to low-side monitoring. For sub-requirement 2.1, most units will not be able to return to schedule due to a limiting factor. Such limiting factors may include, but are not limited to: 1) terminal voltage, 2) bus voltage, 3) equipment temperature, 4) transformer, 5) auxiliary equipment, 6) Volts/Hz limits, and 7) excitation or regulator limits. GOP shall have evidence to show compliance with requirement R2 by providing 1) Communications with the TOP when the Generator Operator was operating outside of the prescribed voltage or Reactive Power schedule tolerance band for 30 minutes or less (the 30 minutes allow for 15 minutes to call and 15 minutes to be outside of the tolerance band) AND Generator Operator is no longer able to return to its voltage or Reactive Power schedule; 2) Generator Operator implemented an alternative method to control reactive output when the AVR was out-of-service or unavailable; 3) compliance with directive to modify voltage or a notification that the directive could not be met. Evidence may include, but is not limited to Generator Operator logs, SCADA data, phone logs, and any other alarming notifications that would alert the Transmission Operator that both conditions were met. Timing for Requirement R2.1 is crucial, and Generator Operators are expected to begin timing an event as soon as the unit is operating outside of the tolerance band. Further, voltage documentation during a system event maybe requested by an auditor to show measures were taken to bring the unit back into schedule.

Rationale for R3:

This requirement has been modified to limit the notifications required when an AVR goes out of service and quickly comes back in service. Such notifications provided little to no benefit to reliability. Fifteen (15) minutes have been built into the requirement to allow a GOP time to resolve an issue before having to notify the TOP of a status or capability change. The requirement has also been amended to remove the sub-requirement to provide an estimate for the expected duration of the status change. The 15-minute window should resolve most issues.

~~**Rationale for R3:**~~

~~This requirement has been modified to reduce the number of violations for when an AVR goes out of service and then comes back in service. Fifteen (15) minutes have been built into the requirement to allow a Generator Operator time to resolve an issue before having to notify the Transmission Operator of a status or capability change. The requirement has also been amended to remove the sub-requirement to provide an estimate for the expected duration of the status change. The 15-minute window should resolve most issues, and further trouble-shooting will probably be required if the status change is unresolved within 15 minutes.~~

R3. Each Generator Operator shall notify its associated Transmission Operator of a status ~~or capability~~ change on the AVR,~~any generator Reactive Power resource, including the status of each automatic voltage regulator and~~ power system stabilizer, or alternative voltage controlling device~~ and the expected duration of the change in status or capability~~ within 30 minutes of the change. If the status has been restored within the first 15 minutes of such change, then there is no need to notify~~call~~ the Transmission Operator~~TOP~~. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of ~~any of~~ the change~~changes~~ identified in Requirement R3~~3~~. If the status has been restored within the first 15 minutes, no notification~~call~~ is necessary; therefore, if a status ~~on Reactive Power resource has changed, and that~~ change lasts more~~greater~~ than 15 minutes, the GOP must notify its associated Transmission Operator~~TOP~~ within 30 minutes of when the change first occurred.

~~**Rationale for R4:**~~

~~This requirement and corresponding measure language has been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.~~

Rationale for R4:

This requirement has been bifurcated from the earlier Requirement R3. This requirement allows GOPs to report reactive capability changes after they are made aware of the change. The current standard requires notification as soon as the change occurs, but many GOPs are already in non-compliance situations by the time it is known that a reactive capability change has taken place.

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes after becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within the first 15 minutes of such change, then there is no need to notify the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of the recognition of a reactive capability change identified in Requirement R4. If the capability has been restored within the first 15 minutes, no notification is necessary; therefore, if a capability change lasts more than 15 minutes, the Generator Operator must notify its associated Transmission Operator within 30 minutes of when the change first occurred.

Rationale for R5:

This requirement and corresponding measure language has been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

Rationale for R5:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected. The original sub-requirement 4.1.4 (the +/- voltage range with step-change in % for load-tap changing transformers) has been removed.

~~R4.~~R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

~~4.1.~~5.1. For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

~~4.1.1.~~5.1.1. Tap settings.

~~4.1.2.~~5.1.2. Available fixed tap ranges.

~~4.1.3.~~5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirements R5 part 5~~4~~.1.1 through part 5~~4~~.1.3.

Rationale for R6:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

~~R5.~~R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]~~].~~*

~~5.1.~~6.1. If the Generator Operator cannot~~can't~~ comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation as identified in Requirement R6~~5~~. The Generator Operator shall have evidence that it notified its associated Transmission Operator when it could not~~couldn't~~ comply with the Transmission Operator's step-up transformer tap specifications as identified in Requirement R6 part 6~~5~~.1.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to~~means~~ NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. The Generator Operator shall maintain all other evidence for the current and previous calendar year.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Real-time Operations	Medium	N/A	N/A	N/A	Unless exempted, the~~The~~ responsible entity did not operate each generator in the automatic voltage control mode and failed to notify the Transmission Operator as identified in Requirement R1.
~~R2~~	~~Real-time Operations~~	~~Medium~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The responsible entity did not perform any of the sub-requirements.~~
~~R3~~	~~Real-time Operations~~	~~Medium~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The responsible entity did not make the notification within 30 minutes.~~
R2~~R4~~	Real-time Operations	Medium~~Lower~~	N/A ~~When directed by the Transmission Operator to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for up to and including 45 minutes.~~	N/A~~When directed by the Transmission Operator to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for more than 45 minutes up to and including 60~~	The responsible entity did not have conversion methodology when it monitors at a location different from the schedule provided by the Transmission Operator.~~When directed by the Transmission Operator to maintain the~~	The responsible entity did not maintain voltage or Reactive schedule as~~When~~ directed by the Transmission Operator and did not make ~~to maintain~~ the necessary notifications required by the Transmission Operator~~generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for more than 75 minutes~~. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~minutes.~~ ~~OR~~ ~~When a generator's automatic voltage regulator is out of service, the Generator Operator failed to use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.~~ ~~OR~~ ~~The Generator Operator failed to provide an explanation of why the voltage schedule could not be met.~~	~~generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for more than 60 minutes up to and including 75 minutes.~~	The responsible entity did not have an operating AVR, and the responsible entity did not~~When a generator's automatic voltage regulator is out of service, the Generator Operator failed to~~ use an alternative method for controlling voltage. OR The responsible entity did not modify~~to control the generator~~ voltage when directed, and the responsible entity did not~~and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator and the Generator Operator failed to~~ provide anyan explanation. ~~of why the voltage schedule could not be met.~~
R3	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The responsible entity did not make the notification within 30 minutes.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	Real-time Operations	Medium	N/A	N/A	N/A	The responsible entity did not make the notification within 30 minutes.
R5	Real-time Operations	Lower	N/A	N/A	The responsible entity failed to provide to its associated Transmission Operator and Transmission Planner one of the types of data specified in Requirements R5 parts 5.1.1 or 5.1.2 or 5.1.3.	The responsible entity failed to provide to its associated Transmission Operator and Transmission Planner two or more of the types of data specified in Requirements R5 parts 5.1.1 and 5.1.2 and 5.1.3.
R6~~R5~~	Real-time Operations	Lower	N/A	N/A	N/A	The Generator Owner did not ensure the tap changes were made according the Transmission Operator's specifications. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Generator Operator~~GOP~~ failed to perform the tap changes, and the Generator Operator~~GOP~~ did not provide technical justification for why it cannot comply with the Transmission Operator~~TOP~~ directive.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please review~~see~~ the rationale provided~~VAR White Paper~~ for each requirement. ~~further technical information.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

VAR Directives Project

Implementation Plan for VAR-001-4 and VAR-002-3

Approvals Required

VAR-001-4 – Voltage and Reactive Control
VAR-002-3 — Generator Operation for Maintaining Network Voltage Schedules

Prerequisite Approvals

There are no other standards that must receive approval prior to the approval of this standard.

Revisions to Glossary Terms

None

Applicable Entities

Generator Operators (VAR-002-3)

Generator Owners (VAR-002-3)

Transmission Operators (VAR-001-4)

Applicable Facilities

N/A

Conforming Changes to Other Standards

None

Effective Dates

VAR-001-4 and VAR-002-3 – All requirements shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-001-4 and VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Justification

The currently effective VAR-002 standard is one of the most violated standards; however, the industry argues these violations do not address any reliability gaps. Instead, Generator Operators and Transmission Operators are required to handle many nuisance phone calls for slight deviations from a voltage schedule. The nuisance phone calls can be a distraction during a scheduled maintenance or a system event; thus, the industry would support making the changes as soon as possible. However, since VAR-001 now requires determining voltage and reactive power schedules with associated tolerance bands in addition to any notification requirements, the Transmission Operators need a quarter to prepare documentation. The VAR-002 standards cannot go into effect without the new TOP schedules and notification requirements. Also for Transmission Operators that do not already provide tolerance bands with voltage schedules, those Transmission Operators will need some time to adjust to providing new data (more specifically, the criteria for schedules) to Generator Operators.

Retirements

VAR-001-3 and VAR-002-2b will be retired at midnight of the day immediately prior to the Effective Date of VAR-001-4 and VAR-002-3 in the particular jurisdiction in which the new standards are becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

VAR Directives Project

Implementation Plan for VAR-001 and VAR-002

Approvals Required

VAR-001-4 – Voltage and Reactive Control
VAR-002-3 — Generator Operation for Maintaining Network Voltage Schedules

Prerequisite Approvals

There are no other standards that must receive approval prior to the approval of this standard.

Revisions to Glossary Terms

None

Applicable Entities

Generator Operators (VAR-002-3)

Generator Owners (VAR-002-3)

Transmission Operators (VAR-001-4)

~~Reliability Coordinators~~

Applicable Facilities

N/A

Conforming Changes to Other Standards

None

Effective Dates

VAR-001-4 and VAR-002-3 – All requirements ~~- In those jurisdictions where regulatory approval is required, this standard~~ shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority ~~regulatory approval~~ or as otherwise provided for in a jurisdiction where approval by an~~made effective pursuant to the laws~~ applicable ~~to such ERO~~ governmental authority~~authorities. In those jurisdictions where no regulatory approval~~ is required for a~~, this~~ standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-001-4 and VAR-002-3 shall become effective on the first

day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction~~approval~~.

Justification

The currently effective VAR-002 standard is one of the most violated standards; however, the industry argues these violations do not address any reliability gaps. Instead, Generator Operators and Transmission Operators are required to handle many nuisance phone calls for slight deviations from a voltage schedule. The nuisance phone calls can be a distraction during a scheduled maintenance or a system event; thus, the industry would support making the changes as soon as possible. However, since VAR-001 now requires determining voltage and reactive power schedules with associated tolerance bands in addition to any notification requirements~~a documented policy or procedure for assessments~~,~~;~~ the Transmission Operators need a quarter to prepare documentation. The VAR-002 standards cannot go into effect without the new TOP schedules and notification requirements. Also for Transmission Operators that do not already provide tolerance bands with voltage schedules, those Transmission Operators will need some time to adjust to providing new data (more specifically, the criteria for schedules) to Generator Operators.

Retirements

VAR-001-3 and VAR-002-2b will be retired at midnight of the day immediately prior to the Effective Date of VAR-001-4 and VAR-002-3 in the particular j~~J~~urisdiction in which the new standards are becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2013-04 Voltage and Reactive Control (VAR) Revisions

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments on the draft VAR-001-4 and VAR-002-3 standards. The electronic comment form must be completed by 8:00 p.m. ET by **November 25 , 2013**.

If you have questions please contact Soo Jin Kim via email or by telephone at 404-446-9742.

The project page may be accessed by clicking here.

Background Information

When the first versions of the VAR standards were approved in FERC Order No. 693,[1] the Commission also issued FERC issued several directives with regard to how to improve the standard. Each of the outstanding directives are explained in detail in the technical white paper (see project page).

The informal consensus building for VAR began in February 2013. Specifically, the ad hoc group engaged stakeholders on how best to address the FERC directives, remove paragraph 81 candidates, and implement results-based approaches. A discussion of the ad hoc group's consensus building and collaborative activities are also included in the technical white paper.

Project 2013-04 posted an initial draft for comment and ballot form July 19, 2013 to September 3, 2013. Although the VAR standards did not pass, the industry provided numerous helpful coments, and the standard drafting team made significant revisions based on the stakeholder input.

The proposed VAR-001 answers most of the FERC directives from Order No. 693, and the VAR-002 has been modified to address certain compliance issues today. Some directives are not being addressed at this time pending FERC determiniations in related filings, but those directives may be revisted during a phase 2 of this project. This posting is now soliciting comment on the revised VAR-001 and VAR-002 standards.

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

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

Question

1. Although FERC directed NERC to provide more details on "established limits," the VAR standards development team determined that the FAC and TOP standards provide explicit requirements on voltage limits. Further, the definition of a System Operating Limit requires Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits) to be included. Is it clear that the specifics with regard to voltage limits are to be determined and monitored as part of operating within System Operating Limits and Interconnection Reliability Operating Limits?

☐ Yes
☐ No

Comments:

2. Several requirements were removed because they duplicated other standards. Do you agree with this approach? Do you have any specific questions or comments relating to the requirements in the revised VAR-001-4?

☐ Yes
☐ No

Comments:

3. VAR-002 was modified to remove several compliance issues, and in order to address burdensome notification requirements, the VAR-001 standard has been modified to allow each TOP to tailor notification requirements based on system/area needs. Do you agree with these revisions?

☐ Yes
☐ No

Comments:

4. The VRFs/VSLs for VAR-002 were modified to remove arbitrary time requirements. Do you have any specific comments or questions about the new VSLs/VRFs?

Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Operations

Draft Reliability Standard Compliance Guidance for VAR-001-4 and VAR-002-3
October 21, 2013

Introduction

The NERC Compliance department (Compliance) worked with the VAR standard drafting team (SDT) to review the proposed standards VAR-001-4 and VAR-002-3. The purpose of the review was to discuss the requirements of the proposed standard to obtain an understanding of its intended purpose and the evidence necessary to support compliance. The purpose of this document is to address specific questions posed by the VAR SDT in order to aid in the drafting of the requirements and provide a level of understanding regarding evidentiary support necessary to demonstrate compliance.

While all compliance evaluations require levels of auditor judgment, participating in these reviews allows Compliance to develop training and approaches to support a high level of consistency in audits conducted by the Regional Entities. The following questions and answers are intended to assist the SDT in further refining the standard and to serve as a resource in the development of training for auditors.

VAR-001 and VAR-002 Questions

Question 1

How will compliance determine if sufficient reactive resources were scheduled as part of VAR-001-4 Requirement R2?

Compliance Response to Question 1

For VAR-001-4 Requirement R2, an auditor would review the studies that a TOP used to schedule resources to see that the studies show whether new resources should be brought online, or if the resources online are sufficient to regulate voltage levels. An auditor may observe a TOP reviewing the study and scheduling live and may pull samples from various time periods to determine whether a TOP scheduled resources as required in the study.

Question 2

Is it clear that VAR-001-4 Requirement R4 allows for exemptions, for any duration, from: 1) voltage schedules, 2) being in automatic voltage control mode, or 3) any notification requirements?

Compliance Response to Question

It is clear that VAR-001 Requirement R4 allows for any combination of exemptions for generator operators from 1) voltage schedules, 2) being in automatic voltage control mode, or 3) any notification requirements, as long as the

exemption meets the criteria specified by the TOP. An auditor will not look for any pre-authorization from the TOP; rather an auditor will verify that the generator operator has met the criteria set forth by the TOP.

Question 3

Tolerance bands apply to a set voltage or Reactive Power number with a +/- percentage as the tolerance band. The voltage range or Reactive Power range is a high and low number that a Generator Operator is expected to operate within for reliability purposes. With regard to VAR-001-4 Requirement R5, is it clear that when a voltage range or Reactive Power range is provided as a schedule, a tolerance band is not expected to also be provided?

Compliance Response to Question 3

Yes, it is clear based on VAR-001-4 Requirement R5 that a voltage or Reactive power schedule can be either: 1) a target number with a tolerance band, OR 2) a voltage or Reactive Power range to operate within. An auditor would not expect to see a tolerance band provided with an operating range for voltage or Reactive Power.

Question 4

With regard to VAR-002-3, will generators receive a violation for instances where a system event is affecting system voltage, but the generators made the appropriate conversions and set the AVRs to meet the original schedule provided by the TOP?

Compliance Response to Question 4

No, the generator operators can only be responsible for maintaining the schedule provided by the TOP based on existing facility equipment. In the event that a generator operator does not have the equipment to have visibility of high-side system voltage, the GOP will not have the ability to adjust VARs to maintain system voltage. An auditor is not to determine that, where the GOP does not have the high side monitoring equipment and where the AVR is set appropriately based on existing facility equipment, the generator operator is non-compliant. However, if the TOP provides a new directive or schedule, the GOP is required to follow the new directive. This directive can include modifying an AVR setting or providing more voltage support, and the generator operator is expected to comply pursuant to VAR-002-3.

Question 5

Related to VAR-002-3, generators can monitor voltage on either the low side and high side of the GSU (depending on equipment limitation) and the “number” being monitored by the Generator will not always equate to the number provided by the TOP. Is it clear that VAR-002 Requirement R2, part 2.3 only wants a conversion of the schedule provided to the number monitored? Is it clear that there should not be a violation if the schedule does not match the number being monitored on the low side as long as there is a documented conversion?

Compliance Response to Question 5

The Generator should be able to provide documentation that identifies the "number" being monitored and the calculation demonstrating how the "number" equates to the schedule provided by the TOP. The measure for VAR-002-3 Requirement R2, part 2.3 is clear on what evidence should be able to demonstrate this during an audit.

Question 6

VAR-002-3, Requirement R4 was added because generators cannot report a capability change until they are aware of the change. The currently enforceable standard requires a notification as soon as the capability change occurs; however, many times the change occurred well before the generators were aware of the problem. Is it clear that VAR-002-3 Requirement R4 is only violated after the generator is made aware of the change?

Compliance Response to Question 6

It is clear that VAR-002-3, Requirement R4 will only be a violation if the change is not reported after 30 minutes of becoming aware of the reactive capability change. An auditor will ask an entity for evidence to demonstrate when it became aware of the change in reactive capability. This will not be purely subjective; there are technical instances where it will be clear that an entity would have been made aware of the change in reactive capability. For example, one instance is where a unit is ramping to an expected VAR output, and it cannot reach it; a reactive capability change has occurred.

Conclusion

Following final approval of the Reliability Standard, Compliance will develop the final Reliability Standards Auditor Worksheet (RSAW) and associated training.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VAR Mapping Document

Transition of VAR-001-3 and VAR-002-2b

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R1	Requirement R1	This requirement is duplicated in other standards, and the new requirement has been simplified to require the specification of the voltage and Reactive Power schedules and associated tolerance bands. A new part 1.1 has been added to allow for voltage coordination with adjacent TOPs and applicable RCs.
VAR-001-3 R2	Requirement R2	The new requirement has been updated to scheduling of resources. It eliminates the need for the existing R7, R8, and R9. It also maintains a list of sufficient reactive resources.
VAR-001-3 R3	Requirement R4	The new requirement has been simplified by removing the need to maintain an exemption list. Instead, the standard focuses on whether the exemption criteria are known and whether a granted exemption was communicated to the applicable Generator.

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R4	Requirement R5	The new requirements have been updated to allow the TOP to provide the voltage or Reactive Power schedule at either the high side or the low side of the GSU. Also as tolerance band is now required under the new requirement. New parts have also been added to direct a GOP to operate in AVR, to require the TOP to provide notification requirements, and to provide the criteria for developing schedules and tolerance bands upon request.
VAR-001-3 R5	Deleted	Pending a final rulemaking on P81, this requirement has been deleted.
VAR-001-3 R6	Deleted	This requirement is deleted because the TOP standards require knowing the status of Reactive Power resources. Although power system stabilizers are not specifically named in the TOP standards, the areas that rely on PSS equipment will require monitoring the status under the data specifications of the TOP standards.
VAR-001-3 R7	Deleted	This has moved into the new R3.
VAR-001-3 R8	Deleted	This has moved into the new R3.
VAR-001-3 R9	Deleted	See comments for new R2.
VAR-001-3 R10	Deleted	This is duplicative of TOP-001-2 and the Tv definition.
VAR-001-3 R11	Requirement R6	The requirement has been updated to allow for scheduling consultation.
VAR-001-3 R12	Deleted	This requirement was deleted because the EOP standards address taking any corrective action including load-shedding. Also the new TOP-002-3 R2 and TOP-001-2 R11 address the TOP taking corrective actions.

Standard: VAR-002-3 – Capacity Benefit Margin		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b R1	Requirement R1	The requirement has been modified to allow for testing and exemptions for other AVR modes when necessary.
VAR-002-2b R2	Requirement R2	The new requirement has been updated to allow for TOP-defined notification requirements. The requirement also adds parts to allow for the conversion of a high side schedule to a low side number for monitoring purposes.
VAR-002-2b R3	Requirement R3 and R4.	The old requirement has been broken into two requirements: 1) one for AVR/PSS status, and 2) one for reactive capability. Both allow 15 minutes to correct an issue before having to notify the TOP.
VAR-002-2b R3	Requirement R4	The requirement has not been modified.
VAR-002-2b R4	Requirement R5	The requirement has not been modified.

VAR Mapping Document

Transition of VAR-001-3 and VAR-002-2b ~~(the *pro forma* standard)~~

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R1	Requirement R1	This requirement is duplicated in other standards,~~The *pro forma* creates adds additional sub-requirements that requires the policies~~ and the new requirement has been simplified~~procedures~~ to require the specification of the~~include criteria for system assessments. The assessments must now include steady-state limits,~~ voltage and Reactive Power schedules ~~stability limits~~ and associated ~~operating margins, and voltage schedules along with associated~~ tolerance bands. A new part 1.1 has been added to allow for voltage coordination with adjacent~~The sub-requirements also now mandate that information is shared with neighboring~~ TOPs and ~~the~~ applicable RCs~~RC~~.
VAR-001-3 R2	Requirement R2	The new requirement has been updated to ~~incorporate real-time and day-ahead~~ scheduling of resources. It eliminates the need for the existing R7, R8, and R9. It also maintains a list of sufficient reactive resources.

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R3	Requirement R4~~R3~~	The new requirement has been simplified by removing the need to maintain an exemption list. Instead, the standard focuses on whether the exemption criteria are known and whether a granted exemption was communicated to the applicable Generator.
VAR-001-3 R4	Requirement R5~~R4~~	The new requirements have been updated to allow the TOP to provide the voltage or Reactive Power schedule at either the high side or the low side of the GSU. Also as tolerance band is now required under the new requirement. New parts have also been added to direct a GOP to operate in AVR, to require the TOP to provide notification requirements, and to provide the criteria for developing schedules and tolerance bands upon request.
VAR-001-3 R5	Deleted	Pending a final rulemaking on P81, this requirement has been deleted.
VAR-001-3 R6	Deleted~~Requirement R5~~	This requirement is deleted because the TOP standards require knowing the status of Reactive Power resources. Although power system stabilizers are not specifically named in the TOP standards, the areas that rely on PSS equipment will require monitoring the status under the data specifications of the TOP standards.~~The sub-requirement R6.1 was deleted because it is duplicative of VAR-002's requirement R1 and R2.~~
VAR-001-3 R7	Deleted	This has moved into the~~See comments for~~ new R3~~R2~~.
VAR-001-3 R8	Deleted	This has moved into the~~See comments for~~ new R3~~R2~~.
VAR-001-3 R9	Deleted	See comments for new R2.
VAR-001-3 R10	Deleted	This is duplicative of TOP-001-2 and the Tv definition.

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R11	Requirement R6	The requirement has been updated to allow for scheduling consultation.~~The only change is the numbering due to other deletions.~~
VAR-001-3 R12	Deleted	This requirement was deleted because the EOP standards address taking any corrective action including load-shedding. Also the new TOP-002-3 R2 and TOP-001-2 R11 address the TOP taking corrective actions.

Standard: VAR-002-3 – Capacity Benefit Margin		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b R1	Requirement R1	The requirement has ~~not~~ been modified to allow for testing and exemptions for other AVR modes when necessary.
VAR-002-2b R2	Requirement R2	The new ~~*pro forma*~~ requirement has been updated to allow for TOP-defined notification requirements. The ~~by including a new sub-~~ requirement also adds parts~~to allowing GOPs~~ to allow for the conversion of a high side schedule to a low side number for monitoring purposes~~only call in certain instances when deviating from voltage schedules~~.
VAR-002-2b R3~~R2~~	Requirement R3 ~~-~~and R4.	The old~~new *pro forma*~~ requirement has been broken into two requirements: 1) one for AVR/PSS ~~updated by including a new sub-requirement to allowing GOPs to investigate why the~~ status, and 2) one for reactive capability. Both allow 15 minutes to correct an issue~~has changed on AVR equipment~~ before having to notify the TOP.

Standard: VAR-002-3 – Capacity Benefit Margin		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b R3~~R2~~	Requirement R4	The requirement has not been modified.
VAR-002-2b R4~~R2~~	Requirement R5	The requirement has not been modified.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Reliability Standard Audit Worksheet[1]

VAR-001-4 – Voltage and Reactive Control

This section to be completed by the Compliance Enforcement Authority.

Audit ID: Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity: Registered name of entity being audited
NCR Number: NCRnnnnn
Compliance Enforcement Authority: Region or NERC performing audit
Compliance Assessment Date(s)[2]: Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method: Audit
Names of Auditors: Supplied by CEA

Applicability of Requirements *[RSAW developer to insert correct applicability]*

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1													X		
R2													X		
R3													X		
R4													X		
R5													X		
R6													X		

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Subject Matter Experts

Identify Subject Matter Expert(s) responsible for this Reliability Standard. (Insert additional rows if necessary)

Registered Entity Response (Required):

SME Name	Title	Organization	Requirement(s)

DRAFT

R1 Supporting Evidence and Documentation

R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.

1.1. Each Transmission Operator shall provide a copy of the voltage schedules and associated tolerance bands to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.

M1. The Transmission Operator shall have evidence that it specified system voltage schedules using either a range or a target value with an associated tolerance band.

For part 1.1, the Transmission Operator shall have evidence that the voltage schedules were provided to its Reliability Coordinator and adjacent Transmission Operators within 30 days of a request. Evidence may include, but is not limited to, emails, website postings, and meeting minutes.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[3]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M1.
Documentation of request made per Part 1.1 from Reliability Coordinator and/or adjacent Transmission Operators, if applicable and requested by auditor.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

[3] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-001-4, R1
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R1) Review evidence provided and ensure it meets the requirements outlined in Requirement R1.
	(Part 1.1) Examine evidence to verify that voltage schedules were provided within 30 days of request per Part 1.1.

Note to Auditor: Auditors, at their discretion and based on the risk of the entity's compliance with this requirement to the BES, may communicate with Balancing Authorities and other Transmission Operators to determine if data requests were made of the entity. Auditors may also accept entity assertions regarding whether data requests made.

Entity assertions that no data requests were made do not have to be in writing.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load.

M2. Each Transmission Operator shall have evidence of scheduling sufficient reactive resources based on their assessments of the system. For the operational planning time horizon, Transmission Operators shall provide copies of assessments used as the basis for how resources were scheduled.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[4]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M2.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-001-4, R2
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Review the studies/assessments that entity used to schedule resources to determine that the studies show whether new resources should be brought online, or if the resources online are sufficient to regulate voltage levels. Auditors should verify that actual scheduling reflected the results of the studies/assessments.

[4] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound, only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough instances, per above, to gain reasonable assurance that entity is complying with Requirement R2.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary.

M3. Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as needed in Real-time. This may include directions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[5]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
Any written policies, procedures or protocols describing how the entity operates or directs devices to regulate transmission voltage and reactive flow as necessary, if the entity has such documents.
Evidence as outlined in M3 as requested by auditor.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location

[5] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-001-4, R3
This section to be completed by the Compliance Enforcement Authority

	Review evidence to understand how entity operates or directs devices to regulate transmission voltage and reactive flow as necessary. Auditors may sample system events or other instances of voltage irregularities to verify that operations or directions occurred as required per Requirement R2.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound, only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough events or other instances of voltage irregularities, per above, to gain reasonable assurance that entity is complying with Requirement R2.

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. The Transmission Operator shall specify the criteria that will exempt generators from compliance with the requirements defined in Requirement R5, part 5.1, and any associated notification requirements.

4.1 If a Transmission Operator determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.

M4. Each Transmission Operator shall have evidence of the documented criteria for generator exemptions.

For part 4.1, the Transmission Operator shall also have evidence to show that, for each generating unit in its area that is exempt from: 1) following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any notifications, the associated Generator Operator was notified of this exemption.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[6]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M4.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-001-4, R4
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R4) Review evidence and note existence of exemption criteria per Requirement R4. For a sample of exempted generators, verify that exemption was granted in accordance with criteria.

[6] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

	(Part 1.1) For a sample of exempted generators, ensure exempted generator was notified.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound, only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough generators, per above, to gain reasonable assurance that entity is complying with Requirement R4.

Requirement R4 allows for any combination of exemptions for generator operators from 1) voltage schedules, 2) being in automatic voltage control mode, or 3) any notification requirements, as long as the exemption meets the criteria specified by the entity. An auditor will not look for any pre-authorization from the entity; rather an auditor will verify that the generator operator has met the criteria set forth by the entity.

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the Generator Step-Up transformer at the Transmission Operator's discretion.

5.1. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).

5.2. The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule.

5.3. The Transmission Operator shall provide the criteria used to develop voltage schedules and associated tolerance bands to the Generator Operator within 30 days of receiving a request.

M5. The Transmission Operator shall have evidence of a documented voltage or Reactive Power Schedule and tolerance band.

For part 5.1, the Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule and tolerance band to the applicable Generator Operators, and that the Generator Operator was directed to comply with the schedule in automatic voltage control mode, unless exempted. The evidence shall include written records, email, or voice recordings.

For part 5.2, the Transmission Operator shall have evidence it provided notification requirements for deviations from the voltage or Reactive Power schedule and associated tolerance band. The evidence shall include written records, email, or voice recordings.

For part 5.3, the Transmission Operator shall have evidence it provided the criteria used to develop voltage schedules and associated tolerance bands within 30 days of receiving a request by a Generator Operator.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[7]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M5.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-001-4, R5
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R5) Verify existence of voltage or Reactive Power schedule and that it meets the requirements of Requirement R5.
	(Part 5.1) For a sample of Generator Operators, verify voltage or Reactive Power schedule was provided

[7] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

	per Part 5.1.
	(Part 5.2) For a sample of Generator Operators, verify the notification requirements for deviations from the voltage or Reactive Power schedule was provided per Part 5.2.
	(Part 5.3) For a sample of Generator Operators, verify criteria was provided as requested per Part 5.3.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound, only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough notifications, per above, to gain reasonable assurance that entity is complying with Requirement R5.

It is clear based on VAR-001-4 Requirement R5 that a voltage or Reactive power schedule can be either: 1) a target number with a tolerance band, Or 2) a voltage or Reactive Power range to operate within. An auditor would not expect to see a tolerance band provided with an operating range for voltage or Reactive Power.

Auditor Notes:

R6 Supporting Evidence and Documentation

R6. After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.

M6. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with the requirement and that it consulted with the Generator Owner.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[8]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.

[8] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

See M6.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-001-4, R6
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Understand entity's procedures concerning coordinating tap settings with Generator Owners per Requirement R6.
	For a sample of Generator Owners, verify tap setting changes were executed per Requirement R6.
Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound, only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough tap setting communications, per above, to gain reasonable assurance that entity is complying with Requirement R6.	

Auditor Notes:

Revision History

Version	Date	Reviewers	Revision Description
1	11/07/2013	NERC compliance, Standards	New Document

DRAFT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Reliability Standard Audit Worksheet[1]

VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules

This section to be completed by the Compliance Enforcement Authority.

Audit ID: Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity: Registered name of entity being audited
NCR Number: NCRnnnnn
Compliance Enforcement Authority: Region or NERC performing audit
Compliance Assessment Date(s)[2]: Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method: Audit
Names of Auditors: Supplied by CEA

Applicability of Requirements *[RSAW developer to insert correct applicability]*

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1				X											
R2				X											
R3				X											
R4				X											
R5			X												
R6			X												

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Subject Matter Experts

Identify Subject Matter Expert(s) responsible for this Reliability Standard. (Insert additional rows if necessary)

Registered Entity Response (Required):

SME Name	Title	Organization	Requirement(s)

DRAFT

R1 Supporting Evidence and Documentation

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless the Generator Operator 1) is exempted by the Transmission Operator, or 2) has notified the Transmission Operator of one of the following:

- That the generator is being operated in start-up,[3] shutdown,[4] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in the automatic voltage control mode for a reason other than start-up, shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode. Such evidence must include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If exempted, the Generator Operator shall also have evidence that it is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

Registered Entity Response to Question (Required):

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[5]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.

[3] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.
[4] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.
[5] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

See M1.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R1
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	For instances where entity did not operate a generator in automatic voltage control mode, ensure notification was given to the Transmission Operator in accordance with Requirement R1.

Note to Auditor: Auditors can identify instances where entities operated generators outside of automatic voltage control mode through their general knowledge of the interconnected transmission system in the entity's area. Auditor knowledge is obtained through activities such as conversations with the entity under audit or the Transmission Operator, and an awareness of events occurring on the interconnected transmission system. In situations where the entity's compliance with this requirement poses little risk to the BES, conversations with other entities, such as Transmission Operators, is most likely not necessary.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[6] (within each generating Facility's capabilities[7]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage schedule provided by the Transmission Operator.

2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.

2.2. When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a unit is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage schedule.

For part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.

For part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's directions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the direction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For part 2.3, for units that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall document or be able to demonstrate the method of conversion from the voltage level monitored to the voltage level specified on the voltage schedule.

Question: As a Generation Operator, have you operated the generator with the AVR out of service?

[6] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.

[7] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a Generator is operating in manual control, reactive power capability may change based on stability considerations.

Registered Entity Response to Question (Required):

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[8]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M2.
Any written policies, procedures or protocols describing how the entity maintains the generator voltage or Reactive Power schedule provided by Transmission Operator, if the entity has such documents.
Generator voltage or Reactive Power schedule provided to entity by Transmission Operator, or entity's record thereof, for timeframes selected by the auditor.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R2
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.

[8] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

	Interview entity staff and/or review documentation provided by the entity to understand how they maintain the generator voltage or Reactive Power schedule or authorized exemption per Requirement R2.
	Read entity's response to compliance Question above and understand how entity complies with Requirement R2, when they operate a generator with AVR in not in service.
	Select a sample of timeframes during the audit period and have entity walkthrough how they complied with Requirement R2 for those timeframes.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough timeframes, per above, to gain reasonable assurance that entity is complying with Requirement R2.

For part 2.3, the entity should be able to provide documentation that identifies the voltage number being monitored and the calculation demonstrating how it equates to the schedule provided by the Transmission Operator. The measure for VAR-002-3 Requirement R2, part 2.3 is clear on what evidence should be able to demonstrate this during an audit. The entity can only be responsible for maintaining the schedule provided by the Transmission Operator based on existing facility equipment. In the event that an entity does not have the equipment to have visibility of high-side system voltage, the entity will not have the ability to adjust VARs to maintain system voltage. An auditor is not to determine that, where the entity does not have the high side monitoring equipment and where the AVR is set appropriately based on existing facility equipment, the entity is non-compliant. However, if the Transmission Operator provides a new directive or schedule, the entity is required to follow the new directive. This directive can include modifying an AVR setting or providing more voltage support, and the entity is expected to comply pursuant to VAR-002-3.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within the first 15 minutes of such change, then there is no need to notify the Transmission Operator.

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of the change identified in Requirement R3. If the status has been restored within the first 15 minutes, no notification is necessary; therefore, if a status change lasts more than 15

minutes, the GOP must notify its associated Transmission Operator within 30 minutes of when the change first occurred.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[9]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
Any written policies, procedures or protocols describing how the entity responds to a status change on AVR, if the entity has such documents. An example of entity's response to a status change on AVR provided by entity, if applicable.
Auditor may select certain instances where entity had a status change on AVR. In such instances, provide associated evidence of awareness and resolution/notification.
Evidence as outlined in M3.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R3
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Interview entity staff and/or review documentation provided by the entity to understand how they

[9] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

	respond to status changes on AVR.
	Review evidence provided to determine if entity responded to status change on AVR in accordance with Requirement R3.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough timeframes, per above, to gain reasonable assurance that entity is complying with Requirement R3.

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes after becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within the first 15 minutes of such change, then there is no need to notify the Transmission Operator.

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of the recognition of a reactive capability change identified in Requirement R4. If the capability has been restored within the first 15 minutes, no notification is necessary; therefore, if a capability change lasts more than 15 minutes, the Generator Operator must notify its associated Transmission Operator within 30 minutes of when the change first occurred.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[10]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means

[10] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

of reduction of the quantity of evidence submitted.
Any written policies, procedures or protocols describing how the entity responds to a change in reactive capability, if the entity has such documents. An example of entity's response to a change in reactive capability provided by entity, if applicable.
Auditor may select certain instances where entity should have been aware of a status change in reactive capability. In such instances, provide associated evidence of awareness and resolution/notification. See Note to Auditor for additional details.
Evidence as outlined in M4.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R4
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Interview entity staff and/or review documentation provided by the entity to understand how they respond to change in reactive capability.
	Review evidence provided to determine if entity responded to change in reactive capability in accordance with Requirement R4.
Note to Auditor: It is clear that VAR-002-3, Requirement R4 will only be a violation if the change is not reported after 30 minutes of becoming aware of the status change in reactive capability. An auditor will ask an entity for evidence to demonstrate when it became aware of the change. This will not be purely subjective; there are technical instances (e.g. unit trips, ramping, equipment/AVR failures) where it will be clear that an entity would have been made aware of the change in reactive capability. For example, one instance is where a unit is ramping to an expected VAR output, and it cannot reach it; a reactive capability change has occurred.	

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request.

5.1. For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

5.1.1. Tap settings.

5.1.2. Available fixed tap ranges.

5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirements R5 part 5.1.1 through part 5.1.3.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[11]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
Evidence as outlined in M4. Evidence of transmittal of the data could include, but is not limited to, items such as an electronic message or a transmittal letter with the information included or attached.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

[11] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

Compliance Assessment Approach Specific to VAR-002-3, R5
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Review evidence (documented date of request and reply) to determine if entity responded to information request(s) as required in Requirement R5 within 30 days of receiving a request from associated Transmission Operator.

Note to Auditor: Based on the auditors professional judgment, he or she may confirm with Transmission Operators to determine if requests for data were made or simply confirm the existence of such requests with the entity under audit.

Auditor Notes:

R6 Supporting Evidence and Documentation

R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement.

6.1. If the Generator Operator cannot comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation as identified in Requirement R6. The Generator Operator shall have evidence that it notified its associated Transmission Operator when it could not comply with the Transmission Operator's step-up transformer tap specifications as identified in Requirement R6 part 6.1.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[12]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M6.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R6
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Review evidence (documented date of request and response) to determine if entity responded to change(s) as required in Requirement R6.
Note to Auditor: Based on the auditors professional judgment, he or she may confirm with Transmission Operators to determine if requests for changes to transformer tap positions were made or simply confirm the existence of such requests with the entity under audit.	

Auditor Notes:

Revision History

Version	Date	Reviewers	Revision Description
1	11/XX/2013	NERC compliance,	New Document

[12] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

		Standards	

DRAFT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-001-4 & VAR-002-3

Comment Period: October 11, 2013 – November 25, 2013

Upcoming:
Additional Ballot and Non-Binding Poll: November 15, 2013 – November 25, 2013

Now Available

A 45-day formal comment period for **VAR-001-4 and VAR-002-3** is open through **8 p.m. Eastern on Monday, November 25, 2013.**

Background information for this project can be found on the project page.

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Monday, November 25, 2013.** Please use the electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Arielle Cunningham. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) will be conducted as previously outlined. During the initial comment period, two ballot pools were formed (one to ballot the standards and one for the non-binding polls). For this ballot and non-binding poll, each standard and its associated non-binding poll will be balloted separately (for a total of two standard ballots and two non-binding polls). The original ballot pools will be used for the individual standard ballots and non-binding polls.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Arielle Cunningham, Standards Development Administrator, at Arielle.Cunningham@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement Reminder

Project 2013-04 Voltage and Reactive Control
VAR-001-4 and VAR-002-3

Additional Ballots and Non-Binding Polls now open through November 25, 2013

Now Available

Additional ballots for **VAR-001-4 and VAR-002-3** and non-binding polls of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) are open through **8 p.m. Eastern on Monday, November 25, 2013.**

Background information for this project can be found on the project page.

Instructions for Commenting
Members of the ballot pools associated with this project may log in and submit their vote for the standards and non-binding polls of the associated VRFs and VSLs by clicking here.

Next Steps
The ballot results for **VAR-001-4 and VAR-002-3** will be announced and posted on the project page. The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the standards. If the comments do not show the need for significant revisions, the standards will proceed to final ballots.

Standards Development Process
The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-001-4 & VAR-002-3

Comment Period: October 11, 2013 – November 25, 2013

Upcoming:
Additional Ballot and Non-Binding Poll: November 15, 2013 – November 25, 2013

Now Available

A 45-day formal comment period for **VAR-001-4 and VAR-002-3** is open through **8 p.m. Eastern on Monday, November 25, 2013.**

Background information for this project can be found on the project page.

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Monday, November 25, 2013.** Please use the electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Arielle Cunningham. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) will be conducted as previously outlined. During the initial comment period, two ballot pools were formed (one to ballot the standards and one for the non-binding polls). For this ballot and non-binding poll, each standard and its associated non-binding poll will be balloted separately (for a total of two standard ballots and two non-binding polls). The original ballot pools will be used for the individual standard ballots and non-binding polls.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Arielle Cunningham, Standards Development Administrator, at Arielle.Cunningham@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-001-4 and VAR-002-3

Additional Ballot and Non-Binding Poll Results

Now Available

Additional ballots for **VAR-001-4 and VAR-002-3** and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels concluded at **8 p.m. Eastern on Tuesday, November 26, 2013.**

VAR-001-4 received sufficient affirmative votes for approval. Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results for the ballots.

	Ballot	Non-Binding Poll
	Quorum /Approval	Quorum/Supportive Opinions
VAR-001-4	80.81% / 69.43%	78.73% / 57.75%
VAR-002-3	81.06% / 66.09%	79.01% / 57.87%

Background information for this project can be found on the project page.

Next Steps

The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the standards. If the comments show the need for significant revisions, the standards will proceed to an additional comment and ballot period. If the comments do not show the need for significant revisions, the standards will proceed to a final ballot.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results	
Ballot Name:	Project 2013-04 Voltage and Reactive Control VAR-001-4 Additional Ballot
Ballot Period:	11/15/2013 - 11/26/2013
Ballot Type:	Additional Ballot
Total # Votes:	320
Total Ballot Pool:	396
Quorum:	**80.81 % The Quorum has been reached**
Weighted Segment Vote:	69.43 %
Ballot Results:	**The Ballot has passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	106	1	49	0.636	28	0.364	0	8	21
2 - Segment 2	9	0.9	7	0.7	2	0.2	0	0	0
3 - Segment 3	86	1	41	0.641	23	0.359	0	7	15
4 - Segment 4	30	1	14	0.737	5	0.263	0	7	4
5 - Segment 5	98	1	37	0.587	26	0.413	1	11	23
6 - Segment 6	52	1	23	0.59	16	0.41	0	3	10
7 - Segment 7	0	0	0	0	0	0	0	0	0
8 - Segment 8	4	0.2	2	0.2	0	0	0	0	2
9 - Segment 9	3	0.2	2	0.2	0	0	0	0	1
10 - Segment 10	8	0.6	5	0.5	1	0.1	0	2	0
Totals	**396**	**6.9**	**180**	**4.791**	**101**	**2.109**	**1**	**38**	**76**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	SUPPORTS THIRD PARTY COMMENTS - (Ameren)
1	American Electric Power	Paul B Johnson		
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Negative	COMMENT RECEIVED
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton		
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel		
1	Colorado Springs Utilities	Paul Morland	Negative	SUPPORTS THIRD PARTY COMMENTS - FMPA
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	COMMENT RECEIVED
1	CPS Energy	Richard Castrejana		
1	Dairyland Power Coop.	Robert W. Roddy	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
1	El Paso Electric Company	Pablo Onate	Abstain	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Abstain	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
1	Hydro One Networks, Inc.	Ajay Garg		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	

1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
1	JDRJC Associates	Jim D Cyrulewski	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Jennifer Flandermeyer		
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam		
1	Long Island Power Authority	Robert Ganley		
1	Los Angeles Department of Water & Power	John Burnett		
1	Lower Colorado River Authority	Martyn Turner		
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
1	Minnkota Power Coop. Inc.	Daniel L Inman	Abstain	
1	Muscatine Power & Water	Andrew J Kurriger	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	SUPPORTS THIRD PARTY COMMENTS - (NPCC RSC Comments)
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southwest Power Pool)
1	Omaha Public Power District	Doug Peterchuck	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO)
1	Oncor Electric Delivery	Jen Fiegel		
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	SUPPORTS THIRD PARTY COMMENTS - (Consolidated Edison Co. of NY, Inc.)
1	Orlando Utilities Commission	Brad Chase	Abstain	
1	Otter Tail Power Company	Daryl Hanson	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
				SUPPORTS THIRD PARTY

1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	COMMENTS - (Public Service Enterprise Group)
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Abstain	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Abstain	
1	SaskPower	Wayne Guttormson		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Negative	SUPPORTS THIRD PARTY COMMENTS - (North American Generator Forum)
1	Southern California Edison Company	Steven Mavis		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Texas Municipal Power Agency	Brent J Hebert		
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Group)
1	Western Area Power Administration	Lloyd A Linke	Negative	COMMENT RECEIVED
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Alice Ireland, Xcel Energy)
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Negative	COMMENT RECEIVED
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Services	Mark Peters		
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	

3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blue Ridge Electric	James L Layton		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo		
3	City of Bartow, Florida	Matt Culverhouse	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (fmpa)
3	City of Farmington	Linda R Jacobson		
3	City of Garland	Ronnie C Hoeinghaus	Negative	COMMENT RECEIVED
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Charles Morgan	Negative	SUPPORTS THIRD PARTY COMMENTS - (- Florida Municipal Power Agency comments)
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	COMMENT RECEIVED
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	CPS Energy	Jose Escamilla		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	Entergy	Joel T Plessinger		
3	FirstEnergy Corp.	Cindy E Stewart	Abstain	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
3	Georgia System Operations Corporation	Scott McGough	Abstain	
3	Great River Energy	Brian Glover	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
3	Hydro One Networks, Inc.	David Kiguel	Abstain	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke		
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Abstain	

3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Supporting Southwest Power Pool comments.)
3	New York Power Authority	David R Rivera	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southwest Power Pool)
3	Old Dominion Electric Coop.	Bill Watson		
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Consolidated Edison Co. of NY, Inc.)
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward		
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	COMMENT RECEIVED - (North American Generator Forum)
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative)
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-County Electric Cooperative, Inc.	Mike Swearingen	Affirmative	
				COMMENT

3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	RECEIVED
3	Westar Energy	Bo Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Group)
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	SUPPORTS THIRD PARTY COMMENTS - (Xcel Energy's)
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache		
4	City of Clewiston	Kevin McCarthy		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell	Affirmative	
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Jerry Farringer)
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Abstain	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
4	Georgia System Operations Corporation	Guy Andrews	Abstain	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	Ohio Edison Company	Douglas Hohlbaugh	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative (Brett Galbraith))
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Negative	SUPPORTS THIRD PARTY COMMENTS - (See Ameren comments)
5	Arizona Public Service Co.	Scott Takinen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Commnets

				submitted by AZPS)
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Abstain	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Negative	SUPPORTS THIRD PARTY COMMENTS - FMPA
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	COMMENT RECEIVED
5	Consumers Energy Company	David C Greyerbiehl		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
5	Detroit Edison Company	Alexander Eizans	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
5	Dynegy Inc.	Dan Roethemeyer	Negative	NO COMMENT RECEIVED - (SERC OC)
5	El Paso Electric Company	Gustavo Estrada		
5	Electric Power Supply Association	John R Cashin		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Essential Power, LLC	Patrick Brown		
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Abstain	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
5	Hydro-Québec Production	Roger Dufresne	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lafayette Utilities System	Jamie B Webb	Affirmative	
				SUPPORTS THIRD PARTY COMMENTS -

5	Lakeland Electric	James M Howard	Negative	(Florida Municipal Power Association)
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Karin Schweitzer	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Abstain	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing		
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Compliance Grp)
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	NiSource	Huston Ferguson		
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Occidental Chemical	Michelle R DAntuono		
5	Oglethorpe Power Corporation	Bernard Johnson		
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southwest Power Pool)
5	Omaha Public Power District	Mahmood Z. Safi	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO)
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Abstain	
5	PacifiCorp	Bonnie Marino-Blair	Negative	COMMENT RECEIVED
5	Pattern Gulf Wind LLC	Grit Schmieder-Copeland		
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Abstain	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Negative	SUPPORTS THIRD PARTY COMMENTS - (PSEG (John Seelke))
5	Public Utility District No. 1 of Chelan County	John Yale		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Raven Power	Scott A Etnoyer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	COMMENT RECEIVED - (North American Generator Forum)
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Bret Galbraith on behalf of Seminole Electric Cooperative

				Inc.)
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe		
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State G & T Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	SUPPORTS THIRD PARTY COMMENTS - (mro nsrf)
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Utility System Effeciencies, Inc. (USE)	Robert L Dintelman	Negative	COMMENT RECEIVED
5	Vandolah Power Company L.L.C.	Douglas A. Jensen	Abstain	
5	Westar Energy	Bryan Taggart	Negative	SUPPORTS THIRD PARTY COMMENTS - (support the SPP Standards Group's comments)
5	Western Farmers Electric Coop.	Clem Cassmeyer		
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Negative	SUPPORTS THIRD PARTY COMMENTS - (Alice Ireland)
6	AEP Marketing	Edward P. Cox		
6	Ameren Energy Marketing Co.	Jennifer Richardson		
6	APS	Randy A. Young	Negative	COMMENT RECEIVED
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Negative	COMMENT RECEIVED
6	Con Edison Company of New York	David Balban	Negative	COMMENT RECEIVED
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke energy)
6	FirstEnergy Solutions	Kevin Querry	Abstain	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Municipal Power Pool	Thomas Washburn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brenda Hampton	Abstain	

6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley		
6	New York Power Authority	Saul Rojas		
6	Northern California Power Agency	Steve C Hill		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson		
6	Oklahoma Gas & Electric Services	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southwest Power Pool)
6	Omaha Public Power District	Douglas Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO Comments)
6	PacifiCorp	Kelly Cumiskey	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	COMMENT RECEIVED - (North American Generator Forum)
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (Bret Galbraith will be submitting comments on behalf of Seminole Electric Cooperative, Inc.)
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	Southern California Edison Company	Lujuanna Medina		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson		
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS - (Lloyd Linke)
6	Wisconsin Public Service Corp.	David Hathaway	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (Alice Ireland, Xcel Energy)
8		Edward C Stein		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	

9	National Association of Regulatory Utility Commissioners	Diane J. Barney		
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Abstain	
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Ballot Results	
Ballot Name:	Project 2013-04 Voltage and Reactive Control VAR-002-3 Additional Ballot
Ballot Period:	11/15/2013 - 11/26/2013
Ballot Type:	Additional Ballot
Total # Votes:	321
Total Ballot Pool:	396
Quorum:	**81.06 % The Quorum has been reached**
Weighted Segment Vote:	66.09 %
Ballot Results:	**The Ballot has closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	106	1	44	0.611	28	0.389	0	13	21
2 - Segment 2	9	0.8	6	0.6	2	0.2	0	0	1
3 - Segment 3	86	1	41	0.641	23	0.359	0	7	15
4 - Segment 4	30	1	16	0.727	6	0.273	0	4	4
5 - Segment 5	98	1	36	0.537	31	0.463	1	8	22
6 - Segment 6	52	1	21	0.512	20	0.488	0	2	9
7 - Segment 7	0	0	0	0	0	0	0	0	0
8 - Segment 8	4	0.2	2	0.2	0	0	0	0	2
9 - Segment 9	3	0.2	2	0.2	0	0	0	0	1
10 - Segment 10	8	0.5	4	0.4	1	0.1	0	3	0
Totals	**396**	**6.7**	**172**	**4.428**	**111**	**2.272**	**1**	**37**	**75**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	SUPPORTS THIRD PARTY COMMENTS - (Ameren)
1	American Electric Power	Paul B Johnson		
1	American Transmission Company, LLC	Andrew Z Pusztai	Abstain	
1	Arizona Public Service Co.	Robert Smith	Negative	COMMENT RECEIVED
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton		
1	Austin Energy	James Armke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Andrew Gallo)
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Negative	SUPPORTS THIRD PARTY COMMENTS - (Exelon Companies)
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Abstain	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel		
1	Colorado Springs Utilities	Paul Morland	Negative	SUPPORTS THIRD PARTY COMMENTS - FMPA
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	COMMENT RECEIVED
1	CPS Energy	Richard Castrejana		
1	Dairyland Power Coop.	Robert W. Roddy	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	El Paso Electric Company	Pablo Onate	Abstain	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS -

				(NSRF)
1	Hydro One Networks, Inc.	Ajay Garg		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
1	JDRJC Associates	Jim D Cyrulewski	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRo NSRF)
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Jennifer Flandermeyer		
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam		
1	Long Island Power Authority	Robert Ganley		
1	Los Angeles Department of Water & Power	John Burnett		
1	Lower Colorado River Authority	Martyn Turner		
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
1	Minnkota Power Coop. Inc.	Daniel L Inman	Abstain	
1	Muscatine Power & Water	Andrew J Kurriger	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Abstain	
1	Nebraska Public Power District	Cole C Brodine	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Abstain	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO)
1	Oncor Electric Delivery	Jen Fiegel		
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	SUPPORTS THIRD PARTY COMMENTS - (Consolidated Edison Co. of NY, Inc.)
1	Orlando Utilities Commission	Brad Chase	Abstain	
1	Otter Tail Power Company	Daryl Hanson	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRG)
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments submitted by PGE Angela Gaines.)
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	

1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Abstain	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Abstain	
1	SaskPower	Wayne Guttormson		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Negative	SUPPORTS THIRD PARTY COMMENTS - (North American Generator Forum)
1	Southern California Edison Company	Steven Mavis		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Texas Municipal Power Agency	Brent J Hebert		
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Group)
1	Western Area Power Administration	Lloyd A Linke	Negative	COMMENT RECEIVED
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Alice Ireland, Xcel Energy)
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Negative	COMMENT RECEIVED
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman		
2	Midwest ISO, Inc.	Marie Knox	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Services	Mark Peters		

3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blue Ridge Electric	James L Layton		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	COMMENT RECEIVED
3	City of Bartow, Florida	Matt Culverhouse	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (fmpa)
3	City of Farmington	Linda R Jacobson		
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Charles Morgan	Negative	SUPPORTS THIRD PARTY COMMENTS - (- Florida Municipal Power Agency comments)
3	ComEd	John Bee	Negative	SUPPORTS THIRD PARTY COMMENTS - (Exelon Companies)
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	COMMENT RECEIVED
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	CPS Energy	Jose Escamilla		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	Entergy	Joel T Plessinger		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
3	Georgia System Operations Corporation	Scott McGough	Abstain	
3	Great River Energy	Brian Glover	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
3	Hydro One Networks, Inc.	David Kiguel	Abstain	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke		
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)

3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Supporting Southwest Power Pool comments.)
3	New York Power Authority	David R Rivera	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Abstain	
3	Old Dominion Electric Coop.	Bill Watson		
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Consolidated Edison Co. of NY, Inc.)
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward		
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	COMMENT RECEIVED - (North American Generator Forum)
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative)
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	

3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-County Electric Cooperative, Inc.	Mike Swearingen	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Group)
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	SUPPORTS THIRD PARTY COMMENTS - (Xcel Energy)
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache		
4	City of Clewiston	Kevin McCarthy		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell	Negative	SUPPORTS THIRD PARTY COMMENTS - (Exelon Companies)
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Jerry Farringer)
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Abstain	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
4	Georgia System Operations Corporation	Guy Andrews	Abstain	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative (Brett Galbraith))
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
				SUPPORTS

5	Amerenue	Sam Dwyer	Negative	THIRD PARTY COMMENTS - (see Ameren's comments)
5	Arizona Public Service Co.	Scott Takinen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments submitted by AZPS)
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Abstain	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	SUPPORTS THIRD PARTY COMMENTS - (Andrew Gallo)
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Negative	SUPPORTS THIRD PARTY COMMENTS - FMPA
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	COMMENT RECEIVED
5	Consumers Energy Company	David C Greyerbiehl		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
5	Detroit Edison Company	Alexander Eizans	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
5	Dynegy Inc.	Dan Roethemeyer	Negative	NO COMMENT RECEIVED - (SERC OC)
5	El Paso Electric Company	Gustavo Estrada		
5	Electric Power Supply Association	John R Cashin		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Essential Power, LLC	Patrick Brown		
5	Exelon Nuclear	Mark F Draper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Exelon Companies)
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS -

				(NSRF)
5	Hydro-Québec Production	Roger Dufresne	Negative	COMMENT RECEIVED
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lafayette Utilities System	Jamie B Webb	Affirmative	
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municpal Power Association)
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Karin Schweitzer		
5	Luminant Generation Company LLC	Rick Terrill	Negative	COMMENT RECEIVED
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing		
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Compliance Grp)
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	NiSource	Huston Ferguson		
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO)
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	PacifiCorp	Bonnie Marino-Blair	Negative	COMMENT RECEIVED
5	Pattern Gulf Wind LLC	Grit Schmieder-Copeland		
5	Portland General Electric Co.	Matt E. Jastram	Negative	COMMENT RECEIVED
5	PowerSouth Energy Cooperative	Tim Hattaway	Abstain	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Negative	SUPPORTS THIRD PARTY COMMENTS - (PSEG (John Seelke))
5	Public Utility District No. 1 of Chelan County	John Yale		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Raven Power	Scott A Etnoyer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
				COMMENT

5	Santee Cooper	Lewis P Pierce	Negative	RECEIVED - (North American Generator Forum)
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Bret Galbraith on behalf of Seminole Electric Cooperative Inc)
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe		
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State G & T Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Utility System Effeciencies, Inc. (USE)	Robert L Dintelman	Negative	COMMENT RECEIVED
5	Vandolah Power Company L.L.C.	Douglas A. Jensen	Abstain	
5	Westar Energy	Bryan Taggart	Negative	SUPPORTS THIRD PARTY COMMENTS - (support the SPP Standards Group's comments)
5	Western Farmers Electric Coop.	Clem Cassmeyer		
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Negative	SUPPORTS THIRD PARTY COMMENTS - (Alice Ireland)
6	AEP Marketing	Edward P. Cox		
6	Ameren Energy Marketing Co.	Jennifer Richardson		
6	APS	Randy A. Young	Negative	COMMENT RECEIVED
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Negative)
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Negative	COMMENT RECEIVED
6	Con Edison Company of New York	David Balban	Negative	COMMENT RECEIVED
6	Constellation Energy Commodities Group	David J Carlson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Exelon Companies)
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke energy)
6	FirstEnergy Solutions	Kevin Querry	Affirmative	

6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Municipal Power Pool	Thomas Washburn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brenda Hampton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Luminant Generation Company LLC)
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
6	New York Power Authority	Saul Rojas		
6	Northern California Power Agency	Steve C Hill		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson		
6	Oklahoma Gas & Electric Services	Jerry Nottnagel	Abstain	
6	Omaha Public Power District	Douglas Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO Comments)
6	PacifiCorp	Kelly Cumiskey	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	SUPPORTS THIRD PARTY COMMENTS - (North American Generator Forum)
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (Bret Galbraith will be submitting comments on behalf of Seminole Electric Cooperative, Inc.)
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	Southern California Edison Company	Lujuanna Medina		

6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson		
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS - (Lloyd Linke)
6	Wisconsin Public Service Corp.	David Hathaway	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Negative	SUPPORTS THIRD PARTY COMMENTS - (Alice Ireland, Xcel Energy)
8		Edward C Stein		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney		
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Joseph W Spencer	Abstain	
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Non-Binding Poll Results

Project 2013-04 Voltage and Reactive Control (VAR) VAR-001-4

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2013-04 VRC VAR-001-4 Non-binding Poll
Poll Period:	11/15/2013 - 11/26/2013
Total # Opinions:	285
Total Ballot Pool:	362
Summary Results:	78.73% of those who registered to participate provided an opinion or an abstention; 57.75% of those who provided an opinion indicated support for the VRFs and VSLs.

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	Comments
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson		
1	Arizona Public Service Co.	Robert Smith	Negative	COMMENT RECEIVED
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton		
1	Austin Energy	James Armke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Andrew Gallo)
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Abstain	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida

				Municipal Power Agency)
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel		
1	Colorado Springs Utilities	Paul Morland	Negative	SUPPORTS THIRD PARTY COMMENTS - FMPA
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	COMMENT RECEIVED
1	CPS Energy	Richard Castrejana		
1	Dairyland Power Coop.	Robert W. Roddy	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Abstain	
1	Duke Energy Carolina	Douglas E. Hils	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
1	El Paso Electric Company	Pablo Onate	Abstain	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Abstain	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
1	Hydro One Networks, Inc.	Ajay Garg		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Jennifer Flandermeyer		

1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam		
1	Long Island Power Authority	Robert Ganley		
1	Los Angeles Department of Water & Power	John Burnett		
1	Lower Colorado River Authority	Martyn Turner		
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
1	Minnkota Power Coop. Inc.	Daniel L Inman	Abstain	
1	Muscatine Power & Water	Andrew J Kurriger	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Abstain	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz - American Electric Power)
1	Oklahoma Gas and Electric Co.	Terri Pyle	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southwest Power Pool)
1	Omaha Public Power District	Doug Peterchuck	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO)
1	Oncor Electric Delivery	Jen Fiegel		
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	SUPPORTS THIRD PARTY COMMENTS - (Consolidated Edison Co. of NY, Inc.)

1	Orlando Utilities Commission	Brad Chase	Abstain	
1	Otter Tail Power Company	Daryl Hanson	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Abstain	
1	Sacramento Municipal Utility District	Tim Kelley	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Abstain	
1	SaskPower	Wayne Guttormson		
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Negative	SUPPORTS THIRD PARTY COMMENTS - (North American Generator Forum)
1	Southern California Edison Company	Steven Mavis		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Texas Municipal Power Agency	Brent J Hebert		
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Group)
1	Western Area Power Administration	Lloyd A Linke	Negative	COMMENT

				RECEIVED
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Abstain	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman		
2	Midwest ISO, Inc.	Marie Knox	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Abstain	
3	AEP	Michael E Deloach	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz - American Electric Power)
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Services	Mark Peters		
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo		
3	City of Bartow, Florida	Matt Culverhouse	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (fmpa)
3	City of Farmington	Linda R Jacobson		
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Tallahassee	Bill R Fowler	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Charles Morgan	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (- Florida Municipal Power Agency comments)
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	COMMENT RECEIVED
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	CPS Energy	Jose Escamilla		
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	Entergy	Joel T Plessinger		
3	FirstEnergy Corp.	Cindy E Stewart	Abstain	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
3	Georgia System Operations Corporation	Scott McGough	Abstain	
3	Great River Energy	Brian Glover	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
3	Hydro One Networks, Inc.	David Kiguel	Abstain	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke		
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Abstain	
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Supporting Southwest Power Pool comments.)
3	New York Power Authority	David R Rivera	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southwest Power Pool)
3	Old Dominion Electric Coop.	Bill Watson		
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Consolidated Edison Co. of NY, Inc.)
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Abstain	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	COMMENT RECEIVED - (North American Generator Forum)
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative)
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	

3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-County Electric Cooperative, Inc.	Mike Swearingen	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Group)
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache		
4	City of Clewiston	Kevin McCarthy		
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Jerry Farringer)
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Abstain	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Georgia System Operations Corporation	Guy Andrews	Abstain	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	Ohio Edison Company	Douglas Hohlbaugh	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Abstain	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative (Brett

				Galbraith))
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz - American Electric Power)
5	Amerenue	Sam Dwyer	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments submitted by AZPS)
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke	Abstain	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Abstain	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	SUPPORTS THIRD PARTY COMMENTS - (Andrew Gallo)
5	City of Tallahassee	Karen Webb	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Negative	SUPPORTS THIRD PARTY COMMENTS - FMPA
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	COMMENT

				RECEIVED
5	Consumers Energy Company	David C Greyerbiehl		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
5	Detroit Edison Company	Alexander Eizans	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
5	Dynegy Inc.	Dan Roethemeyer	Negative	NO COMMENT RECEIVED - (SERC OC)
5	El Paso Electric Company	Gustavo Estrada		
5	Electric Power Supply Association	John R Cashin		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Essential Power, LLC	Patrick Brown		
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Abstain	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
5	Hydro-Québec Production	Roger Dufresne	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Karin Schweitzer	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Abstain	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing		

5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Compliance Grp)
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	NiSource	Huston Ferguson		
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Occidental Chemical	Michelle R DAntuono		
5	Oglethorpe Power Corporation	Bernard Johnson		
5	Oklahoma Gas and Electric Co.	Henry L Staples	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southwest Power Pool)
5	Omaha Public Power District	Mahmood Z. Safi	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO)
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Abstain	
5	PacifiCorp	Bonnie Marino-Blair	Negative	COMMENT RECEIVED
5	Pattern Gulf Wind LLC	Grit Schmieder-Copeland		
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Abstain	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Chelan County	John Yale		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Raven Power	Scott A Etnoyer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Abstain	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	COMMENT RECEIVED - (North American Generator Forum)
5	Seattle City Light	Michael J. Haynes	Abstain	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Bret

				Galbraith on behalf of Seminole Electric Cooperative Inc.)
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	Southern California Edison Company	Denise Yaffe		
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State G & T Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	SUPPORTS THIRD PARTY COMMENTS - (mro nsrf)
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Utility System Effeciencies, Inc. (USE)	Robert L Dintelman	Negative	COMMENT RECEIVED
5	Western Farmers Electric Coop.	Clem Cassmeyer		
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles		
6	AEP Marketing	Edward P. Cox		
6	Ameren Energy Marketing Co.	Jennifer Richardson		
6	APS	Randy A. Young	Negative	COMMENT RECEIVED
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Andrew Gallo)
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Negative	COMMENT RECEIVED
6	Con Edison Company of New York	David Balban	Negative	COMMENT RECEIVED
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke energy)
6	FirstEnergy Solutions	Kevin Querry	Abstain	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Municipal Power Pool	Thomas Washburn	Negative	SUPPORTS

				THIRD PARTY COMMENTS - (FMPA)
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brenda Hampton	Abstain	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley		
6	New York Power Authority	Saul Rojas		
6	Northern California Power Agency	Steve C Hill		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson		
6	Oklahoma Gas & Electric Services	Jerry Nottnagel	Negative	SUPPORTS THIRD PARTY COMMENTS - (Southwest Power Pool)
6	Omaha Public Power District	Douglas Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO Comments)
6	PacifiCorp	Kelly Cumiskey	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Abstain	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	COMMENT RECEIVED - (North American Generator Forum)
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (Bret

				Galbraith will be submitting comments on behalf of Seminole Electric Cooperative, Inc.)
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	Southern California Edison Company	Lujuanna Medina		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS - (Lloyde Linke)
8		Edward C Stein		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Abstain	
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Non-Binding Poll Results

Project 2013-04 Voltage and Reactive Control (VAR) VAR-002-3

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2013-04 VRC VAR-002-3 Non-binding Poll
Poll Period:	11/15/2013 - 11/26/2013
Total # Opinions:	286
Total Ballot Pool:	362
Summary Results:	79.01% of those who registered to participate provided an opinion or an abstention; 57.87% of those who provided an opinion indicated support for the VRFs and VSLs.

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	Comments
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson		
1	Arizona Public Service Co.	Robert Smith	Negative	COMMENT RECEIVED
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton		
1	Austin Energy	James Armke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Andrew Gallo)
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Abstain	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	COMMENT RECEIVED
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Abstain	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel		

1	Colorado Springs Utilities	Paul Morland	Negative	SUPPORTS THIRD PARTY COMMENTS - FMPA
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	COMMENT RECEIVED
1	CPS Energy	Richard Castrejana		
1	Dairyland Power Coop.	Robert W. Roddy	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Abstain	
1	Duke Energy Carolina	Douglas E. Hils	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
1	El Paso Electric Company	Pablo Onate	Abstain	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
1	Hydro One Networks, Inc.	Ajay Garg		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Jennifer Flandermeyer		
1	Lakeland Electric	Larry E Watt		
1	Lincoln Electric System	Doug Bantam		
1	Long Island Power Authority	Robert Ganley		
1	Los Angeles Department of Water & Power	John Burnett		
1	Lower Colorado River Authority	Martyn Turner		
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Abstain	
1	Muscatine Power & Water	Andrew J Kurriger	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)

1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Abstain	
1	Nebraska Public Power District	Cole C Brodine	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Abstain	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz - American Electric Power)
1	Oklahoma Gas and Electric Co.	Terri Pyle	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO)
1	Oncor Electric Delivery	Jen Fiegel		
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	SUPPORTS THIRD PARTY COMMENTS - (Consolidated Edison Co. of NY, Inc.)
1	Orlando Utilities Commission	Brad Chase	Abstain	
1	Otter Tail Power Company	Daryl Hanson	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments submitted by PGE Angela Gaines.)
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Abstain	
1	Sacramento Municipal Utility District	Tim Kelley	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Abstain	
1	SaskPower	Wayne Guttormson		
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	

1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Negative	SUPPORTS THIRD PARTY COMMENTS - (North American Generator Forum)
1	Southern California Edison Company	Steven Mavis		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Texas Municipal Power Agency	Brent J Hebert		
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Group)
1	Western Area Power Administration	Lloyd A Linke	Negative	COMMENT RECEIVED
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Abstain	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman		
2	Midwest ISO, Inc.	Marie Knox	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Abstain	
3	AEP	Michael E Deloach	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz - American Electric Power)
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Services	Mark Peters		
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	

3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo		
3	City of Bartow, Florida	Matt Culverhouse	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (fmpa)
3	City of Farmington	Linda R Jacobson		
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Tallahassee	Bill R Fowler	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Charles Morgan	Negative	SUPPORTS THIRD PARTY COMMENTS - (- Florida Municipal Power Agency comments)
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	COMMENT RECEIVED
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	CPS Energy	Jose Escamilla		
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	Entergy	Joel T Plessinger		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
3	Georgia System Operations Corporation	Scott McGough	Abstain	
3	Great River Energy	Brian Glover	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
3	Hydro One Networks, Inc.	David Kiguel	Abstain	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke		
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	Lakeland Electric	Mace D Hunter	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
3	Lincoln Electric System	Jason Fortik	Affirmative	

3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Supporting Southwest Power Pool comments.)
3	New York Power Authority	David R Rivera	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Abstain	
3	Old Dominion Electric Coop.	Bill Watson		
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	SUPPORTS THIRD PARTY COMMENTS - (Consolidated Edison Co. of NY, Inc.)
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Abstain	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	COMMENT RECEIVED - (North American Generator Forum)
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative)
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	

3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-County Electric Cooperative, Inc.	Mike Swearingen	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Standards Group)
3	Xcel Energy, Inc.	Michael Ibold	Negative	SUPPORTS THIRD PARTY COMMENTS - (Xcel Energy)
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache		
4	City of Clewiston	Kevin McCarthy		
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP)
4	Consumers Energy Company	Tracy Goble	Negative	SUPPORTS THIRD PARTY COMMENTS - (Jerry Farringer)
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Abstain	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Georgia System Operations Corporation	Guy Andrews	Abstain	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Abstain	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	SUPPORTS THIRD PARTY COMMENTS - (Seminole Electric Cooperative (Bret Galbraith))
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Negative	SUPPORTS THIRD

				PARTY COMMENTS - (Thomas Foltz - American Electric Power)
5	Amerenue	Sam Dwyer	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Negative	SUPPORTS THIRD PARTY COMMENTS - (Comments submitted by AZPS)
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Abstain	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	SUPPORTS THIRD PARTY COMMENTS - (Andrew Gallo)
5	City of Tallahassee	Karen Webb	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Negative	SUPPORTS THIRD PARTY COMMENTS - FMPA
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	COMMENT RECEIVED
5	Consumers Energy Company	David C Greyerbiehl		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
5	Detroit Edison Company	Alexander Eizans	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
5	Dynegy Inc.	Dan Roethemeyer	Negative	NO COMMENT RECEIVED - (SERC OC)
5	El Paso Electric Company	Gustavo Estrada		

5	Electric Power Supply Association	John R Cashin		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Essential Power, LLC	Patrick Brown		
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
5	Hydro-Québec Production	Roger Dufresne	Negative	COMMENT RECEIVED
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Karin Schweitzer		
5	Luminant Generation Company LLC	Rick Terrill	Negative	COMMENT RECEIVED
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing		
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP Compliance Grp)
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	NiSource	Huston Ferguson		
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO)
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	PacifiCorp	Bonnie Marino-Blair	Negative	COMMENT RECEIVED

5	Pattern Gulf Wind LLC	Grit Schmieder-Copeland		
5	Portland General Electric Co.	Matt E. Jastram	Negative	COMMENT RECEIVED
5	PowerSouth Energy Cooperative	Tim Hattaway	Abstain	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Chelan County	John Yale		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Raven Power	Scott A Etnoyer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Abstain	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	COMMENT RECEIVED - (North American Generator Forum)
5	Seattle City Light	Michael J. Haynes	Abstain	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Bret gailbraith on behalf of Seminole Electric Cooperative Inc.)
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	Southern California Edison Company	Denise Yaffe		
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State G & T Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	SUPPORTS THIRD PARTY COMMENTS - (MRO NSRF)
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Utility System Effeciencies, Inc. (USE)	Robert L Dintelman	Negative	COMMENT RECEIVED
5	Western Farmers Electric Coop.	Clem Cassmeyer		
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles		
6	AEP Marketing	Edward P. Cox		
6	Ameren Energy Marketing Co.	Jennifer Richardson		
6	APS	Randy A. Young	Negative	COMMENT RECEIVED
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	

6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Negative	SUPPORTS THIRD PARTY COMMENTS - (Andrew Gallo)
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Negative	COMMENT RECEIVED
6	Con Edison Company of New York	David Balban	Negative	COMMENT RECEIVED
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke energy)
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Municipal Power Pool	Thomas Washburn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Negative	SUPPORTS THIRD PARTY COMMENTS - (NSRF)
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brenda Hampton	Abstain	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley		
6	New York Power Authority	Saul Rojas		
6	Northern California Power Agency	Steve C Hill		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson		
6	Oklahoma Gas & Electric Services	Jerry Nottnagel	Abstain	
6	Omaha Public Power District	Douglas Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (SPP RTO Comments)
6	PacifiCorp	Kelly Cumiskey	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Abstain	

6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	COMMENT RECEIVED - (North American Generator Forum)
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	SUPPORTS THIRD PARTY COMMENTS - (Bret Galbraith will be submitting comments on behalf of Seminole Electric Cooperative, Inc.)
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	Southern California Edison Company	Lujuanna Medina		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS - (Lloyd Linke)
8		Edward C Stein		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Abstain	
10	Texas Reliability Entity, Inc.	Donald G Jones	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Individual or group. (59 Responses)
Name (39 Responses)
Organization (39 Responses)
Group Name (20 Responses)
Lead Contact (20 Responses)
IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE. (12 Responses)
Comments (59 Responses)
Question 1 (34 Responses)
Question 1 Comments (47 Responses)
Question 2 (43 Responses)
Question 2 Comments (47 Responses)
Question 3 (0 Responses)
Question 3 Comments (47 Responses)
Question 3 (0 Responses)
Question 3 Comments (47 Responses)

Group
MRO NSRF
Russel Mountjoy
Yes
In requirement 5.1 a Transmission Operator is required direct a Generator Operator to "comply with the schedule" provided by the Transmission Operator. In 5.2, however, the potential for deviations from the schedule is implied. To avoid conflict between these two, the following change to 5.1 is recommended: "The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode unless notification of deviation is provided in accordance with 5.2." For consistency M2 should be reworded as follows: "For the operational planning time horizon, Transmission Operators shall have evidence of assessments used as the basis for how resources were scheduled" The current wording of "shall provide copies" imposes an action that is not included in the associated requirement. In previous comments regarding voltage schedules issued by a Transmission Operator a mechanism for a Generator Operator to provide explanations if a proposed schedule could not reasonably be met based on specific equipment limitations and to get a revised schedule or exemption was suggested. In this version the Transmission Operator is obligated to provide additional information about the schedule, but is not obligated to respond to Generator Operator concerns regarding the schedule. Under VAR-002 a Generator Operator is required to comply with the schedule provide by the Transmission Operator unless notification is provided. There then is the potential situation where a schedule issued by a Transmission Operator cannot be met due to equipment or system conditions and the only action available is for a Generator Operator to provide multiple notifications. A better solution it seems would be to include some sort of feedback process

between Generator Operators and Transmission Operations in the VAR-001 standard that would result in an agreed-upon schedule that could reasonably be met without burdensome periodic notifications. As recommended in previous comments a process of reaching “mutual agreement” on the schedule for making transformer tap changes is suggested . The SDT responded in the consideration of comments that they did not chose to include the suggested agreement language but did add a requirement for the transmission operator to provide an “implementation schedule”. While this change is an improvement it does not completely solve the concern presented. The objective should be that a tap change schedule is agreed upon that would meet the reasonable needs of both the Transmission Operator and Generator Operator. The following from requirement R2: “Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load” implies that all of the items listed need to be considered. If the intent is that the items are intended to be examples it is suggested that the words “including , but not limited to” be replaced by “such as”. It is recommended that R5.1 be modified as recommended by the NERC IGVT report of September 2012: 5.1. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR or plant-level volt/var regulator is in service and controlling voltage). The standard should be reviewed and where AVR is referred to, the plant-level volt/var regulator should be added in a similar way to this recommended change to R5.1. The referenced NERC report provides the technical basis for this recommendation.

The revised VAR-002 R2.1 removes the 15 minute deviation criteria for notification by Generator Operators to Transmission Operators. The revised VAR-001-4 requires Transmission Operators to provide notification requirements. The drafting team in the consideration of comments explained “In an effort to remove prescriptive notification requirements for the entire continent” the change was made. This leaves the Generator Operators at the mercy of Transmission Operators who could potentially set a no deviation criteria. It is recommended that a compromise be struck by specifying a limit on the criteria such as “no less than 15 minutes”. For clarification it is recommended that the word “generator” be added before the word “stability” in the last sentence of footnote 6. [Note to NSRF: a comment on this was submitted previously but it did not have a recommended language change] In M2 it is recommended that “alarm logs” be added to the list of evidence. We support the deletion of the language regarding notification of the expected duration of a change in status. At the time a status change occurs it is often difficult to provide a meaningful estimate of the duration of the change. Requirement 3 should be revised to state – Notification must be made within 30 minutes of becoming aware of the change from automatic controlling voltage for the AVR, and from in-service of the PSS. Measure 3 should be revised to reflect this as well. The following change to requirement R4 is recommended: “Reactive capability changes due to factors such as a change in the wind speed for wind generators or a change in the solar resource for solar facilities do not require Transmission Operator notification” Measure 4 should be revised to reflect the wording in Requirement 4 – Notification must be made within 30 minutes of becoming aware of the change of state of the AVR. For the same reason

described above for VAR-001 (NERC IGVT Report), R1 should be modified as follows: “R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) or plant-level volt/var regulator in service and controlling voltage) unless the Generator Operator 1) is exempted by the Transmission Operator, or 2) has notified the Transmission Operator of one of the following:” A similar addition should be made where the AVR is referred to in the other requirements of VAR-002.
Group
Northeast Power Coordinating Council
Guy Zito
Yes
We support the direction being taken and the SDT’s decision to not reiterate or duplicate the voltage assessment requirements already addressed by the FAC and TOP standards.
Yes
We support the SDT’s proposal to remove the requirements that may be redundant with other standards. However, regarding VAR-001-4 Requirement R1 was revised to read: R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits 1.1 Each Transmission Operator shall provide a copy of the voltage schedules and asspociated tolerance bands to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request. What is meant by “system voltage schedule.” Is it a high-level, overall voltage schedule by voltage class, or a voltage schedule by station (even if there is no direct means of controlling voltage at that station)? Requirement R5 already addresses specification of generator voltage schedules, so if that is what is intended to be addressed under R1, why is R1 needed at all? Requirement R5 states: R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range, or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the Generator Step-Up transformer at the Transmission Operator’s discretion. There is inconsistency in the tense used in various VSLs. Some are in present tense while others are in the past tense. This should be reviewed and and revised as appropriate. “Schedule” is used in both VAR-001 Requirements R1 and R5. However, it is modified by different phrases in each, implying different types of “schedules.” These two different types of “schedules” have caused confusion, making the use and intended meaning less than perfectly clear. VAR-001 Requirement R1 - To improve clarity and consistency, suggest that the word “schedule” be deleted here and only be used when referring to GOP operation. Suggest revising Requirement R1 wording as follows: R1. Each Transmission Operator shall specify a system voltage range or a target value with an associated tolerance band as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits. Note that Requirement R1 only requires that the TOP establish the target system voltage level and tolerance band. There is no mention of GOP operation. Requirement R2 requires that the TOP schedule its arrangement of sufficient reactive resources, whether actually used (dispatched)

or not, a Planning function (see Measure M2). The Rationale box states: “to ensuring sufficient reactive resources are online or scheduled.” The use of the word “scheduled” here again has caused confusion. We suggest it be replaced to clarify the meaning, as follows: R2. Each Transmission Operator shall make arrangements for sufficient on-line, available reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, making arrangements for reactive generation resources, transmission line and reactive resource switching, and using controllable load. Further recommend revising M2 to synchronize it with the revised Requirement R2 above, as follows: M2. Each Transmission Operator shall have evidence of sufficient reactive resources based on their assessments of the system. For the operational planning time horizon, Transmission Operators shall provide copies of assessments used as the basis for determining how resources were made available. Organizationally, R4 should be swapped with R5. A requirement dealing with exemptions should come after the “foundation” requirement. The Drafting Team must consider the following regarding Hydro-Quebec TransEnergie. "Schedule" in the standard is confusing and does not apply to Hydro-Québec TransÉnergie. Hydro-Quebec TransEnergie does not issue a schedule of voltage or reactive power. Hydro-Quebec TransEnergie sets voltage ranges to comply at all times for the different voltage levels. During light or peak load, these operating situations are governed with voltage setupoints for specific substations. The standard should therefore consider (in addition to the preceding comments) the terms used. For example, consider substituting the term " voltage or reactive power setpoint " for the word “schedule” which does not reflect our operating procedures. Regarding Requirement R5, NERC now requires a specified program voltage or reactive power be given to central planning and forecasting. This requirement is not applicable to Hydro-Québec TransÉnergie because there is no voltage or reactive power schedule, but rather the requirement that every generating facility of more than 10 MW have an automatic voltage regulation system. Hydro-Quebec TransEnergie also requires them to provide a specific power factor for each of those generating units.
Suggest the following changes to more effectively convey the intents of Measure M3 and Requirement R6. Suggest that Measure M3 be reworded to require demonstration of compliance rather than to require actions which should have been stipulated in the requirement. Specifically, we proposed the last part in Measure M3 be revised to: “…therefore, if a status change lasts more than 15 minutes, the GOP shall provide evidence such as system log, electronic message or a transmittal letter that it notified its associated Transmission Operator within 30 minutes of when the change first occurred.” Regarding R6, the wording “the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator…” is not a direct action and may not be measurable. Suggest revising it to read: “the Generator Owner shall implement the transformer tap positions according to the specifications provided by the Transmission Operator….” We further propose that the SDT insert the evidence language into the first sentence of Measure M3 which asks for evidence that the Generator notified its associated Transmission Operator within 30 minutes of the change identified in Requirement R3. Generators may be asked by their TOP to operate in other modes. Reword Requirement

R1 as follows: R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless the Generator Operator 1) is exempted by the Transmission Operator, 2) is notified by the Transmission Operator to operate in a different viable operating mode (e.g., constant VAR output mode), or 3) has notified the Transmission Operator of one of the following:… The comments in Question 2 regarding Hydro-Quebec regarding the word "schedule" apply.
We support the proposed VRFs and VSLs.
Individual
aaa
bbb
Agree
Group
Bureau of Reclamation
Erika Doot
Yes
Yes
The Bureau of Reclamation (Reclamation) notes that the WECC variance indicates that it is intended to replace requirements R3 and R4. However, R3 and R4 in VAR-001-4 are not the same as R3 and R4 in VAR-001-3. Reclamation suggests that the drafting team should examine the WECC variance to determine which requirements it will replace because it appears that the WECC variance should replace R4 and R5. In WECC, it would be difficult for Transmission Operators to comply with both R5 and E.A. 14 because they refer to different voltage schedule reference points. VAR-001-4 R3 specifies that Transmission Operators must operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary. Measure M3 specifies that “this may include directions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments.” Reclamation suggests that this detail should be included in Requirement R3 rather than solely in the measure. VAR-001-4 R4 requires a Transmission Operator to notify a Generator Operator if the “Transmission Operator determines that a generator has satisfied exemption criteria” but does not specify a timeframe for this notification. Reclamation suggests that the drafting team update VAR-001-4 R4 to specify that the Transmission Operator must notify the Generator Operator within 30 days if the Transmission Operator determines that a generator has satisfied criteria for exemption from voltage or Reactive Power requirements and associated notification requirements. Reclamation also suggests that R4 on exemptions should follow R5 on voltage or Reactive Power scheduling and notification criteria. VAR-001 R5 allows the Transmission Operator to specify a voltage or Reactive Power schedule at either the high voltage side or low voltage side of the Generator Step Up transformer. Reclamation suggests that like in requirement E.A.14, Transmission Operators should be able to specify the voltage schedule at the generator terminals, high side of the generator step-up transformer, point of interconnection, or a location designated by mutual

agreement. VAR-001 R5.2 specifies that “The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule.” M5 regarding part 5.2 specifies that voice recordings may be used to establish compliance with this requirement. Reclamation suggests that voice recordings should be removed from the list in M5 for part 5.2 because notification requirements established in the planning horizon should be transmitted in writing. Reclamation notes that there is a potential inconsistency between the Transmission Operator notification requirements discussed in VAR-001 R5.2 and the Generator Operator notification requirements discussed VAR-002 R3 and R4. Reclamation recommends that VAR-001 R5.2 be modified to solely address planning horizon notifications. For consistency with the Generator Operator real-time notification requirements established in VAR-002 R3 and R4, Reclamation also recommends that VAR-001-4 R5 should include an additional subrequirement which specifies that the “TOP shall develop real-time notification requirements for the deviations from the voltage of Reactive Power schedule within 30 minutes of when a Generator Operator becomes aware of a change in reactive capability, AVR status, power system stabilizer status, or alternative voltage controlling device status, unless the status is restored within 15 minutes.” VAR-001-4 R5 requires the Transmission Operator to specify a voltage or Reactive Power schedule “at either the high voltage side or low voltage side of the Generator Step-Up transformer.” VAR-002-3 R2.3 allows Generator Operators to monitor voltages at another location so long as the Generator Operator has a “methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.” Reclamation suggests that having the Transmission Operator and Generator Operator monitor voltages at different locations could lead to confusion in real-time communications. Reclamation suggests that VAR-001-4 R5 be updated to require the Transmission Operator to set voltages based on common monitoring locations to avoid confusion in real-time communications between Transmission Operators and Generator Operators. Reclamation suggests that R6 should be updated to specify that the Transmission Operator must coordinate outages to accommodate required step-up transformer tap changes. Reclamation suggests the drafting team update the requirement to read “After consultation with the Generator Owner regarding necessary step-up transformer tap changes, associated outages, and the implementation schedule…”. Reclamation also notes that "Generator Step-Up transformer" is sometimes capitalized in the standard. However, it is not capitalized in the WECC variance or NERC Glossary. Reclamation suggests that the drafting team remove capitalization in the term “Generator Step-Up transformer” because it is not defined in the NERC Glossary.
Reclamation believes that the notification requirements in R2 and R3 should provide the continent-wide standard. Reclamation suggests that the bullet points in R1 should be relabeled as sub-requirements R1.1 and R1.2. Reclamation requests that the drafting team clarify the timeframe for notifications required by R1. Reclamation suggests that the drafting team update VAR-002-3 R2 to allow Generator Operators to notify Transmission Operators that a voltage schedule cannot be met for equipment or other reasons, so that the Transmission Operator can alter the voltage schedule accordingly. R2.2 recognizes that a Generator Operator can provide an explanation that a voltage schedule cannot be met “when

directed to modify voltage" but does not address the planning horizon. Reclamation appreciates that R2 recognizes that generators only need to comply with voltage schedules within facility capabilities, and that footnote 6 recognizes that generating facility capability may not be sufficient at times to pull the system voltage within scheduled tolerance bands. Nevertheless, Reclamation believes that R2 subrequirements should more clearly articulate that (1) Generator Operators should provide Transmission Operators with feedback that they cannot meet voltage schedules in the planning horizon, and (2) generators may not always be capable of modifying system voltage. Reclamation notes that R2.3 applies to real-time operations, and suggests that R2.3 should be updated to require Generator Operators and Transmission Operators to monitor voltage at mutually-agreed upon locations to avoid confusion in real-time communications. Reclamation suggests that the drafting team update VAR-002-3 R3 to specify that the "Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of becoming aware of the change." Reclamation also suggests that M3 should be updated to specify that the GOP must notify its associated Transmission Operator "within 30 minutes of becoming aware of the change" rather than "within 30 minutes of when the change first occurred." Reclamation notes that VAR-002-3 R4 specifies that the "Generator Operator shall notify its associated Transmission Operator within 30 minutes after becoming aware of a change in reactive capability… ." Reclamation suggests that M4 should be updated to match this language and specify that the GOP must notify its associated Transmission Operator "within 30 minutes of becoming aware of the change" rather than "within 30 minutes of when the change first occurred." Reclamation requests clarification on types of "changes in reactive capability" that could trigger the notification requirement in R4. Reclamation notes that the time horizon for VAR-002-3 R6 should probably be changed from "Real-Time Operations" to "Operations Planning" to match VAR-001-4 R6 and reflect that tap setting changes are agreed upon in advance rather than in real-time. Reclamation suggests that VAR-002-3 R6 should be updated to match VAR-001-4 R6 and to specify that the Transmission Operator must coordinate outages to accommodate required step-up transformer tap changes. Reclamation suggests the drafting team update the requirement to read "After consultation with the Generator Owner regarding necessary step-up transformer tap changes, associated outages, and the implementation schedule…".
Reclamation suggests that the VSLs for VAR-002-3 R3 and R4 should reflect a range of noncompliance like in VAR-002-2. A failure to notify the Transmission Operator of an AVR, power system stabilizer, or reactive capability change for 35 minutes should not be treated the same as a failure to notify the Transmission Operator of the status change for 75 minutes.
Individual
John Canavan
NorthWestern Energy
Yes
For R2, M2 - It would be very helpful if "their assessments of the system" be clearly defined. For example, would TPL studies suffice as evidence for meeting this requirement or is this more of a real time requirement and if so, what types of evidence is NERC lokking for.

Individual
Chris de Graffenried
Consolidated Edison Co. of NY, Inc.
Yes
The drafting team used the word “schedule” in both VAR-001 Requirements R1 and R5. However, it is modified by different phrases in each, implying different types of “schedules.” These two different types of “schedules” has caused confusion, making the use and intended meaning less than perfectly clear. VAR-001 Requirement R1 - To improve clarity and consistency, we recommend that the word “schedule” be deleted here and only be used when referring to GOP operation. The revised Requirement R1 wording recommended follows: R1. Each Transmission Operator shall specify a system voltage [delete: schedule (which is either a] range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits. Note that Requirement R1 only requires that the TOP establish the target system voltage level and tolerance band. There is no mention of GOP operation. Requirement R2 requires that the TOP document its arrangement of sufficient reactive resources, whether actually used (dispatched) or not, a Planning function (see Measure M2). The Rationale box states: “to ensuring sufficient reactive resources are online or scheduled.” Comment: The use of the word “scheduled” here again has caused confusion. We recommend it be replaced to clarify the meaning, as follows: R2. Each Transmission Operator shall make arrangement for [delete: schedule] sufficient on-line, available reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, making arrangements for reactive generation resources [delete: scheduling], transmission line and reactive resource switching, and using controllable load. We further recommend revising M2 to synchronize it with the revised Requirement R2 above, as follows: M2. Each Transmission Operator shall have evidence of [delete: scheduling]sufficient reactive resources based on their assessments of the system. For the operational planning time horizon, Transmission Operators shall provide copies of assessments used as the basis for determining how resources were [delete: scheduled] made available. The verbiage of R4 should come after R5 is stated. From an organizational perspective, a requirement paragraph on exemptions should come after the referenced requirement.
Generators may be asked by their TOP to operate in other modes. Reword Requirement R1 as follows: R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless the Generator Operator 1) is exempted by the Transmission Operator, [delete: or] 2) is notified by the Transmission Operator to operate in a different viable operating mode (e.g., constant VAR output mode), or 3) has notified the Transmission Operator of one of the following:
Individual
Ronnie C. Hoeinghaus
City of Garland

Yes
1st question: Yes - we agree with this approach 2nd question: We have comments on R2. In ERCOT, the TOP can only plan to respond to voltage issues with the resources they have available. They do not have authority to order generation on line for voltage support nor do they have authority to back down fully loaded generation for voltage support. Only the RC has this authority.
Individual
Thomas Foltz
American Electric Power
No
R5: Rather than allowing only 30 days, we instead recommend that the Generator Owner be allowed to provide the data within the timeframe agreed upon by the GO and either the Transmission Operator or Transmission Planner. This data is often part of larger data submission that may stretch beyond the proposed time horizon. In addition, providing this data to the TP appears to be duplicative of the MOD standards currently being updated. As a result, we recommend removing the TP from this requirement. R6: We recommend that Requirement 6 and its subrequirement be applicable only to the Generator Owner and not split between the Generator Owner and Generator Operator. If both are to be retained, we recommend that the subrequirement be changed to state "*If* the Generator Owner cannot provide tap setting changes as requested, the Generator Owner or Generator Operator should notify the Transmission Operator…"
R3 & R4 do not require communications for all instances. As a result, the severe VSL text must be qualified so that it only applies to those situations where notification is actually necessary.
Individual
Oliver Burke
Entergy Services, Inc.
Agree
SERC OC Review Group
Individual
John Seelke
Public Service Enterprise Group
No
1. R4 and part 4.1 address generator exemptions. R4 requires TOPs to develop criteria for exempting generators from R5, part 5.1. Those criteria should be made available. However, TOPs, not generators, must comply with R5, part 5.1. If the SDT's intent is to exempt specific generators from following a voltage or Reactive Power schedule, we suggest the following rewrite for R4, with no change to part 4.1: R4. Each Transmission Operator shall specify the generator criteria that will exempt Generator Operators of generators that meet these criteria from compliance with the requirement to maintain a voltage or Reactive Power schedule and

publish or provide such criteria upon request. M4 would have to be rewritten, with item 2) and item 3) deleted. Because 1) exempts a generator from having to meet a voltage of Reactive Power Schedule and 2) exempts a generator from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, being exempt from having to meet a voltage schedule in 1) is equivalent to being exempt from 2). Item 3) is addressed by exemptions stated in VAR-002-3, R1 and R2. 2. R5, part 5.1 should have the phrase “in automatic voltage control mode (the AVR is in service and controlling voltage)” stricken since it would not apply to a Reactive Power schedule. In addition, the TOP should not be required to provide voltage or Reactive Power schedules to exempt generators under part 5.1. Finally, the text box for R5 refers to maintaining a schedule for “normal operations.” “Normal operations” is a critical assumption, which we believe is equivalent to “normal operating conditions.” For example, a generator that experiences a fault on its GSU will be outside of any voltage or Reactive Power schedule during that fault. Therefore, part 5.1 should be rewritten: 5.1. Except for exempt generators, the Transmission Operator shall provide the voltage or Reactive Power schedule for the associated Generator Operator and direct the Generator Operator to comply with the schedule during normal operating conditions. 3. R5, part 5.3 should have the phrase “or Reactive Power” inserted after “voltage.”
1. In R1, a generator that is exempt from having to meet a voltage or Reactive Power schedule is exempt from R1. However, a generator that must meet a Reactive Power schedule should also be exempted from R1 because R1only applies to AVRs in the voltage control mode. R1 should be rewritten as follows: R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless the Generator Operator 1) is exempted by the Transmission Operator, or 2) has been directed by its Transmission Operator to meet a Reactive Power schedule, or 3) has notified the Transmission Operator of one of the following: 2. We suggest R2 have “or Reactive Power” inserted in the following phrase: “…for otherwise shall meet the conditions of notifications for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator.” 3. R2, part 2.3 should be moved to M3 since it addresses measures to prove compliance with R2. We suggest the second sentence in M2 be modified as follows: “The Generator Operator shall have evidence to show that the its generator(s) maintained the voltage or Reactive Power schedule provided by the Transmission Operator (either at the location specified by the Transmission Operator or at an alternate location that includes a methodology for converting the schedule from Transmission Operator’s location to the alternate location), or shall have evidence of meeting the conditions of notification for deviations from the voltage schedule provided by the Transmission Operator."
Individual
Shirley Mayadewi
Manitoba Hydro
Yes
Yes

(1) M1 – the language in the second paragraph re: Part 1.1 does not match the language of the requirement itself in that the measure refers only to voltage schedules, not voltage schedules 'and associated tolerance bands'. (2) R3 – without further clarification, 'as necessary' will be interpreted to mean as deemed necessary by the Transmission Operator. (3) M3 – the measure in this part contains more details and is more narrow than the requirement itself. The requirement refers to the operation of 'devices to regulate transmission voltage and reactive flow' while the measure refers to the operation of 'capacitive and inductive resources'. Language should be consistent. (4) R4 – the language goes back and forth between 'generators' and 'generating units' – this should be made consistent. Also, the reference to 'associated notification requirements' presumably refers to the associated notification requirements in R5 but this is not specified. (5) M4 – the qualification language that it refers only to generating units 'in its area' appears only in the measure and not in Part 4.1 itself. (6) R5 – neither Generator nor Step-Up is a defined term so they should not be capitalized. (7) M5 – there is a shift in language here. Generally the measures indicate that the responsible entity 'shall have evidence' and that the evidence 'may include'. In this measure, the language is that the responsible entity 'shall have evidence' and that the evidence 'shall include'. This is much more restrictive and may make compliance more difficult as there is no longer flexibility in the evidence that will meet the criteria of the measure. (8) Compliance, Evidence Retention 1.2 – Measures 5 and 6 are not mentioned. (9) Compliance, Compliance Monitoring, 1.3 - The language refers specifically to processes found in the NERC Rules of Procedure. Generally in draft standards, there is just a list of processes that may be used. The reference included in this draft standard is concerning because MB Hydro has their own Compliance and Monitoring program and has only adopted select aspects of the NERC Rules of Procedure. (10) VSLs, R4 – the words 'of the Generator Operator' are missing from the end of this section. (11) VSLs, R5 – the words 'and associated tolerance bands' is missing from Moderate VSL after 'voltage schedules' and is not fully referenced in Severe VSL. (12) VSLs, R6 – the words 'Documentation specifying requiring tap changes was provided to the Generator Owner but' could be inserted at the start of each of the Lower VSL and Severe VSL.
Although Manitoba Hydro is in general agreement with the standards, we have the following comments: (1) M1 – the language in the measure is that evidence 'must' include which is a shift from typical language that evidence 'may' include. It also seems to be a shift from what is discussed in the rationale that the measure has been updated to include some of the evidence that 'can be used' for compliance purposes as the evidence listed is made mandatory by the 'must'. (2) R1 – footnote 2 and 4 seems to be missing (3) M2 – refers to 'unit' while rest of standard refers to generator. For part 2.3, I believe the reference to 'units' should be to 'Generator Operators'. (4) M3 –the acronym GOP is used while every other reference in the standard is to Generator Operator. (5) M4 – the language between the measure and the requirement differs slightly. The measure requires evidence of notification within 30 minutes of 'the recognition' of a change, while the requirement requires notification within 30 minutes of 'becoming aware' of a change. (6) M5 – there is nothing in the measure that addresses the timeline upon which the Generator Owner is required to provide information. (7) R6/M6 – the requirement and measure refers to both Generator Owner and Generator Operator. Its not

clear whether this is intentional or inadvertent. The words 'and provided technical justification' should be added to the end of M6 after 'tap specifications'. (8) Compliance, 1.2 – there is no time limit on the requirement for a Generator Owner to keep documentation on its step up and auxillary transformers. Its it meant to be for as long as that version is current? (9) Compliance, Compliance Monitoring, 1.3 - The language refers specifically to processes found in the NERC Rules of Procedure. Generally in draft standards, there is just a list of processes that may be used. The reference included in this draft standard is concerning because MB Hydro has their own Compliance and Monitoring program and has only adopted select aspects of the NERC Rules of Procedure.

(1) VSLs, - not clear why the references throughout the VSLs are to 'responsible entity' when the requirements are clear as to an obligation on either the Generator Owner or Generator Operator. Those entities should be listed in the VSLs as they are in the requirements and standards. (2) VSLs, R2, Severe VSL – the word 'Power' is missing after 'Reactive'. Also doesn't mention that the Generator Operator 'did not have an exemption'. (3) VSLs, R3 and R4 – would read better if stated 'the Generator Operator did not make the notification of a change that lasted more than 15 minutes within 30 minutes of the first occurrence of the change as required'.

Individual

Jonathan Appelbaum

The United Illuminating Company

No

Please note that my affirmative ballot vote was in error. We are voting NO on VAR-001. Since there is no catchall section for comments on VAR-001, we are providing comments here. Although We do agree with the removal of duplicative requirements, we are voting No on VAR-001. VAR-001 R2 remove everything after the but not limited to phrase. The various methods to obtain reactive power do not belong in the requirement but they can be included in the measure. VAR-001 R3: Clearly this is something a TOP perfroms but the compliance evidence will be overwhelming. The TOP is being asked to demonstrate that it has constantly monitored reactive and provided direction to operate reactive devices. This will require the retention of the evidence of why a reactive adjustment was necessary as well as the various adjustments made. This would mean maintaining snapshots of the normal operation of the system, records of adjustments, corrections, etc.

Yes

Individual

Angela P Gaines

Portland General Electric Co

PGE appreciates NERC's efforts to revise VAR-002. The standard as whole is a significant improvement from the previous version. However, R3 still requires a 30 minute notification for notifying the transmission operator (TOP). The 30 minute limit is a challenge for generator operations to meet. The SDT should consider increasing this limit to 60 minutes. In addition,

the requirement should allow registered entities to set up an alternative method to provide real-time AVR/PSS/voltage control device telemetry. This method would eliminate a need for notifying the transmission operator within 30 minutes. Also, the NERC glossary should fully define the term, 'voltage controlling device', as stated in R3.
Group
Dominion
Louis Slade
Yes
Yes
Yes. In order to be consistent, Dominion also suggests reviewing the need to use "its associated Transmission Operator" throughout the entire standard (i.e. R1 - "has notified the Transmission Operator", R2/M2 - "provided by the Transmission Operator", R6 - "specifications provided by the Transmission Operator", etc).
Individual
Anthony Jablonski
ReliabilityFirst
1. General Comment - ReliabilityFirst believes that due to the interdependency of the VAR-001-4 and VAR-002-3 standards, the SDT should consider combining the two into a single standard. It would be a natural progression to list a requirement associated with the Transmission Operator having it immediately followed by the associated Generator Owner/Operator requirement. ReliabilityFirst believes the Generator Owner/Operator would benefit from knowing what is being required of the associated Transmission Operator. Specific VAR-002-3 Comments 1. Requirement R6 - The parent Requirement R6 is applicable to the Generator Owner while the sub-part 6.1 specifies the Generator Operator. The same applicable entity listed in the "parent" requirement should be the same as any associated sub-parts. Since only Requirements are enforceable in Reliability Standards, if the Generator Operator fails to notify the Transmission Operator and fails to provide the technical justification per sub-part 6.1, a Possible Violation would be rolled up to Requirement R6. This would not work since Requirement R6 is only applicable to the Generator Owner. ReliabilityFirst completely understands that the Generator Owner is the responsible entity for ensuring that transformer tap positions are changed and that the Generator Operator is the entity responsible for actually performing the change. ReliabilityFirst recommends splitting Requirement R6 and sub-part 6.1 into two separate requirements (i.e., create a new Requirement R7 using the language of sub-part 6.1).
Group
Arizona Public Service Company
Janet Smith, Regulatory Affairs Supervisor
Yes
Yes

Yes
The VRF of “high” is not justified for any of the requirements. We would suggest a VRF of “medium” or “low”. If the drafting team thinks a VRF of “high “ is justified, some reasoning should be provided by the team. Lack of documented voltage schedules does not mean the system is being operated unreliably. Units are still being operated in AVR mode as required by other schedules and transmission operators coordinate the voltage schedules as needed.
Individual
Bill Fowler
City of Tallahassee
Agree
FMPA
Individual
Cheryl Moseley
Electric Reliability Council of Texas, Inc.
Yes
ERCOT agrees it is clear voltage limits are to be monitored as either SOLs or IROLs. However it seems the SDT could make more changes to clear up more items. A. VAR-001 R3 grammatical: recommend deleting “as necessary” from this sentence. It adds no value and is not needed. B. It appears VAR-001 R4 allows the TOP to not comply with the VAR Standards by utilizing exemptions?
Yes
ERCOT agrees that duplicative requirements should be removed. However, the standard would benefit from additional revisions. A. R1 and R5 should be merged. This could be accomplished in the following manner: “Each Transmission Operator shall notify associated RCs and adjacent TOPs, and specify assigned GOs the a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan required forassigned GOs to operate within System Operating Limits and Interconnection Reliability Operating Limits. B. The second sentence of VAR-001 R2 is not needed. This is not an actionable requirement, but rather is an instruction as to how it’s to be done. The 2nd sentence is not a requirement. C. Recommend deleting from R5.1 the words, “…in automatic voltage control mode (the AVR is in service and controlling voltage).” The standard should establish what needs to be done, and how the GO elects to comply with the requirement should be left to the discretion of the GO. Furthermore, VAR-002 requires the GO to have its AVR in service and in auto, so this requirement is also redundant. D. It appears that VAR-001 R6 is redundant to R5.3. Also see comments on VAR-002 R6.
Yes. ERCOT supports the revisions but recommends that the SDT consider the following additional issues: A. Consider revising R2 as follows: “The generator shall follow the voltage schedule assigned by its TOP.” Otherwise this is effectively a “fill in the blank” standard. As drafted, R2 also establishes “how” entities are required to meet their obligations. The standards should establish what is required and leave it to the discretion of the functional entity to determine how to meet the relevant objective. R3 provides the needed notification.

B. VAR-002 R2 requires GOs to notify TOPs of voltage. This seems to create an unnecessary requirement given that TOPs are obligated to monitor system voltage. C. VAR-002 R2.1 appears to require that GOs maintain the voltage assigned. Consistent with the general principle that the standards should establish what is required, how GOs maintain voltage assignments should be within the discretion of the entity. D. VAR-002 R2.2 is redundant. If GOs have to maintain the voltage assigned, this is unnecessary. E. VAR-002 R2.3 is redundant if a GO has to maintain the voltage assigned. F. VAR-002 M2 includes a statement that has a "will" in it. This effectively establishes a requirement. Measures are means of demonstrating compliance, they are not requirements. The measure should be revised accordingly. G. VAR-002 R3 should state that the notification is not required during startup or shutdown. A TOP can determine from telemetered information when a unit is operating below their lower stability limit. Requiring reporting of AVR/PSS status coming on/going off line is not necessary and creates unnecessary distractions that could undermine reliability. H. The 2nd sentence of R3 is redundant with the 1st. If notification is required within 30 minutes it is implicit that the entity does not have to notify within 15 minutes? I. If a GO maintains the assigned voltage, the status of a GO's AVR is irrelevant. If a GO failed to maintain the assigned voltage they are in violation of R2 regardless of the reason. M3 seems to unnecessarily create the potential for double violation issue on a reporting obligation.J. The standard should make clear that telemetry on status of AVRs and PSSs to TOPs meets this notification obligation. The term 'notify' seems to imply a manual written or verbal communication. K. VAR-002 R4 second sentence dealing with 15 min language- - please refer to R3/M3 comments. L. VAR-002 R5 – This requirement is unnecessary if GOs have to respond to any reasonable data request from their TOP. M. VAR-002 R6 is redundant with R2. If a GO has to maintain assigned voltage, and adjusting taps is necessary to do that, then this instructional requirement is not needed. If R6 is kept, in VAR-002-3 Standard the entity changes in R6.1. VAR-001-4 states the TOP will work with the GO in R6. Then in VAR-002-3 it states the following: R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. [Violation Risk Factor: Lower] [Time Horizon: Real-time Operations] 6.1. If the Generator Operator cannot comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification. Why does it change from the GO to the GOP? The SDT should address the differences within VAR-002-3 to mirror R6 in the VAR-001-4 Standard.
Individual
Michael Falvo
Independent Electricity System Operator
Yes
We support this direction and the SDT's decision to not reiterate or duplicate the voltage assessment requirements already addressed by the FAC and TOP standards.
Yes

We support the SDT's proposal to remove the requirements that may be redundant with other standards. We do not have any comments on the requirements, Measures or VRFs, but we do have some comments on the VSLs: a. R1: The word "schedule" after "system voltage" is missing from the VSL. b. There is inconsistency in the tense used in various VSLs – some are in present tense while others in past tense. Please review and revise as appropriate.
We agree with most of the proposed changes, but would suggest the following changes to more effective convey the intent of Requirement R3 and Measure M3. a. R3: The wording "the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator" is not a direct action and may not be measurable. We suggest to revise it to read: "the Generator Owner shall implement the transformer tap positions according to the specifications provided by the Transmission Operator…." b. M3: We suggest it be reworded to require demonstration of compliance rather than to require actions which should have been stipulated in the requirement. Specifically, we proposed the last part in Measure M3 be revised to: "…therefore, if a status change lasts more than 15 minutes, the GOP shall provide evidence such as system log, electronic message or a transmittal letter that it notified its associated Transmission Operator within 30 minutes of when the change first occurred." We further propose that the SDT insert the evidence language into the first sentence of Measure M3 which asks for evidence that the Generator notified its associated Transmission Operator within 30 minutes of the change identified in Requirement R3. We assess the changes proposed under Q2 and Q 3, above, are not substantive and do not materially change the intent or content of the standards. Therefore, if the standards receives 2/3 majority approval at the ballot, these changes can be implemented and posted for recirculating ballot without having to post and ballot the standards for a successive ballot.
We support the proposed VRFs and VSLs.
Group
Southern Company: Southern Company Services, Inc.; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing
Marcus Pelt
Yes
R1: The modifications in this version of VAR-001 R1 are good because they standards that are now enforceable, particularly FAC-011 and FAC-014. M2: All Transmission Operators are required to run contingency analysis on the real time system on a periodic basis per TOP-008-1 R4. We suggest modifying VAR-001 M2 to state: "If the assessment is performed in the Operations Planning Horizon, Transmission Operators shall provide copies of assessments used as the basis for how resources were scheduled." M3: Actions are not always required to be taken because of automatic settings of reactive devices. We suggest modifying VAR-001 M3 to state: "Each Transmission Operator shall have evidence that actions were taken as necessary to operate capacitive and inductive resources as needed in Real-time. This may include directions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments." R5.3 states, "The Transmission Operator

shall provide the criteria used to develop voltage schedules and associated tolerance bands to the Generator Operator within 30 days of receiving a request." We suggest that this requirement is removed due to administrative burden. We recognize the need for transpency; however, this requirement does not serve a reliabity purpose.
Yes
: The High VSL for VAR-001 R4 should be changed from the proposed state to "The TOP has exemption criteria, but did not notify the GOP." As it is currently written, the TOP satisfied R4, but simply cannot show documentation to prove the satisfaction. The proposed change wording focuses on the TOP not satisfying the requirement. The first clause in the Severe VSL for VAR-001 R5 should be corrected to state "voltage or Reactive Power schedules." In addition, the Severe VSL for VAR-001 R5 should have another OR clause to include the failure to comply with R5.3.
Adding "testing" to VAR-002 R1 was a good move. This will serve to avoid nuisance notifications for routine testing. Modifying VAR-002 R2 to allow the TOP to specify notification instructions is a good move. Each TOP will be able to specify notifications appropriate for characteristics of their transmission system. Removing the VAR-002 R3 notification of duration was a good move - the GO often does not know how long it will be out until some troubleshooting is performed. Splitting the old R3 into new R3 and new R4 was a good move. This separates two distinct types of trouble. The addition of "after becoming aware of a change in reactive capability" to the new R4 was a good move - this change is not always immediately evident. M4 should be modified to match R4 - "after becoming aware of a change needs to appear in M4".
The removal of "up to 45 minutes for the R2 VSL was a major improvement. The comma in the second and third OR statements of the Severe VSL for VAR-002 R2 is not needed. The comma in the second OR statement of the Severe VSL for VAR-002 R6 is not needed.
Individual
Brett Holland
Kansas City Power & Light
Yes
I agree with the approach to condense standards if they are duplicated in other standards.
NO. R2 is the part of VAR-002 that I disagree with because the Transmission System Operator is monitoring the system voltage and notifies each generating facility when they need to raise/lower voltage in that particular area of the system. If the voltage at the generating facility is high/low the TSO has received an alarm and will be notifying the plants control operator to correct the voltage and there already is a requirement for the control operators to comply with the TSO request.
No.
Individual
Andrew Z. Pusztai
American Transmission Company, LLC

Yes
No
ATC agrees with the approach in removing any duplicate requirements. ATC also has a couple comments and is recommending the following changes for the drafting team to consider: 1. For consistency, Measure M2, 2nd sentence should be reworded as follows: “For the operational planning time horizon, Transmission Operators shall “have evidence of assessments” used as the basis for how resources were scheduled” The current wording of “shall provide copies” imposes an action that is not included in the associated requirement R2. 2. The following from requirement R2: “Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load” implies that all of the items listed need to be considered. If the intent is that the items are intended to be examples it is suggested that the words “including , but not limited to” be replaced by “such as”.
Individual
Alice Ireland
Xcel Energy
Yes
Yes
Xcel Energy appreciates the hard work of the Standard Drafting Team. We recognize that significant effort has been put into the modifications of the VAR-001 and VAR-002 standards and we applaud the direction the team is moving. We are voting Negative on VAR-001-4 for one reason which we explain below. Xcel Energy believes that the WECC Regional Variance should not replace R4 in the NERC standard based on the rationale provided for modifications to the proposed R4. Instead, WECC Regional Variance Requirement E.A.13 should be removed and the remaining Regional Variance Requirements should supplement the NERC Requirements in the Western Interconnection. As proposed, the NERC standard states that the TOP is not bound to provide a voltage schedule for each BES generator; however , due to the WECC variance, the TOP would be found in violation if any BES Generator was not provided a voltage schedule. In order to resolve the issue, Xcel Energy asks the drafting team to delete E.A.13 in its entirety and modify the language of the Regional Variance to state that the additional requirements are for in addition to the NERC requirements. Once this modification is made, Xcel Energy could support the proposed standard.
Yes. Xcel Energy appreciates the hard work of the Standard Drafting Team. We recognize that significant effort has been put into the modifications of the VAR-001 and VAR-002 standards and we applaud the direction the team is moving. We are voting Negative on VAR-002 for one reason which we explain below. Xcel Energy understands that the existing language in the VAR-002 standard uses the term “status change” but believe that this term is not well defined and is subject to different interpretations. AVRs and PSSs are designed to cycle based on the parameters being monitored by the devices. This as-designed cycling may be interpreted as a status change. We note here that the drafting team does not use the term status change in its

rationale statement. Instead, the rationale statement is much clearer in meaning than the proposed requirement language. To address Xcel Energy's concern, we request that the drafting team replace the first sentence in Requirement R3 with the following sentence. (We believe that this change does not constitute a significant modification but is instead providing more clarity in the requirement language based on the wording of the Rationale for Requirement R3.) "Each Generator Operator shall notify its associated Transmission Operator when the AVR, power system stabilizer, or alternative voltage controlling device goes out of service within 30 minutes of the change."
If the drafting team makes the requested modifications to the requirements, Xcel Energy has no concerns with either the VSLs or VRFs.
Individual
Lynda Kupfer
Puget Sound Energy
- The implementation period might be as short as one day as the Effective Date section is currently formulated. For example, if approval occurs on 12/31/2013, the first day of the first calendar quarter after that date would be 1/1/2014. A short implementation period for this standard is appropriate; however, language such as "The first day of the first calendar quarter that is one month beyond the date that this standard is approved..." would ensure that a minimum of one month is available for implementation.
Yes
- The first paragraph of the Regional Variance section of VAR-001 should be updated to reflect that requirements R3 and R4 of the current standard are requirements R4 and R5 in the proposed standard. - M4 should be updated to reflect that the Generator Operator "must notify its associated Transmission Operator within 30 minutes of when the change first occurred. after becoming aware of the change in reactive capability" to be consistent with the wording of R4.
Group
Salt River Project
Bob Steiger
Yes
Yes
Yes
No.
Individual
Silvia Parada Mitchell
NextEra Energy
Agree
MidAmerican
Individual

Rjick Terrill
Luminant Generation
Yes
Yes
Luminant appreciates the work of the SDT and agrees that most of the revisions are appropriate, and that the intent of the SDT to allow for more than one method of voltage support is correct. However, as written, VAR-002, R2, does not clearly identify that generators can provide voltage support by a method other than maintaining a voltage schedule, continuously monitoring voltage and reporting deviations from the voltage schedule. In some areas of the country, the TOP monitors the voltage at all busses in it area, including the busses connecting generators, and directs generators to modify reactive output as the TOP requests. Luminant believes the language of VAR-002, R2 should be modified to provide clarity as follows: R2. Unless exempted by the Transmission Operator, each Generator Operator shall provide generator voltage support or Reactive Power support (within each generating Facility's capabilities4) as follows: [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] 2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to provide voltage or Reactive Power support directed by the Transmission Operator. 2.2. When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the request cannot be met. 2.3. When directed by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule3 (within each generating Facility's capabilities4) provided by the Transmission Operator, and shall meet the conditions of notification for deviations from the voltage schedule provided by the Transmission Operator. 2..3.1 Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator. With this proposed language, the GOP would have to maintain a voltage schedule and report deviations only if that is the normal method of voltage support requested by the TOP. 2.3 and 2.3.1 would only apply to a GOP that maintains a voltage schedule. The measures for 2.1 and 2.2 would include operator logs, voice recordings, etc.
Individual
Andrew Gallo
City of Austin dba Austin Energy
Yes
Yes
City of Austin dba Austin Energy (AE) agrees with removing duplication. AE does not have any comments about the requirements, but requests the SDT review the VSL for R2 because the text does not match the requirement text.
Yes.

No. Because NERC has not provided an area for "Additional Comments," we are adding them here. The City of Austin dba Austin Energy (AE) commends the Standard Drafting Team's efforts related to Project 2013-04. The quality of the standard is enhanced over previous approved versions, providing additional clarity and compliance sensitivity. AE respectfully submits the following comments on VAR-001-4 and VAR-002-3 to the Standard Drafting Team (SDT): VAR-002-3, R1, Pertaining to the phrase "… unless the Generator Operator 1) is exempted by the Transmission Operator, or 2) has notified the Transmission Operator…" AE recommends the SDT clarify whether the TOP may exempt all the units represented by a GOP, or instead, specific generating facilities or a generator bus. AE suggests altering the language to read "… unless 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator…" This change will make the language in VAR-002-3 R1 consistent with the language in VAR-001-4 R4. VAR-002-3, R2.3: The requirement makes it mandatory for Generator Operators to monitor the voltage at the location specified in the voltage schedule or have a methodology for converting the scheduled voltage specified by the TOP. This may imply that the Generator Operator should make voltage corrections independent from the TOP. AE believes that maintaining the appropriate transmission level voltage is the key for sustaining system stability and that responsibility falls on the TOP. Because the TOP already monitors the transmission level voltages, the R2.3 requirement for GOPs to monitor voltage is redundant and may create a situation where the TOP and GOP do not agree on the monitored value (i.e. the voltage readings can be different due to step-up voltage equipment). To avoid confusion and potential compliance ambiguities, AE suggests the standard specifically state TOPs are responsible for monitoring the system voltage schedule and notifying the GOP when voltage drifts outside acceptable parameters. This appears to be a common practice of operating the grid. The GOP will be responsible for meeting the reactive support requested by the TOP. If the GOP cannot meet the reactive support requested by the TOP, the GOP should have to notify the TOP. AE suggests the following: Add "Transmission Operators" under R4 – "4.3 Transmission Operators", and alter R2.3 to: "Each Transmission Operator shall monitor the system voltage and notify its associated GOPs for additional voltage support if system voltage fails to meet the voltage schedule. If the GOP cannot meet the reactive support requested by the TOP due to equipment limitations, it shall notify the TOP of the limitations within 15 minutes. VAR-002-3, R4: AE believes the phrase "a change in reactive capability" is vague. As written, even the slightest change in reactive capability must be reported to the TOP. Is it the SDT intent the TOP be notified if a reactive capability (leading or lagging) of a generation resource changes by 1 MVAR? Detecting and reporting small reductions in reactive capability will create onerous reporting. AE recommends the following for R4: "Each Generator Operator shall notify its associated Transmission Operator within 30 minutes that a resource's reactive capability changed by 20 MVAR or 10%, whichever is greater, of the previously provided reactive capability due to factors other than a status change described in Requirement R3."
Individual
David Jendras
Ameren

Yes
No
We request that the SDT leave the language as currently used in VAR-001-2, R4.
We request that the SDT support adding to R3 the "…after becoming aware of…" language now proposed for R4. This will help reduce the number of unnecessary GOP notifications to the TOP.
Group
Florida Municipal Power Agency
Frank Gaffney
Yes
Yes
FMPA appreciates the efforts of the SDT to remove some of the duplicative requirements of the VAR standards with other standards (e.g., TOP and FAC standards). However, FMPA is voting Negative because we believe more requirements ought to be treated in the same fashion as described in our earlier comments on the September posting, as provided in a mapping document submitted directly the the SDT to better illustrate those duplications, and as summarized below. VAR-001-4 R2 is duplicative of the requirements of TOPs to plan for and operate to SOLs in the TOP and FAC standards. In order to plan to and operate to SOLs, TOPs must schedule sufficient reactive resources, or they will violate those requirements (just as must-run generators need to be scheduled, yet those are not discussed within the standards). Operating to SOLs is results based, VAR-001-4 R2 is not. VAR-001-4 R2 ought to be deleted. VAR-001-4 R3 is duplicative of requirements of TOPs to plan for and operate to SOLs as described above. As far as TOPs ability to direct, that is covered in TOP-001. VAR-001-4 R3 should be deleted. Although FMPA supports both VAR-001-4 R1 and R5, we wonder if there is some duplication between those requirements and whether they can be combined into a single requirement.
FMPA appreciates these changes. However, VAR-002-3 remains duplicative of other requirements within the standards VAR-002-3 R2, bullet 2.3 is duplicative of TOP-001-2 R1. Both require the GOP to follow the direction of the TOP. Bullet 2.3 should be deleted. VAR-002-3 R5 is duplicative of TOP-003-2 and should be deleted. VAR-002-3 R5 requires the GO to provide the TOP information about the GSU. TOP-003-2 R5 requires the GO to submit data as specified by the TOP. The TOP cannot perform their obligations of VAR-001-4 R6 to specify GSU tap positions without the data of VAR-002-3 R5; however, the TOP will ask for that data in accordance with TOP-003-2 R3. Hence, these requirements are redundant and VAR-002-3 R5 ought to be deleted. FMPA also wonders how duplication between TOP-003-2 that gives TOPs a carte blanche opportunity to develop data requests on any information they need and the notification requirements of VAR-002-3 will be managed. In other words, the TOP can develop their TOP-003-2 data specification to include the notification requirements of VAR-002-3 and as such GOPs would be subject to double jeopardy risk.
Group

Tennessee Valley Authority
Brandy Spraker
Yes
Yes
The SDT is requested to clarify the word “directions” as used in M3. The word “directions” is close to, but not, the word “directive” which has a very specific meaning. If the intent is to capture directives, then the word directives should be used. If the intent is to capture communications that are not directives, then the word “directions” should be replaced with wording that is not so close to the word “directives.” Current M3 draft language: M3. Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as needed in Real-time. This may include directions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments. The SDT is requested to consider a modification to R4: Current R4 draft language: R4. The Transmission Operator shall specify the criteria that will exempt generators from compliance with the requirements defined in Requirement R5, part 5.1, and any associated notification requirements. Suggested modification to R4: R4. The Transmission Operator shall specify the criteria, ADD: “if any” that will exempt generators from compliance with the requirements defined in Requirement R5, part 5.1, and any associated notification requirements.
Yes
No comments
Individual
Kathleen Goodman
ISO New England Inc.
Agree
IRC SRC
Individual
Karen Webb
City of Tallahassee - Electric Utility
Agree
FMPA
Group
PacifiCorp
Ryan Millard
Yes
Yes
PacifiCorp supports MidAmerican's comments.
The following change to requirement R4 is recommended: “Reactive capability changes due to change in the wind speed for wind generators or a change in the solar resource for solar

facilities do not require Transmission Operator notification." Given the variable nature of wind, the reliance of weather forecasting does not rest explicitly with the GOP. The TOP has access to weather forecasting that would make the need of notification by the GOP unnecessary. Additionally, PacifiCorp supports the following comments from MidAmerican: We support the deletion of the language regarding notification of the expected duration of a change in status. At the time a status change occurs it is often difficult to provide a meaningful estimate of the duration of the change. Requirement 3 should be revised to state – Notification must be made within 30 minutes of becoming aware of the change from automatic controlling voltage for the AVR, and from in-service of the PSS. Measure 3 should be revised to reflect this as well. The revised VAR-002 R2.1 removes the 15 minute deviation criteria for notification by Generator Operators to Transmission Operators. The revised VAR-001-4 requires Transmission Operators to provide notification requirements. The drafting team in the consideration of comments explained "In an effort to remove prescriptive notification requirements for the entire continent" the change was made. This leaves the Generator Operators at the mercy of Transmission Operators who could potentially set a no deviation criteria. It is recommended that a comprise be struck by specifying a limit on the criteria such as "no less than 15 minutes".
Individual
Robert L. Dintelman
Utility System Efficiencies, Inc.
Yes
Yes
Many of the other standards that require the provision of this sort of information to the RC and neighboring entities includes a requirement that the entity respond to comments/concerns from the copied entities. Why not here? R2 appears to be a little ambiguous; does this apply to all contingency conditions? Just N-1? Only those chosen by the TOP? This would appear to be hard to determine compliance by the Region. It looks like R6 assumes that the GO has a non-LTC transformer. We are seeing LTCs in generation facilities; shouldn't this be modified to address the LTC GSUs? For M2 and M3 particularly, Evidence Retention could require a lot of data for 12 months.
For R2, what about the situation where the generator cannot actually influence the voltage? There may be a significant amount of hours where they can't keep the voltage in range. For M2, for a generator that does not have an AVR, what type of evidence is required to show compliance for 8760 hours per year? Sounds like a lot of evidence potentially.
No
Group
Duke Energy
Colby Bellville
Yes
Yes

Duke Energy approves of the approach of removing duplicative requirements based on other standards. Duke Energy seeks clarification on the definition of “system voltage schedule” and believes that once this is more clearly defined, it should be added to the NERC Glossary of Terms. The Rationale for Requirement 1 discusses the TOP setting voltage or Reactive Power schedules with associated tolerance bands. However, Requirement 1 makes no mention of using Reactive Power schedules. Is the use of Reactive Power Schedules implied in Requirement 1? Duke Energy suggests changing “Each Transmission Operator shall schedule” to “Each Transmission Operator shall maintain” in Requirement 2 for more clarity. In Duke Energy’s opinion, not all reactive resources can be “scheduled” in order to regulate voltage levels. For example, SVCs cannot be scheduled, the reactive resources of an SVC dynamically change to maintain set voltage levels. The TOP needs to ensure that adequate static and dynamic reactive resources are availble to the System Operator in real time to support the Reliability needs of the BES. Reliability Studies are performed in the Operations Planning horizon to ensure that reactive resources are adequate to support the planned BES configuration.
No. Duke Energy does not agree with the revisions made. Duke Energy is unclear whether the exemptions referenced in R1 and R2 in VAR-002-3 are the same as the exemptions created in VAR-001-4 R4. We believe using the word “exempted” in multiple requirements without identifying the origin of the exemption is a cause of confusion. Requirement 2 - Revise R2.1 to read, ” When a generator’s AVR is out of service, the generator does not have an AVR, or is not in a TOP approved mode of AVR operation as specified in R1, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator. “ The VRF/VSL for Requirement 2 would need to be modified if this change is made. Requirement 3 – Duke Energy is unclear as to what is considered an alternative voltage controlling device. Duke Energy prefers the language in the previous draft of this standard which states, “Each Generator Operator shall notify its associated Transmission Operator of a status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability within 30 minutes of the change. If the status has been restored within the first 15 minutes of such change, then there is no need to call the TOP. “ The language in the previous draft provides more clarity on what would prompt notification from a GOP to a TOP based on status or capability change. Requirement 5 – Duke Energy would like the SDT to review and verify that the Transmission Planner, and not the Planning Authority or Planning Coordinator, is the correct functional entity for this requirement. Lastly, Duke Energy would like to clarify that we encouraged our ballot body members to vote “Negative” on this ballot for reasons stipulated above. However, one of our ballot body members mistakenly voted “Affirmative” which was in error. Our decision to vote “Negative” on this ballot was unanimous among all those involved. We apologize for any confusion this may have caused.
See our comments on VAR-002 Requirement 2.
Individual
Melissa Kurtz

US Army Corps of Engineers
Agree
MRO NSRF
Group
Western Area Power Administration
Lloyd A. Linke
Agree
US Bureau of Reclamation.
Group
PPL NERC Registered Affiliates
Brent Ingebrigtson
Yes
Yes
An additional change should be made – R3 should state that when real-time status is provided to the TOP electronically there is no need for additional notification.
Time requirements are not necessarily arbitrary, and it is in fact important to establish explicit and meaningful criteria regarding the acceptable time (and magnitude) of voltage schedule deviations. The principal reason that VAR-002 has been so troublesome in the past is that one could interpret a 10 MW hydro unit being out of the bandwidth by 0.1 kV for 1 minute as constituting a violation, despite there being no meaningful impact on BES reliability. There are moreover many occasions when a the system voltage unavoidably strays briefly outside the bandwidth due to a disturbance or because there are step-changes in the TOP's voltage schedule. VAR-002-3 makes a slight movement in the right direction by stating in R2 that a unit must keep within the bandwidth or, "meet the conditions of notification," but there is nothing in VAR-001 or 002 to require TOPs to create justifiable requirements in this respect. We presently suffer under a system in which meaningless violations are spawned by abusive practices, such as establishing a bandwidth of only +/- 0.5%, and VAR-001 and 002 should be revised in a fashion that prohibits such practices.
Individual
Gerald G Farringer
Consumers Energyu
Yes
Yes
This is a two part question with only one YES/NO answer. YES we agree with the approach. YES we have questions or comments on the remaining revised requirements. In R4, there should be a statement that the TOP will publish the exemption criteria to GOPs in the area. A consideration should be made to reserves R1 and R5. It is imperative both get the voltage schedules but if the GOP does not have them there is no control.
It is important to clarify the statement of "notification requirements." In the context of VAR-

002 this term refers to the notification from the GOP to the TOP on status of the AVR, Ability to follow the voltage schedule or the status of the unit. We would suggest the timing on VAR-002 R3 be similar to R4 in that the clock starts at the awareness of the GOP of a status change. VAR-001 clearly defines a Voltage or Reactive Power schedule. We suggest this be done in VAR-002 for consistency rather than the footnotes provided.
Individual
Chris Scanlon
Exelon Companies
Yes
Yes
Yes, agree with approach, no additional comments relating to requirements. Exelon companies would vote Affirmative for VAR-001-4 if it were being balloted separately from VAR-002-3.
Exelon appreciates changes made to the standard the current revision is a significant improvement on the previous draft version. As mentioned above, we support VAR-001-4 as written but feel important issues remain unaddressed with VAR-002-3 and will therefore vote Negative. Our principal concerns include: VAR-002-3 Effective Dates. The Implementation Plan for VAR-001-4 and VAR-002-3 requires the new Standard revisions to be implemented the first day of the first calendar quarter after applicable regulatory approval. Although the Implementation Plan justification states that the VAR-002 standard “cannot go into effect without the new TOP schedules and notification requirements” it does not address the implementation associated with changes to VAR-002 with respect to status notifications. This is not sufficient time to allow generating units to implement training of operators and procedural changes necessary to implement the proposed changes to notification requirements associated with the AVR, PSS or alternative voltage controlling device. We suggest at least a 6 month implementation period following regulatory approval. VAR-002 R1 or in the applicability section of the standard. This standard or requirement does not account for dispersed Generation (such as wind or solar as found in the new BES definition). These generators may not have traditional AVR, may only provide limited Reactive resources and the individual elements may not have AVR or be capable of operating in Voltage control mode. VAR-002-3 R2.3 Exelon believes it is reasonable to allow the GOP to monitor the voltage at the location specified in their TOP issued voltage schedule by allowing the GOP to monitor at a different location by applying a methodology for converting the voltage monitored; however, the conversion method should be communicated and agreed to by the Transmission Operator. There is not a one for one conversion between grid voltage and terminal voltage and both parties should agree on the conversion method and monitoring point to avoid any future audit or implementation issues. VAR-002-3 R3 Exelon agrees with the fifteen (15) minutes to allow a GOP time to resolve an issue before having to notify the TOP of a status or capability change; however, postponing the notification by 15 minutes to alleviate short term / nuisance notifications has the effect, as written, of shortening the notification window to 15 minutes. Fifteen minutes is not a reasonable timeframe for such notifications to occur,

especially in large dispersed fleet operators where the GOPs do not communicate directly to their TOP and must notify via a third party (e.g., an independent generation dispatching organization). Exelon suggests that the 30 minute notification timeframe for a status change on the AVR, PPS or alternative voltage controlling device be started following the inability to restore within 15 minutes. VAR-002-3 R4 Exelon suggests that the VAR SDT provide guidance to the industry on examples of reactive capability changes that would require notification to the TOP within 30 minutes after becoming aware of a change. The only guidance provided to date is in the VAR-002 Compliance Analysis Report dated August, 2010.
We understand that R3 and R4 are binary requirements, (did or did not notify in 30 minutes), but it seems unreasonable that a complete failure to notify would have the same VSL as a notification that is one or five minutes late.
Group
SPP Standards Review Group
Robert Rhodes
Yes
We thank the drafting team for taking this stance in not establishing details in the VAR standards and relying on those that already exist within defined SOLs and IROLs. Adding additional detail here would be redundant and possibly conflicting with requirements in other standards.
Yes
We agree with the retirement of redundant requirements and suggest that the drafting team delete R2 and R3 in addition to the other deletions already proposed. R2 is redundant with the pending TOP-002-3, R1. R3 is redundant with pending TOP-001-2, R7 and R9.
Yes. We also offer the following comments on the two standards. Generic Comments on VAR-001-4 We recommend changing ‘real time’ in the Purpose to ‘Real-time’ as defined in the NERC Glossary of Terms. We suggest rewording R1.1 to the following: ‘Each Transmission Operator shall provide a copy of the voltage schedules as specified in R1 to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of such a request.’ Although we have proposed deleting R2, if the drafting team decides to keep it, we recommend deleting the last sentence in R2. It is really an example and doesn’t contribute substantially to the requirement. We also recommended deleting R3 but if the drafting team decides to keep it, we suggest adding ‘to operate within SOLs and IROLs’ following ‘as necessary’ at the end of the requirement. The use of the term ‘direct’ in R3 and R5.1 lead to implications of issuing directives. To get away from this situation, we suggest substituting ‘instruct’ for ‘direct’. This change will also need to be reflected in the Measures and the VSLs. Since R4 contains an exemption for R5, we suggest reordering requirements R4 and R5 such that R5 becomes R4 and R4 becomes R5. That way the exemption follows the requirement. We suggest the drafting team delete the phrase ‘…at the Transmission Operator’s discretion.’ at the end of R5. We suggest changing ’associated’ to ‘applicable’ in and deleting the redundant phrase at the end of R5.1. The requirement would then read: ‘The Transmission Operator shall provide the voltage or Reactive Power schedule to the applicable Generator

Operator.' The Measure will also need to be revised to correspond with the revised requirement. We recommend adding 'for that criteria' following 'request' at the end of R5.3. We recommend changing the Time Horizon in R6 to Long-Term Planning since the Transmission Planner is typically the entity that will determine when a tap change is necessary and will notify the Transmission Operator that it needs to be done. In the Rationale Box for R6 there is a reference to VAR capability and tap setting. We suggest rewording that sentence to the following: 'If the tap setting is not properly set, then the VARs available from that unit can be affected.' The Severe VSL for R3 contains 'real-time'. It needs to be 'Real-time'. Generic Comments on VAR-002-3 The use of the term 'direct' in R2.2 lead to implications of issuing directives. To get away from this situation, we suggest substituting 'instruct' for 'direct'. This change would need to be reflected in the Measure 2.1 and 2.2 and the VSL also. We suggest changing the notification timing requirements in R3 to the Generator Operator must notify the Transmission Operator within 30 minutes of the change of AVR status unless the AVR has been restored to service. In the second sentence in the Rationale Box for R3, use 'provide' instead of 'provided.' In the Rationale Boxes for R5 and R6 there is a reference to VAR capability and tap setting. We suggest rewording that sentence to the following: 'If the tap setting is not properly set, then the VARs available from that unit can be affected.'
We suggest the following change for the High VSL for R2. The responsible entity did not have a conversion methodology when it monitored voltage…' We recommend replacing the word 'directive' with 'specification' in the Severe VSL for R6.
Individual
Texas Reliability Entity
Texas Reliability Entity
(1) Under the currently enforceable TOP standards, there is a requirement to operate within SOLs and IROLs (in TOP-004-2 R1). However, in the proposed TOP standards currently filed at FERC for approval, the wording of this requirement changed. In TOP-001-2 R8 thru R9, the TOP only has to operate within SOLs that "deserved increased attention" according to the rationale stated in the proposed Standard. What effect does that change have on these VAR requirements, and the stated rationales? (2) If it is the SDT's intent for R2 and R3 that the TOP operate within voltage SOLs, then we suggest rewording R3 to remove "as necessary" to say "within System Operating Limits" or "under normal and Contingency conditions" to match R2. (3) The VSL language for VAR-001-4 R2 and R3 does not match the wording in the requirements. If the intent is to require operation within SOLs and IROLs as suggested by the VSLs, then the requirements should expressly say so. If it is not, then the VSLs should be revised to match the requirements. (4) For VAR-001-4 R1 and R5, should there be a process to provide feedback to the TOP on the voltage schedule? For example, if the TOP sets the voltage schedule in a manner that requires the generator to be at or near a reactive limit for the unit, then the unit may not be able to provide the necessary reactive support under a contingency situation.
(1) The status and capability notifications in R3 and R4 may be directly or indirectly in conflict with TOP-005-2a Attachment 1, Item 1.2.4, IRO-005-3.1a R1.1 and R12, IRO-002-2 R5, IRO-003-2 R2, TOP-006-2 R1 and R2, TOP-008-1 R4 and possibly future TOP-003-2 R1. Will the TOP

and RC be able to satisfy their obligations under these other standards in view of the proposed GOP reporting parameters? (2) In VAR-002-3 R4, does the “reactive capability” include static capacitive or reactive devices that are behind the fence (for example, static capacitors and reactors installed on the low voltage feeders at wind plants to meet power factor requirements). Would this requirement apply to such devices if they are not included in the Bulk Electric System per the new BES definition?
Individual
Dave Willis
Idaho Power Company
Yes
Yes
Yes, exempting the intermittent outages of AVR’s and only requiring notification for extended interruptions is an improvement and lessens the documentation necessary to show compliance.
No
Group
ACES Standards Collaborators
Jason Marshall
Yes
Yes this is clear. We thank the drafting team for removing the duplication from the previous draft.
Yes
(1) Requirement VAR-001-4 R1 is vague and ambiguous and may be duplicative of VAR-001-4 R5. It requirements need further refinement. First, it states that the TOP shall specify “a system voltage schedule”. This is singular. A system always has multiple schedules for generators, capacitor banks, reactors, etc. It does not have a single voltage schedule. Second, what equipment or facilities is the voltage schedule supposed to apply? Is this supposed to be the voltage schedule for a generator? Is this supposed to the voltage for reactor or capacitor switching? Is this supposed to be the voltage limits on a transmission bus? Schedule would tend to imply a level of control and, thus, not a limit but the simple reality is that the requirement is vague, ambiguous, and unenforceable as written. Third, if the requirement applies to voltage schedules at generators, it is duplicative to VAR-001-4 R5 because this already compels the TOP to provide voltage schedules for generators. Please provide additional clarifications in the requirement. (2) We appreciate the drafting team removing duplicate requirements. This version of the standard has been improved greatly. However, we still believe there is some duplication that needs to be addressed. For example, VAR-001-4 R1 requires a TOP to “specify a system voltage schedule… as part of its plan to operate with System Operating Limits and Interconnection Reliability Operating Limits” while VAR-001-4 R2 requires the TOP to “schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions”. How does a TOP specify a voltage schedule per R1 and

not also schedule sufficient reactive resources per R2? The TOP can't maintain the voltage schedule without scheduling sufficient reactive resources. Please eliminate the duplication. (3) VAR-001-4 R2 is also duplicative of VAR-001-4 R3. R2 requires the TOP to "schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions" while R3 requires the TOP "to operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow". How does the TOP schedule sufficient reactive resources without regulating transmission voltage and reactive flow? The TOP would be operating the voltage-regulation devices when they schedule sufficient reactive resources since the voltage-regulation devices are reactive resources. If the purpose was to delineate by time frames implied by the use of "Real-time Operation" in R3 and "schedule" in R2, the requirements need further refinement to be clear that the targeted time frames are supposed to be different. Furthermore, the Time Horizons for both R2 and R3 are duplicate covering Real-time Operations, Same-day Operations, and Operational Planning which would imply that different time frames are not intended. Please eliminate the duplication or clarify the time frames as appropriate. Detailed application guidelines would help eliminate some of the confusion. (4) Part 1.1 meets P81 criteria and should be retired. The requirement meets Criterion A (overarching) because it "does little, if anything, to benefit or protect the reliable operation of the BES" and meets criterion B4 – Reporting because it requires the TOP to report to another party and has "no discernible impact on promoting the reliable operation of the BES." The mere fact that Part 1.1 only requires reporting upon receiving a request is supportive that it has no impact on reliability. If it did materially support reliability, the RC would be required to have the data and the TOP would be obligated to provide it. Please remove Part 1.1. If Part 1.1. persists in the next draft, we request that the drafting team provide written justification for why these requirements do not meet P81 criteria and actually materially support reliability. (5) Measure VAR-001-4 M2 is inconsistent with the main requirement R2 and needs to be modified. M2 proposed that the TOP shall have evidence of scheduling resources based on their system assessment. While we agree this is likely the method the TOP will use to schedule resources, the simple fact is that it is not part of the requirement and cannot be compelled in the measure. Please modify the measure to be consistent with the requirement. (6) The second sentence of R2 is an explanation and not a requirement. Thus, it should be moved to the application guidelines section. We understand that FERC previously directed NERC to include use of controllable load as a reactive resource because it was not one of the explicitly listed reactive resources. FERC likely included this statement as evidenced by the first sentence of paragraph 1879 of Order 693 to further a policy goal of expanding the use of demand side management (DSM). At the time the order was issued, DSM was in its infancy. Today, DSM has become ubiquitous as demonstrated by the almost 40,000 MW reported in the NERC 2013 Summer Assessment. Given that all organized markets include at least one DSM product, its proliferation will only continue. Thus, the policy goal has been clearly met and specific mention in NERC standards in no longer necessary. In fact, an equally efficient and effective alternative would be to eliminate specific references of any type of reactive resource by striking the second sentence in its entirety. (7) The Time Horizons for VAR-001-4 R3 are inconsistent with the requirement. R3 specifically states that it deals with Real-time operation. Thus, how could Operational Planning and Same-

day Operation be applicable? These timelines are conflicting and need to be modified. (8) For requirement VAR-001-4 R4, why can't the GOP make a self-determination that it meets the TOP criteria? Is the TOP obligated to make a determination or to simply supply the criteria to the GOP? The RSAW indicates that the auditor will not determine if the GOP received pre-authorization from the TOP. Thus, the requirement should either be modified so that audit practices will have to be modified or aligned with how the RSAW indicates compliance will be assessed. We recommend that the drafting team work with NERC compliance to align the requirement with the RSAW language. (9) VAR-001-4 R5 should be modified to clarify that the TOP is not required to provide a voltage schedule to all generators but only to those generators that it determines it needs to provide reactive supply. A TOP may determine that a generator is too small to control voltage at its location and that it does not need to provide a voltage schedule for this generator. Including all generators is unnecessary for reliability. (10) Part 5.3 meets a P81 criterion and should be retired. The requirement meets Criterion A (overarching) because it "does little, if anything, to benefit or protect the reliable operation of the BES" and meets criterion B4 – Reporting because it requires the TOP to report its criteria to another party and has "no discernible impact on promoting the reliable operation of the BES." The mere fact that Part 5.3 only requires reporting upon receiving a request is supportive that it has no impact on reliability. If it did support reliability, the GOP would be required to have the data. Please remove Part 5.3. If Part 5.3 persists in the next draft, we request that the drafting team provide written justification for why these requirements do not meet P81 criteria and actually materially support reliability. (11) We request that R6 be modified to state that the timeframe shall be mutually agreeable. The TOP is only required to consult with the GO and could still provide an unreasonable timeframe after such consultation. At the very least, the requirement needs to be clear that the GO and GOP are not obligated to take an outage to implement tap changes and would be allowed make them at the next scheduled maintenance or forced outage with sufficiently long outage window to allow such changes. (12) The evidence retention section needs to be updated. First, it covers only measures one through four when there are actually six. Second, it covers measures when it should cover requirements to be consistent with existing standards. (13) As written, the VSL for R1 is overly harsh. If a TOP simply failed to create a single voltage schedule, it would be a severe violation. It seems the VSLs could be graduated based on the number of voltage schedules that are not created as a percentage of the total voltage schedules. (14) The VSLs for R2 and R3 are inconsistent with the requirement. The High VSL and Severe VSL mention avoiding violating an SOL or IROL respectively. However, the requirement mentions neither. This would be inconsistent with FERC guideline three that VSLs should be consistent with the corresponding requirement. (15) The High and Severe VSLs for R2 and R3 overlap with one another. High VSLs for both requirements apply to SOL violations and Severe VSLs for both requirements apply to IROL violations. By definition in the NERC glossary, an IROL is a subset of a SOL. Thus, a failure to schedule or operate reactive resources that results in an IROL violation would be both a High and Severe violation simultaneously. (16) From a compliance perspective, the High VSL for VAR-001-4 R4 is a logical fallacy. Compliance requires evidence. Thus, an auditor cannot make a determination that a TOP has exemption criteria but does not have evidence of exemption criteria. Thus, the High VSL could never be assigned by a

compliance enforcement authority. This needs to be modified. (17) The VSLs for VAR-001-4 R5 need to be modified. In the FERC order approving VSLs, FERC was clear that as many VSLs as possible should be used. Clearly, each VSL could be assigned based on the number of GOPs that the TOP failed to provide voltage schedules. This essentially means that the High VSL should be graduated. We disagree with assigning a moderate VSL for the failure of a TOP to provide its criteria in response to Part 5.3 by one minute. As written, the TOP could literally be one minute past the 30 day time frame and reach a moderate violation. This should not even be a violation let alone a Moderate VSL. The solution is to remove Part 5.3. If Part 5.3 persists, at a minimum, the VSL should be Lower because reliability is not impacted. The second half of the Severe VSL regarding not supplying the notification requirements to the GOP should be moved to Moderate VSL. Failure to provide voltage schedules misses significantly more of the spirit of the requirement than failure to provide exemption criteria. The purpose of failure to provide exemption criteria is an attempt to avoid nuisance violations not directly support reliability. (18) In the regional variances section, E.A. 16 and E.A. 17 meet P81 criteria and should be removed from the next draft. The purpose of these two requirements is to provide transparency between the GOP and TOP in determining voltage schedules and implementation of voltage schedules. While establishing transparency is certainly a laudable goal, it simply does not directly support reliability. Thus, these two regional variance requirements meet Criterion A (overarching) because they do little, if anything, to benefit or protect the reliable operation of the BES and meet criterion B4 – Reporting because they require the TOP and GOP to report to each other. (19) It is unnecessary to require the TOP to direct the Generator Operator to comply with the voltage schedule with the AVR in voltage control mode in VAR-001-4 Part 5.1. It is redundant with VAR-002-3 R2 which compels the GOP to follow the voltage schedule. If drafting team feels the “directive” language is necessary in VAR-001-4 Part 5.1, then VAR-002-3 R2 should be removed because it would be redundant with TOP-001-1a R3 (existing) and TOP-001-2 R1 (pending regulatory approval). Both require the GOP to follow the directives of its TOP.

(1) Consistent with our comment number 9 in question 2, VAR-002-3 R2 and Part 2.1 need to be modified so that the GOP is only required to follow the voltage schedule if provided by the TOP. It is not desirable for the TOP to provide all generators voltage schedules. As an example, the TOP may determine it does not need to provide a voltage schedule to a small generator. To consider this situation, the clause “if a voltage schedule is provided by the TOP” could be added to both Part 2.1 and the main requirement. (2) VAR-002-3 R5 meets multiple P81 criteria and should be removed. It meets Criterion A (overarching) because it does little, if anything, to benefit or protect the reliable operation of the BES and meets B2 – Data Collection/Data Retention and B4 – Reporting because it requires the GOP to gather their tap setting information and report it to a third party (i.e. its TOP) which is unnecessary to implement as a reliability requirements. A GOP is not going to refuse to provide data to its TOP on its generator step up transformer in a compliance driven world. In fact, making this data subject to compliance slows the free exchange of the information because of all the extra checking that goes into managing (i.e. verifying, checking, storing) compliance documentation. This requirement also meets B7 – Redundant because the TOP can specify this data in its data specification per TOP-003-2 R1, distribute to the GO per TOP-003-2 R3 and then GO would

have to respond per TOP-003-2 R5. (3) VAR-002-3 Part 6.1 meets a P81 criterion and should be struck. It meets Criterion A (overarching) because it does little, if anything, to benefit or protect the reliable operation of the BES and meets B4 – Reporting because it requires the GO to report a technical justification for not implementing tap changes. This technical justification simply does not support reliability. The TOP can make adjustments to other voltage schedules to account for the GO's inability to implement the tap changes. What is the purpose of the GO providing the TOP a technical justification? Is it to provide the TOP some assurance there is a technical reason for failing to implement the tap changes? In a compliance driven world, the TOP can reasonably expect the GOP to implement the tap changes unless the changes would violate safety, equipment limits, regulatory or statutory requirements since these only the only deviations allowed by the main requirement. The threat of sanctions assures this. Furthermore, the GOP may legitimately not have a "technical" justification because a regulatory requirement is a legal justification not a technical justification. (4) The RSAW for VAR-002-3 indicates that compliance assessment for R4 could be vague and result in inconsistent outcomes. The RSAW indicates that the auditor will look for evidence when the GOP became aware of changes. If the entity's data historian or another piece of evidence indicates a reactive capability change occurred at a certain time, does this mean that the entity is aware? We think the answer is no. The entity is only aware when its personnel become aware and not when a measurement first records that something is askew. Furthermore, we believe personnel should be limited to the plant operators in the control room who have overall responsibility. Any evidence review for when the entity became aware should be limited to plant operator logs because this evidence will most closely demonstrate what the plant operator knew based on information provided and will not be as likely to be second-guessed on what the plant operator should have known. (5) VAR-002-3 R2 will be problematic for some GOPs because it does not reflect the characteristics of the voltage schedule provided by some TOPs. For example, some TOPs provide an hourly average voltage schedule to avoid the need for notification for every time the GOP drifts out of schedule. How would R2 be applicable in this situation? Would it only apply for the first 15 minutes of each hour looking back at the last hour? Please modify the requirement accordingly to address this issue.
We do not support the VSLs for R5 because it meets P81 criteria and should be removed. We also do not support the VSLs for requirements that need modifications as identified in question 3.
Group
DTE Electric Co.
Kathleen Black
Yes
Yes
Yes Comments: Adding the 15 minute window in VAR-002 is a great improvement.
Individual
Roger Dufresne

Hydro-Québec Production
Yes
No
The requirement number five has to be removed, the reactive power of an auxiliairy transformer unit has a little impact on the ability of a groupe or plant to provide the reactive power required by the network.
Group
ISO/RTO Standards Review Committee
Gregory Campoli
Yes
We support this direction and the SDT's decision to not reiterate or duplicate the voltage assessment requirements already addressed by the FAC and TOP standards.
Yes
We support the SDT's proposal to remove the requirements that may be redundant with other standards. We do not have any comments on the requirements, Measures or VRFs, but we do have some comments on the VSLs: a. R1: The word "schedule" after "system voltage" is missing from the VSL. b. There is inconsistency in the tense used in various VSLs – some are in present tense while others in past tense. Please review and revise as appropriate.
We assess the changes proposed under Q2 and Q 3, above, are not substantive and do not materially change the intent or content of the standards. Therefore, if the standards receives 2/3 majority approval at the ballot, these changes can be implemented and posted for recirculating ballot without having to post and ballot the standards for a successive ballot. We agree with most of the proposed changes, but would suggest the following changes to more effective convey the intent of Requirement R3 and Measure M3. a. R3: The wording "the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator" is not a direct action and may not be measurable. We suggest to revise it to read: "the Generator Owner shall implement the transformer tap positions according to the specifications provided by the Transmission Operator…." b. M3: We suggest it be reworded to require demonstration of compliance rather than to require actions which should have been stipulated in the requirement. Specifically, we proposed the last part in Measure M3 be revised to: "…therefore, if a status change lasts more than 15 minutes, the GOP shall provide evidence such as system log, electronic message or a transmittal letter that it notified its associated Transmission Operator within 30 minutes of when the change first occurred." We further propose that the SDT insert the evidence language into the first sentence of Measure M3 which asks for evidence that the Generator notified its associated Transmission Operator within 30 minutes of the change identified in Requirement R3.
We support the proposed VRFs and VSLs.
Individual
Michelle D'Antuono

Ingleside Cogeneration LP
Yes
Yes
Yes,Ingleside Cogeneration agrees that there must be reasonable notification criteria controlled by TOPs that allows them to specify when notification of change in AVR or reactive resource status is necessary. In many cases, the status is telemetered in real-time, but a call is required anyways to specify the expected duration of the status change. This is overcommunication in most cases, and only serves to tie up resources at the GOP and TOP. The same is true of notifications when the GOP cannot maintain the voltage at the interconnection point. Many GOPs do not control interconnection voltage and could actually resist an adjustment that the TOP is trying to make in response to system conditions. Again, some reasonable notification criteria could stop a lot of nuisance calls under these circumstances.
Individual
Scott Langston
City of Tallahassee
Agree
Florida Municipal Power Agency
Group
Santee Cooper
S. Tom Abrams
We agree with the comments of the North American Generator Forum.
Individual
John D. Brockhan
CenterPoint Energy, Houston Electric LLC.
Yes
CenterPoint Energy believes the language proposed in R1 supplemented by the rationale for R1 is clear in stipulating that a Transmission Operator specified voltage schedule must operate within the boundaries of System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs). What is missing from this standard is the coordination that occurs between the Reliability Coordinators, Transmission Operators, and Generator Operators in defining voltage schedules that do not violate established SOLs and IROLs. Transmission Operators have capabilities to monitor, study, and control their systems but do not have the complete data that a Reliability Coordinator uses to establish SOLs and IROLs. Furthermore, the Reliability Coordinator establishes a baseline voltage profile for the Reliability Coordinators area and its Transmission Operators to review before the schedule is finalized, distributed, and posted. CenterPoint Energy believes that Voltage and Reactive standards that apply strictly to the TOP and/or the GOP and GO create a possible misalignment in the operation of the Bulk Electric System. Moving forward with these standards only to address

the RC's applicability to the monitoring and control of voltage and reactive at a future date would not accurately reflect the industry's Real-Time operation with respect to voltage and reactive processes and does not align with NERC's Functional Model definition and relationships of an RC with other Functional Entities. CenterPoint Energy appreciates the efforts of the Standard Drafting Team and recommends the following requirement lanauge to add the Reliability Coordinator back into the applicability of the standard: "Each Transmission Operator shall coordinate with the applicable Reliability Coordinator to specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and any Interconnection Reliability Operating Limits established by the applicable Reliability Coordinator."
Yes
CenterPoint Energy agrees with the SDT's efforts to eliminate duplicated standards, but has the following concerns. R1.1 is unclear on the applicability of the "30 days of a request." Is the requirement for Transmission Operators to provide their perspective Reliability Coordinators the voltage schedule automatically without a request and only to any adjacent Transmission Operators that requests the schedule within 30 days of the request; or is it the intent of the SDT for the Reliability Coordinator to also request the Transmission Operator for the schedule with the same "30 days of request" requirement. In order for a TOP to obtain evidence to prove compliance to this requirement, a TOP must receive documentable requests from its RC and/or its adjacent Transmission Operators to then provide the voltage schedule within the 30 days of the request. If the Transmission Operators do not receive such requests then essentially according to the standard they do not have to provide the established voltage schedules as the requirement currently specifies. Many Reliability Coordinators or regions have established voltage working groups with processes or its equivalence to aid in the corroboration and defining of company specific voltage schedules within the RCs area or region then such voltage schedules would already be provided as part of the regional processes. CenterPoint Energy recommends the following clarifying language: "If requested, Eeach Transmission Operator shall provide, a copy of the voltage schedules and associated tolerance bands to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of such a request." CenterPoint Energy agrees with providing the Generator Operators the voltage or Reactive Power schedule; however, we believe R5.1, which also requires the Transmission Operator to direct the Generator Operators to comply with such schedule to the specificity that the AVR be in automatic voltage control mode, is redundant and is an unnecessary requirement as well as a compliance burden for the Transmission Operators. Exemptions to the Generator Operator to deviate from the established voltage schedule or the Automatic Voltage Regulator functioning in any mode other than automatic voltage control are addressed in R4 and VAR-002-3 R1 and R2 and will be handled in Real-Time operations and will be scenario specific. VAR-002 R1 and R2 requires Generator Operators to maintain the voltage or Reactive Power schedule and operate each generator with its AVR in service and in the automatic voltage control mode. Based upon this redundancy and Paragraph 81 criteria regarding duplicative and redundant requirements CenterPoint Energy recommends removal of the language "…and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in

service and controlling voltage)”.
Yes, CenterPoint Energy agrees with these revisions to VAR-002 removing compliance issues that address burdensome notification requirements, allowing the Transmission Operator, through VAR-001 to tailor notification requirements based on system/area needs.
CenterPoint Energy believes the VSLs associated with VAR-001 R2 and R3 do not consider changes in Real-Time topography such as forced outages, Resource inadequacy, or changes in weather that can drastically change the outcome of any planned or studied environment in both normal and emergency operations. A transmission operator could have scheduled sufficient reactive resources as necessary and have them available to mitigate known and identified SOLs or IROLs, but cannot schedule sufficient reactive resources for the unknown. CenterPoint energy suggests adding “identified” to the VSL language. “The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an identified SOL or IROL”. CenterPoint energy believes that the High VSL for R4 is inappropriate and is indicative of a zero tolerance environment. If a Transmission Operator has an exemption criteria established, notifies the Generator Operator of such exemption, and captures evidence for compliance to prove notification 99 times out of 100, then the one instance in which the TOP notified the Generator Operator, but failed to capture evidence would warrant a High VSL possible violation.
Individual
RoLynda Shumpert
South Carolina Electric and Gas
Agree
SERC OC Review Group
Individual
Catherine Wesley
PJM Interconnection
Yes
Yes
PJM recommends the drafting team revise R1 as follows: Each Transmission Operator shall specify a system voltage schedule. The remaining language in that requirement is not needed to support reliability. PJM does not understand the scope of controllable load in R2. We urge the drafting team to include clarification. For R3, PJM recommends revision to the Time Horizon to include Real Time only. PJM recommends the following addition to R5 as the last phrase in the requirement for consistency with R4 language. “unless otherwise exempted as noted in R4.”
Yes.
Individual
Sergio Banuelos
Tri-State Generation and Transmission Association, Inc.
No

Yes
In the draft of VAR-001-4 R2 the use of the word 'schedule' when referring to all reactive resources is unclear. This is in conjunction with the Compliance response to question 2 part 2, "…provide the documentation for the day ahead scheduling in addition to documentation supporting that it was scheduled..." found in the NERC document Draft Reliability Standard Compliance Guidance for VAR-001 and VAR-002 dated July 8, 2013. Is it the ad hoc group's intent to have a schedule for all reactive resources including capacitors, reactors, Static var Compensators and generators? Is the schedule meant to be similar to that of a generator (i.e. Insert capacitors at 1.0pu and remove at 1.05) or on a time base? Is schedule just supposed to take into account availability of all reactive resources? Also TSGT believes the statement "(at either the high or low side of the Generator Step-Up transformer at the TOP's discretion)" currently in VAR-001-4 R4 to should be changed to "(at an agreed upon metering point to which the GOP has direct access)." For VAR-001-4 R6 why did the ad hoc group not change the consultation requirement from GO to GOP? Tri-State believes that this information would better serve the GOP function particularly at Co-Owned facilities. This change would not have a negative effect on the reliability of the BES would reduce duplicative notification to be administered by the TOP.
For VAR-002-3 R5 TSGT believes the TOP should consult with the GOP rather than the GO to better align requirement R5 with its subrequirement R5.1.
Individual
Mary Lou Ideus
EDP Renewables North America LLC
Yes
Yes
Yes. EDPR NA believes it is important for TOPs to have the flexibility to tailor its requirements, as long as there is sufficient coordination among affected entities. We also offer the following comment: VAR-002 R1: We support the concept that a GOP need not notify its TOP that its AVR is out of service if it has previously advised its TOP that it will not have its AVR in service during start-up and shut-down. We recommend that similar provision be made for variable energy resources which are not able to provide voltage support when operating in similar circumstances. Wind farms, for example, generally have equipment limitations that can affect their ability to follow voltage schedules when operating at low levels. Wind farms will not telemeter a different status in that circumstance, however. We propose that, if a variable energy resource has notified its TOP of equipment limitations that affect its ability to follow a voltage schedule until it achieves a certain level of production, also not be required to notify the TOP that its AVR is out of service.
No.
Group
Bonneville Power Administration
Andrea Jessup

Yes
The SDT considered standards put in place after Order 693 was issued and avoided overlapping FAC and TOP standards. The SDT did include the tolerance band requirement to be consistent with voltage limit requirements in other standards.
Yes
There are two questions under Question #2. BPA answered the first question in the check box. BPA's answer to the second part of the question is No.
Yes. Comments: BPA requests further clarification of VAR-002-3 R3 and M3, to be revised such that a status or capability change in generator Reactive Power should be reported within 30 minutes from an entity becoming aware of the change in condition, rather than the current form, which is 30 minutes from the change in condition.
No.
Individual
Brenda Hampton
Luminant Energy Company LLC
Agree
Luminant Generation Company, LLC
Group
Colorado Springs Utilities
Kaleb Brimhall
Agree
Florida Municipal Power Authority

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project 2013-04 Voltage & Reactive Control

The Project 2013-04 Voltage & Reactive Control Drafting Team thanks all commenters who submitted comments on the draft VAR-001-4 and VAR-002-3 standards. These standards were posted for a 45-day public comment period from October 11, 2013 to November 25, 2013. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 58 sets of comments, including comments from approximately 165 different people from approximately 107 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

The Industry Segments are:

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

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Russel Mountjoy	MRO NSRF	X	X	X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alice Ireland	Xcel Energy	MRO	1, 3, 5, 6
2.	Chuck Wicklund	Otter Tail Power	MRO	1, 3, 5
3.	Dan Inman	Minnkota Power Cooperative	MRO	1, 3, 5, 6
4.	Dave Rudolph	Basin Electric Power Cooperative	MRO	1, 3, 5, 6
5.	Kayleigh Wilkerson	Lincoln Electric System	MRO	1, 3, 5, 6
6.	Jodi Jensen	Western Area Power Administration	MRO	1, 6
7.	Joseph DePoorter	Madison Gas and Electric	MRO	3, 4, 5, 6
8.	Ken Goldsmith	Alliant Energy	MRO	4
9.	Mahmood Safi	Omaha Public Power District	MRO	1, 3, 5, 6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
10. Marie Knox	Midcontinent Independent System Operator		2									
11. Mike Brytowski	Great River Energy	MRO	1, 3, 5, 6									
12. Randi Nyholm	Minnesota Power	MRO	1, 5									
13. Scott Bos	Muscatine Power and Water	MRO	1, 3, 5, 6									
14. Scott Nickels	Rochester Public Utilities	MRO	4									
15. Terry Harbour	MidAmerican Energy	MRO	1, 3, 5, 6									
16. Tom Breene	Wisconsin Public Service	MRO	3, 4, 5, 6									
17. Tony Eddleman	Nebraska Public Power District	MRO	1, 3, 5									
2. Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Ayesha Sabouba	Hydro One Neworks Inc.	NPCC	1
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
7.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Michael Jones	National Grid	NPCC	1
10.	Mark Kenny	Northeast Utilities	NPCC	1
11.	Christina Koncz	PSEG Power LLC	NPCC	5
12.	Helen Lainis	Independent Electricity System Operator	NPCC	2
13.	Michael Lombardi	Northeast Power Coordinating Council	NPCC	10
14.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9
15.	Bruce Metruck	New York Power Authority	NPCC	5
16.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5
17.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
18.	Robert Pellegrini	The United Illuminating Company	NPCC	1
19.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
20.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
21.	Brian Robinson	Utility Services	NPCC	8

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
22.	Brian Shanahan	National Grid	NPCC 1										
23.	Wayne Sipperly	New York Power Authority	NPCC 5										
24.	Ben Wu	Orange and Rockland Utilities	NPCC 1										
25.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC 3										
26.	David Burke	Orange and Rockland Utilities Inc.	NPCC 3										
3.	Group	Erika Doot	Bureau of Reclamation	X				X					
No Additional Response													
4.	Group	Louis Slade	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Connie Lowe	NERC Compliance Policy	RFC	5, 6
2.	Mike Garton	NERC Compliance Policy	NPCC	5, 6
3.	Randi Heise	NERC Compliance Policy	SERC	1, 3, 5, 6
4.	Michael Crowley	Electric Transmission	SERC	1, 3
5.	Ed Croasdale	Electric Transmission	SERC	1, 3
6.	Chip Humphrey	Power Generation	NPCC	5
7.	Sean Iseminger	Power Generation	SERC	5
8.	Larry Whanger	Power Generation	SERC	5
9.	Jarad Morton	Power Generation	RFC	5
10.	Jeff Bailey	Nuclear		5

5.	Group	Janet Smith, Regulatory Affairs Supervisor	Arizona Public Service Company	X		X		X	X				
No Additional Response													
6.	Group	Marcus Pelt	Southern Company: Southern Company Services, Inc.; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing	X		X		X	X				
No Additional Response													
7.	Group	Bob Steiger	Salt River Project	X		X		X	X				

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
No Additional Response												
8. Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tim Beyrle	City of New Smyrna Beach	FRCC	4
2.	Jim Howard	Lakeland Electric	FRCC	3
3.	Greg Woessner	Kissimmee Utility Authority	FRCC	3
4.	Lynne Mila	City of Clewiston	FRCC	3
5.	Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4
6.	Randy Hahn	Ocala Utility Services	FRCC	3
7.	Stanley Rzad	Keys Energy Services	FRCC	1
8.	Don Cuevas	Beaches Energy Services	FRCC	1

9.	Group	Brandy Spraker	Tennessee Valley Authority	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Paul Palmer		SERC	5
2.	Tony Segovia		SERC	5
3.	Tom Vandervort		SERC	5
4.	Lee Thomas		SERC	5
5.	Ian Grant		SERC	3
6.	Marjorie Parsons		SERC	6
7.	DeWayne Scott		SERC	1
8.	Matt Schebler		SERC	1
9.	David Thompson		SERC	5

10.	Group	Ryan Millard	PacifiCorp					X	X				
No Additional Response													
11.	Group	Colby Bellville	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Lee Schuster	Duke Energy	FRCC	3
3.	Dale Goodwine	Duke Energy	SERC	5

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
4. Greg Cecil	Duke Energy	RFC 6										
12. Group	Lloyd A. Linke	Western Area Power Administration	X					X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Western Area Power Administration	Coloratdo River Storage Project	WECC	6
2.	Western Area Power Administration	Rocky Mountain Region	WECC	1, 6
3.	Western Area Power Administration	Sierra Nevada Region	WECC	1, 6
4.	Western Area Power Administration	Desert Southwest Region	WECC	1, 6
5.	Western Area Power Administration	Upper Great Plains Region	MRO	1, 6

13. Group	Brent Ingebrigtson	PPL NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
2.	Annette Bannon	PPL Generation, LLC	RFC	5
3.		PPL Susquehanna, LLC	RFC	5
4.		PPL Montana, LLC	WECC	5
5.	Elizabeth Davis	PPL EnergyPlus, LLC	MRO	6
6.			NPCC	6
7.			RFC	6
8.			SERC	6
9.			SPP	6
10.			WECC	6

14. Group	Robert Rhodes	SPP Standards Review Group		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Allen	City Utilities of Springfield	SPP	1, 4
2.	Clem Cassmeyer	Western Farmers Electric Cooperative	SPP	1, 3, 5
3.	Kevin Frick	Westar Energy	SPP	1, 3, 5, 6
4.	Ron Gunderson	Nebraska Public Power District	MRO	1, 3, 5
5.	Michael Jacobs	Consolidated Assest Management Services	NA - Not Applicable	NA
6.	Stephanie Johnson	Westar Energy	SPP	1, 3, 5, 6
7.	Bo Jones	Westar Energy	SPP	1, 3, 5, 6

Group/Individual		Commenter	Organization		Registered Ballot Body Segment									
					1	2	3	4	5	6	7	8	9	10
8.	Allen Klassen	Westar Energy	SPP	1, 3, 5, 6										
9.	Tiffany Lake	Westar Energy	SPP	1, 3, 5, 6										
10.	Randy Root	Grand River Dam Authority	SPP	1, 3, 5										
11.	Mahmood Safi	Omaha Public Power District	MRO	1, 3, 5										
12.	Dennis Sauriol	American Electric Power	SPP	1, 3, 5										
13.	Don Schmit	Nebraska Public Power District	MRO	1, 3, 5										
14.	Ashley Stringer	Oklahoma Municipal Power Authority	SPP	4										
15.	Bryan Taggart	Westar Energy	SPP	1, 3, 5, 6										
16.	Scott Williams	City Utilities of Springfield	SPP	1, 4										
15.	Group	Jason Marshall	ACES Standards Collaborators							X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
2.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
3.	Scott Brame	North Carolina Electric Membership Corporation	SERC	1, 3, 4, 5
4.	Michael Brytowski	Great River Energy	MRO	1, 3, 5, 6
5.	Paul Jackson	Buckeye Power	RFC	3, 4
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT	1, 5
7.	John Shaver	Arizona Electric Power Cooperative	WECC	4, 5
8.	John Shaver	Southwest Transmission Cooperative	WECC	1

16.	Group	Kathleen Black	DTE Electric Co.				X	X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Kent Kujala	NERC Compliance	RFC	3
2.	Daniel Herring	NERC Training & Standards Development	RFC	4
3.	Mark Stefaniak	Regulated Marketing	RFC	5
4.	Jeffrey DePriest	NERC Compliance	RFC	

17.	Group	Gregory Campoli	ISO/RTO Standards Review Committee			X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	K. Goodman	ISO-NE	NPCC	2
2.	B. Li	IESO	NPCC	2

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	C. Yeung	SPP	SPP	2									
4.	A. Dicaprio	PJM	RFC	2									
5.	T. Bilke	MISO	RFC	2									
6.	A. Miremadi	CAISO	WECC	2									
18.	Group	S. Tom Abrams	Santee Cooper	X		X		X	X				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1.	Rene Free	Santee Cooper	SERC	1, 3, 5, 6									
2.	Tom Abrams	Santee Cooper	SERC	1, 3, 5, 6									
19.	Group	Andrea Jessup	Bonneville Power Administration	X		X		X	X				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1.	Steve Hitchens	Technical Operations	WECC	1									
2.	Tanner Brier	Power Services	WECC	1									
20.	Group	Kaleb Brimhall	Colorado Springs Utilities	X		X		X	X				
No Additional Response													
21.	Individual	John Canavan	NorthWestern Energy	X									
22.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				
23.	Individual	Ronnie C. Hoeinghaus	City of Garland			X							
24.	Individual	Thomas Foltz	American Electric Power	X		X		X	X				
25.	Individual	Oliver Burke	Entergy Services, Inc.	X									
26.	Individual	John Seelke	Public Service Enterprise Group	X		X		X	X				
27.	Individual	Shirley Mayadewi	Manitoba Hydro	X		X		X	X				
28.	Individual	Jonathan Appelbaum	The United Illuminating Company	X									
29.	Individual	Angela P Gaines	Portland General Electric Co	X		X		X	X				
30.	Individual	Anthony Jablonski	ReliabilityFirst										X
31.	Individual	Bill Fowler	City of Tallahassee			X							
32.	Individual	Cheryl Moseley	Electric Reliability Council of Texas, Inc.		X								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Michael Falvo	Independent Electricity System Operator		X								
34.	Individual	Brett Holland	Kansas City Power & Light	X		X		X	X				
35.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
36.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
37.	Individual	Lynda Kupfer	Puget Sound Energy	X		X		X					
38.	Individual	Silvia Parada Mitchell	NextEra Energy	X		X		X	X				
39.	Individual	Rjick Terrill	Luminant Generation					X					
40.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
41.	Individual	David Jendras	Ameren	X		X		X	X				
42.	Individual	Kathleen Goodman	ISO New England Inc.		X								
43.	Individual	Karen Webb	City of Tallahassee - Electric Utility					X					
44.	Individual	Robert L. Dintelman	Utility System Efficiencies, Inc.					X					
45.	Individual	Melissa Kurtz	US Army Corps of Engineers					X					
46.	Individual	Gerald G Farringer	Consumers Energyu			X							
47.	Individual	Chris Scanlon	Exelon Companies	X		X	X	X	X				
48.	Individual	Texas Reliability Entity	Texas Reliability Entity										X
49.	Individual	Dave Willis	Idaho Power Company	X									
50.	Individual	Roger Dufresne	Hydro-QuÃ©bec Production					X					
51.	Individual	Michelle D'Antuono	Ingleside Cogeneration LP					X					
52.	Individual	Scott Langston	City of Tallahassee	X									
53.	Individual	John D. Brockhan	CenterPoint Energy, Houston Electric LLC.	X		X							
54.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				
55.	Individual	Catherine Wesley	PJM Interconnection		X								
56.	Individual	Sergio Banuelos	Tri-State Generation and Transmission Association, Inc.	X		X		X					
57.	Individual	Mary Lou Ideus	EDP Renewables North America LLC					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
58.	Individual	Brenda Hampton	Luminant Energy Company LLC						X				

If you support the comments submitted by another entity and would like to indicate you agree with their comments, please select "agree" below and enter the entity's name in the comment section (please provide the name of the organization, trade association, group, or committee, rather than the name of the individual submitter).

Organization	Agree	Supporting Comments of "Entity Name"
Western Area Power Administration	Agree	US Bureau of Reclamation.
Colorado Springs Utilities	Agree	Florida Municipal Power Authority
Entergy Services, Inc.	Agree	SERC OC Review Group
City of Tallahassee	Agree	FMPA
NextEra Energy	Agree	MidAmerican
ISO New England Inc.	Agree	IRC SRC
City of Tallahassee - Electric Utility	Agree	FMPA
US Army Corps of Engineers	Agree	MRO NSRF
City of Tallahassee	Agree	Florida Municipal Power Agency
South Carolina Electric and Gas	Agree	SERC OC Review Group
Luminant Energy Company LLC	Agree	Luminant Generation Company, LLC

Organization	Agree	Supporting Comments of "Entity Name"
Santee Cooper		We agree with the comments of the North American Generator Forum.

1. **Although FERC directed NERC to provide more details on "established limits," the VAR standards development team determined that the FAC and TOP standards provide explicit requirements on voltage limits. Further, the definition of a System Operating Limit requires Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits) to be included. Is it clear that the specifics with regard to voltage limits are to be determined and monitored as part of operating within System Operating Limits and Interconnection Reliability Operating Limits?**

Organization	Yes or No	Question 1 Comment
Tri-State Generation and Transmission Association, Inc.	No	
Northeast Power Coordinating Council	Yes	We support the direction being taken and the SDT's decision to not reiterate or duplicate the voltage assessment requirements already addressed by the FAC and TOP standards.
Response: Thank you for your comments. The VAR SDT determined that SOLs and IROLs will cover voltage limits as needed in Order No. 693.		
ISO/RTO Standards Review Committee	Yes	We support this direction and the SDT's decision to not reiterate or duplicate the voltage assessment requirements already addressed by the FAC and TOP standards.
Response: Thank you for your comments.		
Electric Reliability Council of Texas, Inc.	Yes	ERCOT agrees it is clear voltage limits are to be monitored as either SOLs or IROLs. However it seems the SDT could make more changes to clear up more items.A. VAR-001 R3 grammatical: recommend deleting "as necessary" from this sentence. It adds no value and is not needed.B. It appears VAR-001 R4 allows the TOP to not comply with the VAR Standards by utilizing exemptions?

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comments. The phrase "as necessary" was retained because several TOPs do not intervene and direct devices unless the other applicable entities have not taken other steps to control voltage as necessary or required by various other standards. The exemptions provide a mechanism for TOPs to give exemptions based on system needs and individual GOP characteristics. R4 provides exemptions for GOPs from: 1) following a schedule; 2) being in voltage control mode; or 3) providing particular notifications. Based on industry input the standards needed specificity on the types of exemptions that a TOP can provide.		
Independent Electricity System Operator	Yes	We support this direction and the SDT's decision to not reiterate or duplicate the voltage assessment requirements already addressed by the FAC and TOP standards.
Response: Thank you for your comments.		
Southern Company: Southern Company Services, Inc.; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing	Yes	R1: The modifications in this version of VAR-001 R1 are good because they standards that are now enforceable, particularly FAC-011 and FAC-014.M2: All Transmission Operators are required to run contingency analysis on the real time system on a periodic basis per TOP-008-1 R4. We suggest modifying VAR-001 M2 to state: "If the assessment is performed in the Operations Planning Horizon, Transmission Operators shall provide copies of assessments used as the basis for how resources were scheduled." M3: Actions are not always required to be taken because of automatic settings of reactive devices. We suggest modifying VAR-001 M3 to state: "Each Transmission Operator shall have evidence that actions were taken as necessary to operate capacitive and inductive resources as needed in Real-time. This may include directions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments."R5.3 states, "The Transmission Operator shall provide the criteria used to develop voltage schedules and associated tolerance bands to the Generator Operator within 30 days of receiving a request." We suggest that this requirement is removed due to administrative burden.

Organization	Yes or No	Question 1 Comment
		We recognize the need for transpency; however, this requirement does not serve a reliabity purpose.
Response: Thank you for your comments. Since FERC recently proposed remanding the most recent TOP filing, the TOP and VAR interplay will be further evaluated. However, the concerns with regard to TOP-008-1 will be conveyed to Compliance for a future iteration of an RSAW and auditor training. Requirement R5, part 5.3 could not be removed because that specially addresses a FERC directive for VAR-002. Part 5.3 demonstrates who a TOP will provide technically justified schedules.		
Bonneville Power Administration	Yes	The SDT considered standards put in place after Order 693 was issued and avoided overlapping FAC and TOP standards. The SDT did include the tolerance band requirement to be consistent with voltage limit requirements in other standards.
Response: Thank you for your comments.		
SPP Standards Review Group	Yes	We thank the drafting team for taking this stance in not establishing details in the VAR standards and relying on those that already exist within defined SOLs and IROLs. Adding additional detail here would be redundant and possibly conflicting with requirements in other standards.
Response: Thank you for your comments.		
ACES Standards Collaborators	Yes	Yes this is clear. We thank the drafting team for removing the duplication from the previous draft.
Response: Thank you for your comments.		
CenterPoint Energy, Houston Electric LLC.	Yes	CenterPoint Energy believes the language proposed in R1 supplemented by the rationale for R1 is clear in stipulating that a Transmission Operator specified voltage schedule must operate within the boundaries of System Operating Limits (SOLs) and Interconnection Reliability Operating Limits

Organization	Yes or No	Question 1 Comment
		(IROLs). What is missing from this standard is the coordination that occurs between the Reliability Coordinators, Transmission Operators, and Generator Operators in defining voltage schedules that do not violate established SOLs and IROLs. Transmission Operators have capabilities to monitor, study, and control their systems but do not have the complete data that a Reliability Coordinator uses to establish SOLs and IROLs. Furthermore, the Reliability Coordinator establishes a baseline voltage profile for the Reliability Coordinators area and its Transmission Operators to review before the schedule is finalized, distributed, and posted. CenterPoint Energy believes that Voltage and Reactive standards that apply strictly to the TOP and/or the GOP and GO create a possible misalignment in the operation of the Bulk Electric System. Moving forward with these standards only to address the RC's applicability to the monitoring and control of voltage and reactive at a future date would not accurately reflect the industry's Real-Time operation with respect to voltage and reactive processes and does not align with NERC's Functional Model definition and relationships of an RC with other Functional Entities. CenterPoint Energy appreciates the efforts of the Standard Drafting Team and recommends the following requirement lanauge to add the Reliability Coordinator back into the applicability of the standard: "Each Transmission Operator shall coordinate with the applicable Reliability Coordinator to specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and any Interconnection Reliability Operating Limits established by the applicable Reliability Coordinator."
Response: Thank you for your comments. The VAR SDT recognizes the ERCOT roles of the Reliability Coordinator, but it is the VAR SDT's understanding that the coordination between the RC and TOP are handled by registration or contract. Further, the next project addressing the IRO family of standards will address the RC functions.		

Organization	Yes or No	Question 1 Comment
Dominion	Yes	
Arizona Public Service Company	Yes	
Salt River Project	Yes	
Florida Municipal Power Agency	Yes	
Tennessee Valley Authority	Yes	
PacifiCorp	Yes	
Duke Energy	Yes	
PPL NERC Registered Affiliates	Yes	
DTE Electric Co.	Yes	
Manitoba Hydro	Yes	
American Transmission Company, LLC	Yes	
Xcel Energy	Yes	
Luminant Generation	Yes	
City of Austin dba Austin Energy	Yes	
Ameren	Yes	
Utility System Efficiencies, Inc.	Yes	

Organization	Yes or No	Question 1 Comment
Consumers Energyu	Yes	
Exelon Companies	Yes	
Idaho Power Company	Yes	
Hydro-QuÃ©bec Production	Yes	
Ingleside Cogeneration LP	Yes	
PJM Interconnection	Yes	
EDP Renewables North America LLC	Yes	
Puget Sound Energy		- The implementation period might be as short as one day as the Effective Date section is currently formulated. For example, if approval occurs on 12/31/2013, the first day of the first calendar quarter after that date would be 1/1/2014. A short implemen
Response: Thank you for your comments. For the United States, if the VAR-001 standard passes a final ballot in December, the standard would not be presented to the Board of Trustees until February. It is not until the Board of Trustees approves the standard that the new standards would even be filed with FERC. FERC has not typically issued an order on a standards filing within six months. Therefore, it is unlikely that these VAR standards would even be able to go into effect before April 2014 in the United States.		

2. Several requirements were removed because they duplicated other standards. Do you agree with this approach? Do you have any specific questions or comments relating to the requirements in the revised VAR-001-4?

Organization	Yes or No	Question 2 Comment
American Electric Power	No	
Public Service Enterprise Group	No	1. R4 and part 4.1 address generator exemptions. R4 requires TOPs to develop criteria for exempting generators from R5, part 5.1. Those criteria should be made available. However, TOPs, not generators, must comply with R5, part 5.1. If the SDT's intent is to exempt specific generators from following a voltage or Reactive Power schedule, we suggest the following rewrite for R4, with no change to part 4.1:R4. Each Transmission Operator shall specify the generator criteria that will exempt Generator Operators of generators that meet these criteria from compliance with the requirement to maintain a voltage or Reactive Power schedule and publish or provide such criteria upon request.M4 would have to be rewritten, with item 2) and item 3) deleted. Because 1) exempts a generator from having to meet a voltage of Reactive Power Schedule and 2) exempts a generator from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, being exempt from having to meet a voltage schedule in 1) is equivalent to being exempt from 2). Item 3) is addressed by exemptions stated in VAR-002-3, R1 and R2.2. R5, part 5.1 should have the phrase "in automatic voltage control mode (the AVR is in service and controlling voltage)" stricken since it would not apply to a Reactive Power schedule. In addition, the TOP should not be required to provide voltage or Reactive Power schedules to exempt generators under part 5.1. Finally, the text box for R5 refers to maintaining a schedule for "normal operations." "Normal operations" is a critical assumption, which we believe is equivalent to "normal operating conditions." For example, a generator that experiences a fault on its GSU will be outside of any

Organization	Yes or No	Question 2 Comment
		voltage or Reactive Power schedule during that fault. Therefore, part 5.1 should be rewritten:5.1. Except for exempt generators, the Transmission Operator shall provide the voltage or Reactive Power schedule for the associated Generator Operator and direct the Generator Operator to comply with the schedule during normal operating conditions.3. R5, part 5.3 should have the phrase "or Reactive Power" inserted after "voltage."
Response: Thank you for your comments. Exemptions are based solely on the exemption criteria set by the TOP. The language in R4 is broader than the proposed language, and the VAR SDT wanted to provide TOPs with the latitude for providing exemptions as necessary. R4 provides exemptions from: 1) voltage schedules, 2) being in voltage control mode, or 3) any notification requirements. However, an exemption from a schedule does not necessarily equate to an exemption from an AVR setting. Also, since VAR-002 did not pass successive ballot, there is no exemption mechanism in place in VAR-002. Finally, the phrase "or Reactive Power" is being added as clarification to R5.3.		
The United Illuminating Company	No	Please note that my affirmative ballot vote was in error. We are voting NO on VAR-001.Since there is no catchall section for comments on VAR-001, we are providing comments here. Although We do agree with the removal of duplicative requirements, we are voting No on VAR-001.VAR-001 R2 remove everything after the but not limited to phrase. The various methods to obtain reactive power do not belong in the requirement but they can be included in the measure.VAR-001 R3: Clearly this is something a TOP perfroms but the compliance evidence will be overwhelming. The TOP is being asked to demonstrate that it has constantly monitored reactive and provided direction to operate reactive devices. This will require the retention of the evidence of why a reactive adjustment was necessary as well as the various adjustments made. This would mean maintaining snapshots of the normal operation of the system, records of adjustments, corrections, etc.
Response: Thank you for your comments. The draft RSAW clarifies how this requirement would be evaluated during an audit, but the compliance concerns will be conveyed for future iterations of the RSAW and auditor training.		
American Transmission	No	ATC agrees with the approach in removing any duplicate requirements.ATC also has a

Organization	Yes or No	Question 2 Comment
Company, LLC		couple comments and is recommending the following changes for the drafting team to consider:1. For consistency, Measure M2, 2nd sentence should be reworded as follows: “For the operational planning time horizon, Transmission Operators shall “have evidence of assessments” used as the basis for how resources were scheduled” The current wording of “shall provide copies” imposes an action that is not included in the associated requirement R2. 2. The following from requirement R2: “Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load” implies that all of the items listed need to be considered. If the intent is that the items are intended to be examples it is suggested that the words “including , but not limited to” be replaced by “such as”.
Response: Thank you for your response. M2 will be updated to clarify that TOPs shall have evidence of assessments, rather than provide copies of assessments. The list in R2 was originally added to answer a FERC directive on including controllable load. It was approved in an earlier version of VAR-001, so the SDT retained the same list for R2.		
Ameren	No	We request that the SDT leave the language as currently used in VAR-001-2, R4.
Response: Thank you for your comments. VAR-001-2 R4 does not allow for notifications when deviating from voltage schedules, and the VAR SDT improved on that standard language by requiring the TOP to provide more data such as notifications and criteria for schedules upon request.		
Hydro-QuÃ©bec Production	No	The requirement number five has to be removed, the reactive power of an auxiliairy transformer unit has a little impact on the ability of a groupe or plant to provide the reactive power required by the network.
Response: Thank you for your comments. VAR-002 did not pass the last ballot, and the VAR SDT will consider this during the next successive ballot.		
MRO NSRF	Yes	In requirement 5.1 a Transmission Operator is required direct a Generator Operator

Organization	Yes or No	Question 2 Comment
		to "comply with the schedule" provided by the Transmission Operator. In 5.2, however, the potential for deviations from the schedule is implied. To avoid conflict between these two, the following change to 5.1 is recommended: "The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode unless notification of deviation is provided in accordance with 5.2."For consistency M2 should be reworded as follows: "For the operational planning time horizon, Transmission Operators shall have evidence of assessments used as the basis for how resources were scheduled" The current wording of "shall provide copies" imposes an action that is not included in the associated requirement. In previous comments regarding voltage schedules issued by a Transmission Operator a mechanism for a Generator Operator to provide explanations if a proposed schedule could not reasonably be met based on specific equipment limitations and to get a revised schedule or exemption was suggested. In this version the Transmission Operator is obligated to provide additional information about the schedule, but is not obligated to respond to Generator Operator concerns regarding the schedule. Under VAR-002 a Generator Operator is required to comply with the schedule provide by the Transmission Operator unless notification is provided. There then is the potential situation where a schedule issued by a Transmission Operator cannot be met due to equipment or system conditions and the only action available is for a Generator Operator to provide multiple notifications. A better solution it seems would be to include some sort of feedback process between Generator Operators and Transmission Operations in the VAR-001 standard that would result in an agreed-upon schedule that could reasonably be met without burdensome periodic notifications. As recommended in previous comments a process of reaching "mutual agreement" on the schedule for making transformer tap changes is suggested . The SDT responded in the consideration of comments that they did not chose to include the suggested agreement language but did add a requirement for the transmission operator to provide an "implementation schedule". While this change is an improvement it does not completely solve the concern

Organization	Yes or No	Question 2 Comment
		presented. The objective should be that a tap change schedule is agreed upon that would meet the reasonable needs of both the Transmission Operator and Generator Operator. The following from requirement R2: "Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load" implies that all of the items listed need to be considered. If the intent is that the items are intended to be examples it is suggested that the words "including , but not limited to" be replaced by "such as".It is recommended that R5.1 be modified as recommended by the NERC IGVT report of September 2012: 5.1. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR or plant-level volt/var regulator is in service and controlling voltage). The standard should be reviewed and where AVR is referred to, the plant-level volt/var regulator should be added in a similar way to this recommended change to R5.1. The referenced NERC report provides the technical basis for this recommendation.
Response: Thank you for your comments. M2 has been modified to incorporate your suggestions. The VAR SDT determined that the mutually-agreed upon schedule could undermine TOP authority, and the VAR SDT also determined that AVR is a sufficiently broad term to encompass plant-level volt/VAR.		
Northeast Power Coordinating Council	Yes	We support the SDT's proposal to remove the requirements that may be redundant with other standards. However, regarding VAR-001-4 Requirement R1 was revised to read:R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits 1.1 Each Transmission Operator shall provide a copy of the voltage schedules and asspociated tolerance bands to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.What is meant by "system voltage schedule." Is it a highâ€ level, overall voltage schedule by voltage class, or a voltage schedule by station (even if there is no direct means of

Organization	Yes or No	Question 2 Comment
		controlling voltage at that station)? Requirement R5 already addresses specification of generator voltage schedules, so if that is what is intended to be addressed under R1, why is R1 needed at all? Requirement R5 states:R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range, or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the Generator Step-Up transformer at the Transmission Operator's discretion.There is inconsistency in the tense used in various VSLs. Some are in present tense while others are in the past tense. This should be reviewed and and revised as appropriate."Schedule" is used in both VAR-001 Requirements R1 and R5. However, it is modified by different phrases in each, implying different types of "schedules." These two different types of "schedules" have caused confusion, making the use and intended meaning less than perfectly clear. VAR-001 Requirement R1 - To improve clarity and consistency, suggest that the word "schedule" be deleted here and only be used when referring to GOP operation. Suggest revising Requirement R1 wording as follows:R1. Each Transmission Operator shall specify a system voltage range or a target value with an associated tolerance band as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.Note that Requirement R1 only requires that the TOP establish the target system voltage level and tolerance band. There is no mention of GOP operation.Requirement R2 requires that the TOP schedule its arrangement of sufficient reactive resources, whether actually used (dispatched) or not, a Planning function (see Measure M2). The Rationale box states: "to ensuring sufficient reactive resources are online or scheduled." The use of the word "scheduled" here again has caused confusion. We suggest it be replaced to clarify the meaning, as follows: R2. Each Transmission Operator shall make arrangements for sufficient on-line, available reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, making arrangements for reactive generation resources, transmission line and reactive resource switching, and using controllable load. Further recommend revising M2 to synchronize it with the revised

Organization	Yes or No	Question 2 Comment
		Requirement R2 above, as follows:M2. Each Transmission Operator shall have evidence of sufficient reactive resources based on their assessments of the system. For the operational planning time horizon, Transmission Operators shall provide copies of assessments used as the basis for determining how resources were made available. Organizationally, R4 should be swapped with R5. A requirement dealing with exemptions should come after the “foundation” requirement.The Drafting Team must consider the following regarding Hydro-Quebec TransEnergie. "Schedule" in the standard is confusing and does not apply to Hydro-QuÃ©bec TransÃ‰nergie. Hydro-Quebec TransEnergie does not issue a schedule of voltage or reactive power. Hydro-Quebec TransEnergie sets voltage ranges to comply at all times for the different voltage levels. During light or peak load, these operating situations are governed with voltage setupoints for specific substations. The standard should therefore consider (in addition to the preceding comments) the terms used. For example, consider substituting the term " voltage or reactive power setpoint " for the word “schedule” which does not reflect our operating procedures.Regarding Requirement R5, NERC now requires a specified program voltage or reactive power be given to central planning and forecasting. This requirement is not applicable to Hydro-QuÃ©bec TransÃ‰nergie because there is no voltage or reactive power schedule, but rather the requirement that every generating facility of more than 10 MW have an automatic voltage regulation system. Hydro-Quebec TransEnergie also requires them to provide a specific power factor for each of those generating units.
Response: Thank you for your comments. Requirement R1 is the overarching system voltage schedule, and Requirement R5 targets generating voltage schedule. The requirement does not require a schedule for a station with no way of controlling voltage. Voltage schedule is an industry term that is explicitly defined by the parenthetical definition. The VAR SDT could not make the proposed Requirement R2 changes because it could cause clarification for some while causing confusion for other industry members. Requirements R4 and R5 stand independently. Finally, for R5 the VAR SDT determined that the term “schedule” is broad enough to encompass Hydro Quebec’s concerns.		
Bureau of Reclamation	Yes	The Bureau of Reclamation (Reclamation) notes that the WECC variance indicates that it is intended to replace requirements R3 and R4. However, R3 and R4 in VAR-

Organization	Yes or No	Question 2 Comment
		001-4 are not the same as R3 and R4 in VAR-001-3. Reclamation suggests that the drafting team should examine the WECC variance to determine which requirements it will replace because it appears that the WECC variance should replace R4 and R5. In WECC, it would be difficult for Transmission Operators to comply with both R5 and E.A. 14 because they refer to different voltage schedule reference points. VAR-001-4 R3 specifies that Transmission Operators must operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary. Measure M3 specifies that "this may include directions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments." Reclamation suggests that this detail should be included in Requirement R3 rather than solely in the measure.VAR-001-4 R4 requires a Transmission Operator to notify a Generator Operator if the "Transmission Operator determines that a generator has satisfied exemption criteria" but does not specify a timeframe for this notification. Reclamation suggests that the drafting team update VAR-001-4 R4 to specify that the Transmission Operator must notify the Generator Operator within 30 days if the Transmission Operator determines that a generator has satisfied criteria for exemption from voltage or Reactive Power requirements and associated notification requirements. Reclamation also suggests that R4 on exemptions should follow R5 on voltage or Reactive Power scheduling and notification criteria. VAR-001 R5 allows the Transmission Operator to specify a voltage or Reactive Power schedule at either the high voltage side or low voltage side of the Generator Step Up transformer. Reclamation suggests that like in requirement E.A.14, Transmission Operators should be able to specify the voltage schedule at the generator terminals, high side of the generator step-up transformer, point of interconnection, or a location designated by mutual agreement. VAR-001 R5.2 specifies that "The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule." M5 regarding part 5.2 specifies that voice recordings may be used to establish compliance with this requirement. Reclamation suggests that voice recordings should be removed from the list in M5 for part 5.2 because notification

Organization	Yes or No	Question 2 Comment
		requirements established in the planning horizon should be transmitted in writing. Reclamation notes that there is a potential inconsistency between the Transmission Operator notification requirements discussed in VAR-001 R5.2 and the Generator Operator notification requirements discussed VAR-002 R3 and R4. Reclamation recommends that VAR-001 R5.2 be modified to solely address planning horizon notifications. For consistency with the Generator Operator real-time notification requirements established in VAR-002 R3 and R4, Reclamation also recommends that VAR-001-4 R5 should include an additional subrequirement which specifies that the "TOP shall develop real-time notification requirements for the deviations from the voltage of Reactive Power schedule within 30 minutes of when a Generator Operator becomes aware of a change in reactive capability, AVR status, power system stabilizer status, or alternative voltage controlling device status, unless the status is restored within 15 minutes." VAR-001-4 R5 requires the Transmission Operator to specify a voltage or Reactive Power schedule "at either the high voltage side or low voltage side of the Generator Step-Up transformer." VAR-002-3 R2.3 allows Generator Operators to monitor voltages at another location so long as the Generator Operator has a "methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator." Reclamation suggests that having the Transmission Operator and Generator Operator monitor voltages at different locations could lead to confusion in real-time communications. Reclamation suggests that VAR-001-4 R5 be updated to require the Transmission Operator to set voltages based on common monitoring locations to avoid confusion in real-time communications between Transmission Operators and Generator Operators.Reclamation suggests that R6 should be updated to specify that the Transmission Operator must coordinate outages to accommodate required step-up transformer tap changes. Reclamation suggests the drafting team update the requirement to read "After consultation with the Generator Owner regarding necessary step-up transformer tap changes, associated outages, and the implementation schedule...". Reclamation also notes that "Generator Step-Up transformer" is sometimes capitalized in the standard. However, it is not capitalized

Organization	Yes or No	Question 2 Comment
		in the WECC variance or NERC Glossary. Reclamation suggests that the drafting team remove capitalization in the term "Generator Step-Up transformer" because it is not defined in the NERC Glossary.
Response: Thank you for your comments. WECC has a separate process for its regional variance, and WECC will revisit the variance as needed. The measure language does not belong in the standard because it is not an exhaustive list, and it serves as an example for what an auditor should look for in evaluating the requirement. The notifications for exemption are not specified because there may be instances where a GOP receives pre-authorized exemptions. For example, a TOP may specify instances where a GOP does not have to notify the TOP through a pre-approved process. The WECC variance will remain intact, but the variance could not be adopted continent-wide because there was no industry consensus on how to provide the schedule. The language for M5 has been updated to remove the list of evidence because it is not a comprehensive list of all communications. The VAR SDT determined that the GOP must make notifications to the TOP of reactive capability changes, and the deviations are not necessary in VAR-001. The VAR standard cannot add a mutually agreed upon reference point because several GOPs and TOPs can reach a consensus on the mutually agreed upon point. The VAR-002 issues will be addressed in the next successive ballots.		
Southern Company: Southern Company Services, Inc.; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing	Yes	: The High VSL for VAR-001 R4 should be changed from the proposed state to "The TOP has exemption criteria, but did not notify the GOP." As it is currently written, the TOP satisfied R4, but simply cannot show documentation to prove the satisfaction. The proposed change wording focuses on the TOP not satisfying the requirement. The first clause in the Severe VSL for VAR-001 R5 should be corrected to state "voltage or Reactive Power schedules." In addition, the Severe VSL for VAR-001 R5 should have another OR clause to include the failure to comply with R5.3.
Response: Thank you for your comments. The VAR SDT did not agree on all changes for the VSLs at this time, but a failure to comply with R5.3 is already in the moderate VSL category.		
Florida Municipal Power Agency	Yes	FMPA appreciates the efforts of the SDT to remove some of the duplicative requirements of the VAR standards with other standards (e.g., TOP and FAC

Organization	Yes or No	Question 2 Comment
		standards). However, FMPA is voting Negative because we believe more requirements ought to be treated in the same fashion as described in our earlier comments on the September posting, as provided in a mapping document submitted directly the the SDT to better illustrate those duplications, and as summarized below.VAR-001-4 R2 is duplicative of the requirements of TOPs to plan for and operate to SOLs in the TOP and FAC standards. In order to plan to and operate to SOLs, TOPs must schedule sufficient reactive resources, or they will violate those requirements (just as must-run generators need to be scheduled, yet those are not discussed within the standards). Operating to SOLs is results based, VAR-001-4 R2 is not. VAR-001-4 R2 ought to be deleted.VAR-001-4 R3 is duplicative of requirements of TOPs to plan for and operate to SOLs as described above. As far as TOPs ability to direct, that is covered in TOP-001. VAR-001-4 R3 should be deleted.Although FMPA supports both VAR-001-4 R1 and R5, we wonder if there is some duplication between those requirements and whether they can be combined into a single requirement.
Response: Thank you for your comments. However, the recent TOP standards are remanded by FERC and are being reevaluated generally. The standard cannot rely on implied processes in other standards that are currently in development. R2 and R3 are very specific to voltage requirements which are necessary for the reliable operation of the grid. R1 and R5 are not duplicative because R1 addresses an overall system voltage, and R5 is where TOPs provide a schedule for Generator Operators to maintain.		
Tennessee Valley Authority	Yes	The SDT is requested to clarify the word “directions” as used in M3. The word “directions” is close to, but not, the word “directive” which has a very specific meaning. If the intent is to capture directives, then the word directives should be used. If the intent is to capture communications that are not directives, then the word “directions” should be replaced with wording that is not so close to the word “directives.”Current M3 draft language: M3. Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as needed in Real-time. This may include directions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments. The SDT is requested to consider a modification to R4:Current R4 draft language: R4. The Transmission Operator shall specify the criteria that will exempt

Organization	Yes or No	Question 2 Comment
		generators from compliance with the requirements defined in Requirement R5, part 5.1, and any associated notification requirements. Suggested modification to R4: R4. The Transmission Operator shall specify the criteria, ADD: "if any" that will exempt generators from compliance with the requirements defined in Requirement R5, part 5.1, and any associated notification requirements.
Response: Thank you for your comments. M3 has been updated to use the word "instructions" instead of "directions." The standard provides each TOP with the flexibility to determine its own exemption criteria and does not mandate that a TOP issue exemptions.		
PacifiCorp	Yes	PacifiCorp supports MidAmerican's comments.
Duke Energy	Yes	Duke Energy approves of the approach of removing duplicative requirements based on other standards.Duke Energy seeks clarification on the definition of "system voltage schedule" and believes that once this is more clearly defined, it should be added to the NERC Glossary of Terms.The Rationale for Requirement 1 discusses the TOP setting voltage or Reactive Power schedules with associated tolerance bands. However, Requirement 1 makes no mention of using Reactive Power schedules. Is the use of Reactive Power Schedules implied in Requirement 1?Duke Energy suggests changing "Each Transmission Operator shall schedule" to "Each Transmission Operator shall maintain" in Requirement 2 for more clarity. In Duke Energy's opinion, not all reactive resources can be "scheduled" in order to regulate voltage levels. For example, SVCs cannot be scheduled, the reactive resources of an SVC dynamically change to maintain set voltage levels. The TOP needs to ensure that adequate static and dynamic reactive resources are availble to the System Operator in real time to support the Reliability needs of the BES. Reliability Studies are performed in the Operations Planning horizon to ensure that reactive resources are adequate to support the planned BES configuration.
Response: Thank you for your comments. Requirement R1 requires an overarching system voltage schedule, and TOPs do not set Reactive Power schedules for the system. Requirement R5 is the requirement directed towards Generator Operators where a		

Organization	Yes or No	Question 2 Comment
voltage schedule or a Reactive Power schedule is maintained. The VAR SDT cannot come to a consensus that "maintain" will alleviate compliance issues with regard to specific equipment being available to address voltage levels.		
SPP Standards Review Group	Yes	We agree with the retirement of redundant requirements and suggest that the drafting team delete R2 and R3 in addition to the other deletions already proposed. R2 is redundant with the pending TOP-002-3, R1. R3 is redundant with pending TOP-001-2, R7 and R9.
Response: Thank you for your comments, but Requirements R2 and R3 cannot be deleted because they are specific to voltage and reactive flows.		
ACES Standards Collaborators	Yes	(1) Requirement VAR-001-4 R1 is vague and ambiguous and may be duplicative of VAR-001-4 R5. It requirements need further refinement. First, it states that the TOP shall specify "a system voltage schedule". This is singular. A system always has multiple schedules for generators, capacitor banks, reactors, etc. It does not have a single voltage schedule. Second, what equipment or facilities is the voltage schedule supposed to apply? Is this supposed to be the voltage schedule for a generator? Is this supposed to the voltage for reactor or capacitor switching? Is this supposed to be the voltage limits on a transmission bus? Schedule would tend to imply a level of control and, thus, not a limit but the simple reality is that the requirement is vague, ambiguous, and unenforceable as written. Third, if the requirement applies to voltage schedules at generators, it is duplicative to VAR-001-4 R5 because this already compels the TOP to provide voltage schedules for generators. Please provide additional clarifications in the requirement. (2) We appreciate the drafting team removing duplicate requirements. This version of the standard has been improved greatly. However, we still believe there is some duplication that needs to be addressed. For example, VAR-001-4 R1 requires a TOP to "specify a system voltage schedule... as part of its plan to operate with System Operating Limits and Interconnection Reliability Operating Limits" while VAR-001-4 R2 requires the TOP to "schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions". How does a TOP specify a voltage schedule per R1 and not

Organization	Yes or No	Question 2 Comment
		also schedule sufficient reactive resources per R2? The TOP can't maintain the voltage schedule without scheduling sufficient reactive resources. Please eliminate the duplication. (3) VAR-001-4 R2 is also duplicative of VAR-001-4 R3. R2 requires the TOP to "schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions" while R3 requires the TOP "to operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow". How does the TOP schedule sufficient reactive resources without regulating transmission voltage and reactive flow? The TOP would be operating the voltage-regulation devices when they schedule sufficient reactive resources since the voltage-regulation devices are reactive resources. If the purpose was to delineate by time frames implied by the use of "Real-time Operation" in R3 and "schedule" in R2, the requirements need further refinement to be clear that the targeted time frames are supposed to be different. Furthermore, the Time Horizons for both R2 and R3 are duplicate covering Real-time Operations, Same-day Operations, and Operational Planning which would imply that different time frames are not intended. Please eliminate the duplication or clarify the time frames as appropriate. Detailed application guidelines would help eliminate some of the confusion. (4) Part 1.1 meets P81 criteria and should be retired. The requirement meets Criterion A (overarching) because it "does little, if anything, to benefit or protect the reliable operation of the BES" and meets criterion B4 - Reporting because it requires the TOP to report to another party and has "no discernible impact on promoting the reliable operation of the BES." The mere fact that Part 1.1 only requires reporting upon receiving a request is supportive that it has no impact on reliability. If it did materially support reliability, the RC would be required to have the data and the TOP would be obligated to provide it. Please remove Part 1.1. If Part 1.1. persists in the next draft, we request that the drafting team provide written justification for why these requirements do not meet P81 criteria and actually materially support reliability.(5) Measure VAR-001-4 M2 is inconsistent with the main requirement R2 and needs to be modified. M2 proposed that the TOP shall have evidence of scheduling resources based on their system assessment. While we agree this is likely

Organization	Yes or No	Question 2 Comment
		the method the TOP will use to schedule resources, the simple fact is that it is not part of the requirement and cannot be compelled in the measure. Please modify the measure to be consistent with the requirement. (6) The second sentence of R2 is an explanation and not a requirement. Thus, it should be moved to the application guidelines section. We understand that FERC previously directed NERC to include use of controllable load as a reactive resource because it was not one of the explicitly listed reactive resources. FERC likely included this statement as evidenced by the first sentence of paragraph 1879 of Order 693 to further a policy goal of expanding the use of demand side management (DSM). At the time the order was issued, DSM was in its infancy. Today, DSM has become ubiquitous as demonstrated by the almost 40,000 MW reported in the NERC 2013 Summer Assessment. Given that all organized markets include at least one DSM product, its proliferation will only continue. Thus, the policy goal has been clearly met and specific mention in NERC standards in no longer necessary. In fact, an equally efficient and effective alternative would be to eliminate specific references of any type of reactive resource by striking the second sentence in its entirety. (7) The Time Horizons for VAR-001-4 R3 are inconsistent with the requirement. R3 specifically states that it deals with Real-time operation. Thus, how could Operational Planning and Same-day Operation be applicable? These timelines are conflicting and need to be modified.(8) For requirement VAR-001-4 R4, why can't the GOP make a self-determination that it meets the TOP criteria? Is the TOP obligated to make a determination or to simply supply the criteria to the GOP? The RSAW indicates that the auditor will not determine if the GOP received pre-authorization from the TOP. Thus, the requirement should either be modified so that audit practices will have to be modified or aligned with how the RSAW indicates compliance will be assessed. We recommend that the drafting team work with NERC compliance to align the requirement with the RSAW language.(9) VAR-001-4 R5 should be modified to clarify that the TOP is not required to provide a voltage schedule to all generators but only to those generators that it determines it needs to provide reactive supply. A TOP may determine that a generator is too small to control voltage at its location and that it does not need to provide a voltage schedule

Organization	Yes or No	Question 2 Comment
		for this generator. Including all generators is unnecessary for reliability.(10) Part 5.3 meets a P81 criterion and should be retired. The requirement meets Criterion A (overarching) because it "does little, if anything, to benefit or protect the reliable operation of the BES" and meets criterion B4 - Reporting because it requires the TOP to report its criteria to another party and has "no discernible impact on promoting the reliable operation of the BES." The mere fact that Part 5.3 only requires reporting upon receiving a request is supportive that it has no impact on reliability. If it did support reliability, the GOP would be required to have the data. Please remove Part 5.3. If Part 5.3 persists in the next draft, we request that the drafting team provide written justification for why these requirements do not meet P81 criteria and actually materially support reliability.(11) We request that R6 be modified to state that the timeframe shall be mutually agreeable. The TOP is only required to consult with the GO and could still provide an unreasonable timeframe after such consultation. At the very least, the requirement needs to be clear that the GO and GOP are not obligated to take an outage to implement tap changes and would be allowed make them at the next scheduled maintenance or forced outage with sufficiently long outage window to allow such changes. (12) The evidence retention section needs to be updated. First, it covers only measures one through four when there are actually six. Second, it covers measures when it should cover requirements to be consistent with existing standards. (13) As written, the VSL for R1 is overly harsh. If a TOP simply failed to create a single voltage schedule, it would be a severe violation. It seems the VSLs could be graduated based on the number of voltage schedules that are not created as a percentage of the total voltage schedules.(14) The VSLs for R2 and R3 are inconsistent with the requirement. The High VSL and Severe VSL mention avoiding violating an SOL or IROL respectively. However, the requirement mentions neither. This would be inconsistent with FERC guideline three that VSLs should be consistent with the corresponding requirement. (15) The High and Severe VSLs for R2 and R3 overlap with one another. High VSLs for both requirements apply to SOL violations and Severe VSLs for both requirements apply to IROL violations. By definition in the NERC glossary, an IROL is a subset of a SOL. Thus, a failure to schedule or operate

Organization	Yes or No	Question 2 Comment
		reactive resources that results in an IROL violation would be both a High and Severe violation simultaneously. (16) From a compliance perspective, the High VSL for VAR-001-4 R4 is a logical fallacy. Compliance requires evidence. Thus, an auditor cannot make a determination that a TOP has exemption criteria but does not have evidence of exemption criteria. Thus, the High VSL could never be assigned by a compliance enforcement authority. This needs to be modified.(17) The VSLs for VAR-001-4 R5 need to be modified. In the FERC order approving VSLs, FERC was clear that as many VSLs as possible should be used. Clearly, each VSL could be assigned based on the number of GOPs that the TOP failed to provide voltage schedules. This essentially means that the High VSL should be graduated. We disagree with assigning a moderate VSL for the failure of a TOP to provide its criteria in response to Part 5.3 by one minute. As written, the TOP could literally be one minute past the 30 day time frame and reach a moderate violation. This should not even be a violation let alone a Moderate VSL. The solution is to remove Part 5.3. If Part 5.3 persists, at a minimum, the VSL should be Lower because reliability is not impacted. The second half of the Severe VSL regarding not supplying the notification requirements to the GOP should be moved to Moderate VSL. Failure to provide voltage schedules misses significantly more of the spirit of the requirement than failure to provide exemption criteria. The purpose of failure to provide exemption criteria is an attempt to avoid nuisance violations not directly support reliability. (18) In the regional variances section, E.A. 16 and E.A. 17 meet P81 criteria and should be removed from the next draft. The purpose of these two requirements is to provide transparency between the GOP and TOP in determining voltage schedules and implementation of voltage schedules. While establishing transparency is certainly a laudable goal, it simply does not directly support reliability. Thus, these two regional variance requirements meet Criterion A (overarching) because they do little, if anything, to benefit or protect the reliable operation of the BES and meet criterion B4 - Reporting because they require the TOP and GOP to report to each other. (19) It is unnecessary to require the TOP to direct the Generator Operator to comply with the voltage schedule with the AVR in voltage control mode in VAR-001-4 Part 5.1. It is redundant with VAR-002-3 R2 which

Organization	Yes or No	Question 2 Comment
		compels the GOP to follow the voltage schedule. If drafting team feels the "directive" language is necessary in VAR-001-4 Part 5.1, then VAR-002-3 R2 should be removed because it would be redundant with TOP-001-1a R3 (existing) and TOP-001-2 R1 (pending regulatory approval). Both require the GOP to follow the directives of its TOP.
Response: Thank you for your comments. Requirement R1 is intended to be the requirement addressing an overarching system schedule, and R5 is directed to the schedules provided to the GOPs. Requirements R1, R2, and R3 are separate requirements where R1 sets a voltage schedule for the system. R2 and R3 represent the actual action a TOP will take to meet voltage requirements. Further, R1 is part of the operational planning horizon, while R2 and R3 include real-time and same day operations. Part 1.1 requires vital information to be shared between entities, and this is particularly important to have accurate studies with regard to interface facilities. M5 has been updated to remove "provide copy." Controllable Load was added per a FERC directive, and the VAR SDT does not believe that it should be removed through an equally effective and efficient manner. The second sentence in R2 is meant as an illustration. For the time horizon, Real-time events may bleed into next-day or longer operations. Directives may extend from the Operational Planning Horizon into the current-day. For reliability purposes, it would not be reasonable for the GOP to grant its own exemptions. All generators must follow a voltage or Reactive Power schedule. Part 5.3 provides the technical justification for a voltage schedule which answers a FERC directive. The TOP must set notifications and timeframes in order to prevent disputes between TOP and GOPs. The VAR SDT discussed this at length, and the VAR SDT determined "consult" was the appropriate word for making tap changes. The evidence retention section has been modified. Compliance will be provided a copy of these comments. The VSLs reflect the SOL and IROLs because those are the system events that would precipitate a TOP action. The VSLs for Requirements R2 and R3 refer to SOL and IROL violations because the purpose of requiring TOPs to "schedule sufficient reactive" and "operate or direct the Real-time operation of devices" is to avoid violations of SOLs and IROLs. As provided in Requirement R1, TOPs must specify a system voltage schedule to ensure that the system is operated within System Operating Limits and Interconnection Reliability Operating Limits, as required under the FAC and TOP standards. Thus, the VAR SDT did not determine a severity level is necessary for anything except an SOL or IROL violation. For all of the requirements the VRF determines the risk to the system while the VSL determines how a requirement is violated. For R4, the VRF is lower, but the violation is still high because a part of the requirement has been violated. WECC will determine if any updates should be made to the WECC variance. For part 5.1, VAR-001 represents the TOP obligations, and VAR-002 has a sister requirement that represents the GOP obligations.		

Organization	Yes or No	Question 2 Comment
ISO/RTO Standards Review Committee	Yes	We support the SDT's proposal to remove the requirements that may be redundant with other standards. We do not have any comments on the requirements, Measures or VRFs, but we do have some comments on the VSLs:a. R1: The word "schedule" after "system voltage" is missing from the VSL.b. There is inconsistency in the tense used in various VSLs - some are in present tense while others in past tense. Please review and revise as appropriate.
Response: Thank you for your comments. The VSLs have been reviewed and corrected to be in the same tense.		
Bonneville Power Administration	Yes	There are two questions under Question #2. BPA answered the first question in the check box. BPA's answer to the second part of the question is No.
Response: Thank you for your comments.		
NorthWestern Energy	Yes	For R2, M2 - It would be very helpful if "their assessments of the system" be clearly defined. For example, would TPL studies suffice as evidence for meeting this requirement or is this more of a real time requirement and if so, what types of evidence is NERC lokking for.
Response: Thank you for your support. TPL studies are part of a different time horizon than Requirement R1. Assessments may take several forms depending on the internal structure of the entity. Also the measure for this requirement will no longer include copies of the assessments.		
Consolidated Edison Co. of NY, Inc.	Yes	The drafting team used the word "schedule" in both VAR-001 Requirements R1 and R5. However, it is modified by different phrases in each, implying different types of "schedules." These two different types of "schedules" has caused confusion, making the use and intended meaning less than perfectly clear. VAR-001 Requirement R1 - To improve clarity and consistency, we recommend that the word "schedule" be deleted here and only be used when referring to GOP operation. The revised Requirement R1 wording recommended follows:R1. Each Transmission Operator shall specify a system voltage [delete: schedule (which is either a] range or a target value with an

Organization	Yes or No	Question 2 Comment
		associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.Note that Requirement R1 only requires that the TOP establish the target system voltage level and tolerance band. There is no mention of GOP operation.Requirement R2 requires that the TOP document its arrangement of sufficient reactive resources, whether actually used (dispatched) or not, a Planning function (see Measure M2). The Rationale box states: "to ensuring sufficient reactive resources are online or scheduled." Comment: The use of the word "scheduled" here again has caused confusion. We recommend it be replaced to clarify the meaning, as follows: R2. Each Transmission Operator shall make arrangement for [delete: schedule] sufficient on-line, available reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, making arrangements for reactive generation resources [delete: scheduling], transmission line and reactive resource switching, and using controllable load. We further recommend revising M2 to synchronize it with the revised Requirement R2 above, as follows:M2. Each Transmission Operator shall have evidence of [delete: scheduling]sufficient reactive resources based on their assessments of the system. For the operational planning time horizon, Transmission Operators shall provide copies of assessments used as the basis for determining how resources were [delete: scheduled] made available. The verbiage of R4 should come after R5 is stated. From an organizational perspective, a requirement paragraph on exemptions should come after the referenced requirement.
Response: Thank you for your comments. Please see the response to NPCC above.		
City of Garland	Yes	1st question: Yes - we agree with this approach2nd question: We have comments on R2. In ERCOT, the TOP can only plan to respond to voltage issues with the resources they have available. They do not have authority to order generation on line for voltage support nor do they have authority to back down fully loaded generation for voltage support. Only the RC has this authority.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comments. Please see the responses to ERCOT and CenterPoint above.		
Manitoba Hydro	Yes	(1) M1 - the language in the second paragraph re: Part 1.1 does not match the language of the requirement itself in that the measure refers only to voltage schedules, not voltage schedules 'and associated tolerance bands'. (2) R3 - without further clarification, 'as necessary' will be interpreted to mean as deemed necessary by the Transmission Operator. (3) M3 - the measure in this part contains more details and is more narrow than the requirement itself. The requirement refers to the operation of 'devices to regulate transmission voltage and reactive flow' while the measure refers to the operation of 'capacitive and inductive resources'. Language should be consistent. (4) R4 - the language goes back and forth between 'generators' and 'generating units' - this should be made consistent. Also, the reference to 'associated notification requirements' presumably refers to the associated notification requirements in R5 but this is not specified. (5) M4 - the qualification language that it refers only to generating units 'in its area' appears only in the measure and not in Part 4.1 itself. (6) R5 - neither Generator nor Step-Up is a defined term so they should not be capitalized. (7) M5 - there is a shift in language here. Generally the measures indicate that the responsible entity 'shall have evidence' and that the evidence 'may include'. In this measure, the language is that the responsible entity 'shall have evidence' and that the evidence 'shall include'. This is much more restrictive and may make compliance more difficult as there is no longer flexibility in the evidence that will meet the criteria of the measure. (8) Compliance, Evidence Retention 1.2 - Measures 5 and 6 are not mentioned. (9) Compliance, Compliance Monitoring, 1.3 - The language refers specifically to processes found in the NERC Rules of Procedure. Generally in draft standards, there is just a list of processes that may be used. The reference included in this draft standard is concerning because MB Hydro has their own Compliance and Monitoring program and has only adopted select aspects of the NERC Rules of Procedure. (10) VSLs, R4 - the words 'of the Generator Operator' are missing from the end of this section. (11) VSLs, R5 - the words 'and associated tolerance bands' is missing from Moderate VSL after 'voltage

Organization	Yes or No	Question 2 Comment
		schedules' and is not fully referenced in Severe VSL.(12) VSLs, R6 - the words 'Documentation specifying requiring tap changes was provided to the Generator Owner but' could be inserted at the start of each of the Lower VSL and Severe VSL.
Response: Thank you for your comments. Some clarifying language has been added to the VSLs. The measurement for M3 is an example of the type of information that can be provided and does not limit the breadth of the requirement. For R4 the associated notifications are specified because they are also used in VAR-002. The capitalization of generator step up in R5 has been corrected, in addition to the M5. Data retention has been changed to include all of the measures. Compliance Monitoring language has removed a reference to the Rules of Procedures. The VSLs have been updated to include "to the generator operator" and to include the definition of voltage or Reactive Power schedules.		
Electric Reliability Council of Texas, Inc.	Yes	ERCOT agrees that duplicative requirements should be removed. However, the standard would benefit from additional revisions.A. R1 and R5 should be merged. This could be accomplished in the following manner: "Each Transmission Operator shall notify associated RCs and adjacent TOPs, and specify assigned GOs the a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan required forassigned GOs to operate within System Operating Limits and Interconnection Reliability Operating Limits.B. The second sentence of VAR-001 R2 is not needed. This is not an actionable requirement, but rather is an instruction as to how it's to be done. The 2nd sentence is not a requirement.C. Recommend deleting from R5.1 the words, "...in automatic voltage control mode (the AVR is in service and controlling voltage)." The standard should establish what needs to be done, and how the GO elects to comply with the requirement should be left to the discretion of the GO. Furthermore, VAR-002 requires the GO to have its AVR in service and in auto, so this requirement is also redundant.D. It appears that VAR-001 R6 is redundant to R5.3. Also see comments on VAR-002 R6.
Response: Thank you for your comments. The VAR SDT consensus was to leave Requirements R1 and R5 as separate requirements. R1 sets for requirements for the overarching system voltage while R5 specifies schedules for control buses. The second sentence is meant as an illustration. The VAR SDT and NERC staff determined that the AVR operation in the voltage		

Organization	Yes or No	Question 2 Comment
control mode is necessary for system reliability.		
Independent Electricity System Operator	Yes	We support the SDT's proposal to remove the requirements that may be redundant with other standards. We do not have any comments on the requirements, Measures or VRFs, but we do have some comments on the VSLs:a. R1: The word "schedule" after "system voltage" is missing from the VSL.b. There is inconsistency in the tense used in various VSLs - some are in present tense while others in past tense. Please review and revise as appropriate.
Response: Thank you for your comments. The VSLs have been modified to clarify language and correct the differences in tense.		
Kansas City Power & Light	Yes	I agree with the approach to condense standards if they are duplicated in other standards.
Response: Thank you for your comments.		
Xcel Energy	Yes	Xcel Energy appreciates the hard work of the Standard Drafting Team. We recognize that significant effort has been put into the modifications of the VAR-001 and VAR-002 standards and we applaud the direction the team is moving. We are voting Negative on VAR-001-4 for one reason which we explain below.Xcel Energy believes that the WECC Regional Variance should not replace R4 in the NERC standard based on the rationale provided for modifications to the proposed R4. Instead, WECC Regional Variance Requirement E.A.13 should be removed and the remaining Regional Variance Requirements should supplement the NERC Requirements in the Western Interconnection. As proposed, the NERC standard states that the TOP is not bound to provide a voltage schedule for each BES generator; however , due to the WECC variance, the TOP would be found in violation if any BES Generator was not provided a voltage schedule. In order to resolve the issue, Xcel Energy asks the drafting team to delete E.A.13 in its entirety and modify the language of the Regional Variance to state that the additional requirements are for in addition to the NERC requirements. Once this modification is made, Xcel Energy could support the

Organization	Yes or No	Question 2 Comment
		proposed standard.
Response: Thank you for your comments. The regional variance must be addressed through WECC. WECC will determine if the variance should be updated accordingly.		
Puget Sound Energy	Yes	- The first paragraph of the Regional Variance section of VAR-001 should be updated to reflect that requirements R3 and R4 of the current standard are requirements R4 and R5 in the proposed standard.- M4 should be updated to reflect that the Generator Op
Response: Thank you for your comments. The regional variance must be addressed through WECC. WECC will determine if the variance should be updated accordingly.		
City of Austin dba Austin Energy	Yes	City of Austin dba Austin Energy (AE) agrees with removing duplication. AE does not have any comments about the requirements, but requests the SDT review the VSL for R2 because the text does not match the requirement text.
Response: Thank you for your comments. The VSL have been updated to provide clarification and correct the difference in tenses.		
Utility System Efficiencies, Inc.	Yes	Many of the other standards that require the provision of this sort of information to the RC and neighboring entities includes a requirement that the entity respond to comments/concerns from the copied entities. Why not here?R2 appears to be a little ambiguous; does this apply to all contingency conditions? Just N-1? Only those chosen by the TOP? This would appear to be hard to determine compliance by the Region.It looks like R6 assumes that the GO has a non-LTC transformer. We are seeing LTCs in generation facilities; shouldn't this be modified to address the LTC GSUs?For M2 and M3 particularly, Evidence Retention could require a lot of data for 12 months.
Response: Thank you for your comments. The IRO standards will address the RC responsibilities. The contingencies are not		

Organization	Yes or No	Question 2 Comment
uniform across the continent, but the standard is concerned with contingencies to which the entity operates. The VAR standard does not define an entity's contingencies. R6 is focused on non-LTC transformers. An LTC would not require scheduling because the generating unit will not be taken offline to make the tap changes. There is no data retention requirement under VAR-001 for under load tap changers specifically, but the VAR-001 does provide data retention requirements generally.		
Consumers Energyu	Yes	This is a two part question with only one YES/NO answer. YES we agree with the approach. YES we have questions or comments on the remaining revised requirements.In R4, there should be a statement that the TOP will publish the exemption criteria to GOPs in the area.A consideration should be made to reserves R1 and R5. It is imperative both get the voltage schedules but if the GOP does not have them there is no control.
Response: Thank you for your comments. TOPs must notify GOPs when exemption criteria have been met. R1 sets the overarching system voltage schedule, and R5 provides GOPs with individual voltage or Reactive Power schedules.		
Exelon Companies	Yes	Yes, agree with approach, no additional comments relating to requirements. Exelon companies would vote Affirmative for VAR-001-4 if it were being balloted separately from VAR-002-3.
Response: Thank you for your comments. VAR-001-4 and VAR-002-3 were balloted separately.		
CenterPoint Energy, Houston Electric LLC.	Yes	CenterPoint Energy agrees with the SDT's efforts to eliminate duplicated standards, but has the following concerns. R1.1 is unclear on the applicability of the "30 days of a request." Is the requirement for Transmission Operators to provide their perspective Reliability Coordinators the voltage schedule automatically without a request and only to any adjacent Transmission Operators that requests the schedule within 30 days of the request; or is it the intent of the SDT for the Reliability Coordinator to also request the Transmission Operator for the schedule with the same "30 days of request" requirement. In order for a TOP to obtain evidence to prove compliance to this requirement, a TOP must receive documentable requests from its RC and/or its adjacent Transmission Operators to then provide the voltage

Organization	Yes or No	Question 2 Comment
		schedule within the 30 days of the request. If the Transmission Operators do not receive such requests then essentially according to the standard they do not have to provide the established voltage schedules as the requirement currently specifies. Many Reliability Coordinators or regions have established voltage working groups with processes or its equivalence to aid in the corroboration and defining of company specific voltage schedules within the RCs area or region then such voltage schedules would already be provided as part of the regional processes. CenterPoint Energy recommends the following clarifying language:"If requested, Eeach Transmission Operator shall provide, a copy of the voltage schedules and associated tolerance bands to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of such a request." CenterPoint Energy agrees with providing the Generator Operators the voltage or Reactive Power schedule; however, we believe R5.1, which also requires the Transmission Operator to direct the Generator Operators to comply with such schedule to the specificity that the AVR be in automatic voltage control mode, is redundant and is an unnecessary requirement as well as a compliance burden for the Transmission Operators. Exemptions to the Generator Operator to deviate from the established voltage schedule or the Automatic Voltage Regulator functioning in any mode other than automatic voltage control are addressed in R4 and VAR-002-3 R1 and R2 and will be handled in Real-Time operations and will be scenario specific. VAR-002 R1 and R2 requires Generator Operators to maintain the voltage or Reactive Power schedule and operate each generator with its AVR in service and in the automatic voltage control mode. Based upon this redundancy and Paragraph 81 criteria regarding duplicative and redundant requirements CenterPoint Energy recommends removal of the language "...and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage)".
Response: Thank you for your comments. For part 1.1, the voltage schedules are provided to the RC and neighboring TOPs within 30 calendar days of a request by either entity. The VAR-002 issues will be addressed in the next successive ballot for VAR-002. The SDT and NERC staff believes that the AVR operation in the voltage control mode is necessary for system reliability.		

Organization	Yes or No	Question 2 Comment
PJM Interconnection	Yes	PJM recommends the drafting team revise R1 as follows:Each Transmission Operator shall specify a system voltage schedule. The remaining language in that requirement is not needed to support reliability.PJM does not understand the scope of controllable load in R2. We urge the drafting team to include clarification.For R3, PJM recommends revision to the Time Horizon to include Real Time only.PJM recommends the following addition to R5 as the last phrase in the requirement for consistency with R4 language. "unless otherwise exempted as noted in R4."
Response: Thank you for your comments. The additional language in R1 was added to clarify what is meant by "voltage schedule" at the request of my industry participants. Controllable load was added as FERC directive in Order No. 693. The SDT believes R3 applies to Real-time, Same-day, and Operational planning horizons.		
Tri-State Generation and Transmission Association, Inc.	Yes	In the draft of VAR-001-4 R2 the use of the word 'schedule' when referring to all reactive resources is unclear. This is in conjunction with the Compliance response to question 2 part 2, "...provide the documentation for the day ahead scheduling in addition to documentation supporting that it was scheduled..." found in the NERC document Draft Reliability Standard Compliance Guidance for VAR-001 and VAR-002 dated July 8, 2013.Is it the ad hoc group's intent to have a schedule for all reactive resources including capacitors, reactors, Static var Compensators and generators? Is the schedule meant to be similar to that of a generator (i.e. Insert capacitors at 1.0pu and remove at 1.05) or on a time base? Is schedule just supposed to take into account availability of all reactive resources?Also TSGT believes the statement "(at either the high or low side of the Generator Step-Up transformer at the TOP's discretion)" currently in VAR-001-4 R4 to should be changed to "(at an agreed upon metering point to which the GOP has direct access)." For VAR-001-4 R6 why did the ad hoc group not change the consultation requirement from GO to GOP? Tri-State believes that this information would better serve the GOP function particularly at Co-Owned facilities. This change would not have a negative effect on the reliability of the BES would reduce duplicative notification to be administered by the TOP.

Organization	Yes or No	Question 2 Comment
Response: For Requirement R2, the word schedule is used to reflect that equipment is available or on-line to provide voltage support. Compliance will review Tri-State's concerns regarding the RSAW. The VAR SDT did not agree on adding language that adds a mutually agreed upon metering point. Further, the GO is in R6 because that is the entity that would assume a loss when the unit is taken offline.		
Texas Reliability Entity		(1) Under the currently enforceable TOP standards, there is a requirement to operate within SOLs and IROLs (in TOP-004-2 R1). However, in the proposed TOP standards currently filed at FERC for approval, the wording of this requirement changed. In TOP-001-2 R8 thru R9, the TOP only has to operate within SOLs that "deserved increased attention" according to the rationale stated in the proposed Standard. What effect does that change have on these VAR requirements, and the stated rationales?(2) If it is the SDT's intent for R2 and R3 that the TOP operate within voltage SOLs, then we suggest rewording R3 to remove "as necessary" to say "within System Operating Limits" or "under normal and Contingency conditions" to match R2.(3) The VSL language for VAR-001-4 R2 and R3 does not match the wording in the requirements. If the intent is to require operation within SOLs and IROLs as suggested by the VSLs, then the requirements should expressly say so. If it is not, then the VSLs should be revised to match the requirements.(4) For VAR-001-4 R1 and R5, should there be a process to provide feedback to the TOP on the voltage schedule? For example, if the TOP sets the voltage schedule in a manner that requires the generator to be at or near a reactive limit for the unit, then the unit may not be able to provide the necessary reactive support under a contingency situation.
Response: Thank you for your comments. FERC recently remanded the TOP standards for further consideration. The "as necessary" phrase is needed to show a definitive action is not always required. The VSLs have been modified. The standard does not add a feedback mechanism on voltage schedules, but the GOPs and TOPs should be communicating as necessary for voltage coordination. However, VAR-001 does provide a vehicle for providing the criteria for studies.		
Idaho Power Company	Yes	

Organization	Yes or No	Question 2 Comment
Ingleside Cogeneration LP	Yes	
Luminant Generation	Yes	
PPL NERC Registered Affiliates	Yes	
Dominion	Yes	
Arizona Public Service Company	Yes	
Salt River Project	Yes	
DTE Electric Co.	Yes	

3. VAR-002 was modified to remove several compliance issues, and in order to address burdensome notification requirements, the VAR-001 standard has been modified to allow each TOP to tailor notification requirements based on system/area needs. Do you agree with these revisions?

Organization	Question 3 Comment
Southern Company: Southern Company Services, Inc.; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing	Adding "testing" to VAR-002 R1 was a good move. This will serve to avoid nuisance notifications for routine testing.Modifying VAR-002 R2 to allow the TOP to specify notification instructions is a good move. Each TOP will be able to specify notifications appropriate for characteristics of their transmission system. Removing the VAR-002 R3 notification of duration was a good move - the GO often does not know how long it will be out until some troubleshooting is performed. Splitting the old R3 into new R3 and new R4 was a good move. This separates two distinct types of trouble. The addition of "after becoming aware of a change in reactive capability" to the new R4 was a good move - this change is not always immediately evident. M4 should be modified to match R4 - "after becoming aware of a change needs to appear in M4".
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
PPL NERC Registered Affiliates	An additional change should be made - R3 should state that when real-time status is provided to the TOP electronically there is no need for additional notification.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
ACES Standards Collaborators	(1) Consistent with our comment number 9 in question 2, VAR-002-3 R2 and Part 2.1 need to be modified so that the GOP is only required to follow the voltage schedule if provided by the TOP. It is not desirable for the TOP to provide all generators voltage schedules. As an example, the TOP may determine it does not need to provide a voltage schedule to a small generator. To consider this situation, the clause “if a

Organization	Question 3 Comment
	voltage schedule is provided by the TOP" could be added to both Part 2.1 and the main requirement. (2) VAR-002-3 R5 meets multiple P81 criteria and should be removed. It meets Criterion A (overarching) because it does little, if anything, to benefit or protect the reliable operation of the BES and meets B2 - Data Collection/Data Retention and B4 - Reporting because it requires the GOP to gather their tap setting information and report it to a third party (i.e. its TOP) which is unnecessary to implement as a reliability requirements. A GOP is not going to refuse to provide data to its TOP on its generator step up transformer in a compliance driven world. In fact, making this data subject to compliance slows the free exchange of the information because of all the extra checking that goes into managing (i.e. verifying, checking, storing) compliance documentation. This requirement also meets B7 - Redundant because the TOP can specify this data in its data specification per TOP-003-2 R1, distribute to the GO per TOP-003-2 R3 and then GO would have to respond per TOP-003-2 R5. (3) VAR-002-3 Part 6.1 meets a P81 criterion and should be struck. It meets Criterion A (overarching) because it does little, if anything, to benefit or protect the reliable operation of the BES and meets B4 - Reporting because it requires the GO to report a technical justification for not implementing tap changes. This technical justification simply does not support reliability. The TOP can make adjustments to other voltage schedules to account for the GO's inability to implement the tap changes. What is the purpose of the GO providing the TOP a technical justification? Is it to provide the TOP some assurance there is a technical reason for failing to implement the tap changes? In a compliance driven world, the TOP can reasonably expect the GOP to implement the tap changes unless the changes would violate safety, equipment limits, regulatory or statutory requirements since these only the only deviations allowed by the main requirement. The threat of sanctions assures this. Furthermore, the GOP may legitimately not have a "technical" justification because a regulatory requirement is a legal justification not a technical justification. (4) The RSAW for VAR-002-3 indicates that compliance assessment for R4 could be vague and result in inconsistent outcomes. The RSAW indicates that the auditor will look for evidence when the GOP became aware of changes. If the entity's

Organization	Question 3 Comment
	data historian or another piece of evidence indicates a reactive capability change occurred at a certain time, does this mean that the entity is aware? We think the answer is no. The entity is only aware when its personnel become aware and not when a measurement first records that something is askew. Furthermore, we believe personnel should be limited to the plant operators in the control room who have overall responsibility. Any evidence review for when the entity became aware should be limited to plant operator logs because this evidence will most closely demonstrate what the plant operator knew based on information provided and will not be as likely to be second-guessed on what the plant operator should have known.(5) VAR-002-3 R2 will be problematic for some GOPs because it does not reflect the characteristics of the voltage schedule provided by some TOPs. For example, some TOPs provide an hourly average voltage schedule to avoid the need for notification for every time the GOP drifts out of schedule. How would R2 be applicable in this situation? Would it only apply for the first 15 minutes of each hour looking back at the last hour? Please modify the requirement accordingly to address this issue.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Texas Reliability Entity	(1) The status and capability notifications in R3 and R4 may be directly or indirectly in conflict with TOP-005-2a Attachment 1, Item 1.2.4, IRO-005-3.1a R1.1 and R12, IRO-002-2 R5, IRO-003-2 R2, TOP-006-2 R1 and R2, TOP-008-1 R4 and possibly future TOP-003-2 R1. Will the TOP and RC be able to satisfy their obligations under these other standards in view of the proposed GOP reporting parameters?(2) In VAR-002-3 R4, does the “reactive capability” include static capacitive or reactive devices that are behind the fence (for example, static capacitors and reactors installed on the low voltage feeders at wind plants to meet power factor requirements). Would this requirement apply to such devices if they are not included in the Bulk Electric System per the new BES definition?
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the	

Organization	Question 3 Comment
entire standard before posting it for another 45-day comment/ballot.	
ReliabilityFirst	1. General Comment - ReliabilityFirst believes that due to the interdependency of the VAR-001-4 and VAR-002-3 standards, the SDT should consider combining the two into a single standard. It would be a natural progression to list a requirement associated with the Transmission Operator having it immediately followed by the associated Generator Owner/Operator requirement. ReliabilityFirst believes the Generator Owner/Operator would benefit from knowing what is being required of the associated Transmission Operator. Specific VAR-002-3 Comments1. Requirement R6 - The parent Requirement R6 is applicable to the Generator Owner while the sub-part 6.1 specifies the Generator Operator. The same applicable entity listed in the "parent" requirement should be the same as any associated sub-parts. Since only Requirements are enforceable in Reliability Standards, if the Generator Operator fails to notify the Transmission Operator and fails to provide the technical justification per sub-part 6.1, a Possible Violation would be rolled up to Requirement R6. This would not work since Requirement R6 is only applicable to the Generator Owner. ReliabilityFirst completely understands that the Generator Owner is the responsible entity for ensuring that transformer tap positions are changed and that the Generator Operator is the entity responsible for actually performing the change. ReliabilityFirst recommends splitting Requirement R6 and sub-part 6.1 into two separate requirements (i.e., create a new Requirement R7 using the language of sub-part 6.1).
Response: Thank you for your comments. Based on the independent expert report, the VAR standards may eventually be combined in a single family of standards, along with the TOP and IRO standards. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Public Service Enterprise Group	1. In R1, a generator that is exempt from having to meet a voltage or Reactive Power schedule is exempt from R1. However, a generator that must meet a Reactive Power schedule should also be exempted from R1 because R1only applies to AVRs in the voltage control mode. R1 should be rewritten as follows:R1. The Generator Operator

Organization	Question 3 Comment
	shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless the Generator Operator 1) is exempted by the Transmission Operator, or 2) has been directed by its Transmission Operator to meet a Reactive Power schedule, or 3) has notified the Transmission Operator of one of the following:2. We suggest R2 have “or Reactive Power” inserted in the following phrase: “...for otherwise shall meet the conditions of notifications for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator.” 3. R2, part 2.3 should be moved to M3 since it addresses measures to prove compliance with R2. We suggest the second sentence in M2 be modified as follows: “The Generator Operator shall have evidence to show that the its generator(s) maintained the voltage or Reactive Power schedule provided by the Transmission Operator (either at the location specified by the Transmission Operator or at an alternate location that includes a methodology for converting the schedule from Transmission Operator’s location to the alternate location), or shall have evidence of meeting the conditions of notification for deviations from the voltage schedule provided by the Transmission Operator."
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Manitoba Hydro	Although Manitoba Hydro is in general agreement with the standards, we have the following comments:(1) M1 - the language in the measure is that evidence ‘must’ include which is a shift from typical language that evidence ‘may’ include. It also seems to be a shift from what is discussed in the rationale that the measure has been updated to include some of the evidence that ‘can be used’ for compliance purposes as the evidence listed is made mandatory by the ‘must’. (2) R1 - footnote 2 and 4 seems to be missing(3) M2 - refers to ‘unit’ while rest of standard refers to generator. For part 2.3, I believe the reference to ‘units’ should be to ‘Generator Operators’. (4) M3 -the acronym GOP is used while every other reference in the standard is to Generator Operator. (5) M4 - the language between the measure and the

Organization	Question 3 Comment
	requirement differs slightly. The measure requires evidence of notification within 30 minutes of 'the recognition' of a change, while the requirement requires notification within 30 minutes of 'becoming aware' of a change. (6) M5 - there is nothing in the measure that addresses the timeline upon which the Generator Owner is required to provide information. (7) R6/M6 - the requirement and measure refers to both Generator Owner and Generator Operator. Its not clear whether this is intentional or inadvertent. The words 'and provided technical justification' should be added to the end of M6 after 'tap specifications'. (8) Compliance, 1.2 - there is no time limit on the requirement for a Generator Owner to keep documentation on its step up and auxillary transformers. Its it meant to be for as long as that version is current?(9) Compliance, Compliance Monitoring, 1.3 - The language refers specifically to processes found in the NERC Rules of Procedure. Generally in draft standards, there is just a list of processes that may be used. The reference included in this draft standard is concerning because MB Hydro has their own Compliance and Monitoring program and has only adopted select aspects of the NERC Rules of Procedure.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Exelon Companies	Exelon appreciates changes made to the standard the current revision is a significant improvement on the previous draft version. As mentioned above, we support VAR-001-4 as written but feel important issues remain unaddressed with VAR-002-3 and will therefore vote Negative. Our principal concerns include: VAR-002-3 Effective Dates. The Implementation Plan for VAR-001-4 and VAR-002-3 requires the new Standard revisions to be implemented the first day of the first calendar quarter after applicable regulatory approval. Although the Implementation Plan justification states that the VAR-002 standard "cannot go into effect without the new TOP schedules and notification requirements" it does not address the implementation associated with changes to VAR-002 with respect to status notifications. This is not sufficient time to allow generating units to implement training of operators and procedural changes necessary to implement the proposed changes to notification requirements

Organization	Question 3 Comment
	associated with the AVR, PSS or alternative voltage controlling device. We suggest at least a 6 month implementation period following regulatory approval. VAR-002 R1 or in the applicability section of the standard.This standard or requirement does not account for dispersed Generation (such as wind or solar as found in the new BES definition). These generators may not have traditional AVR, may only provide limited Reactive resources and the individual elements may not have AVR or be capable of operating in Voltage control mode. VAR-002-3 R2.3Exelon believes it is reasonable to allow the GOP to monitor the voltage at the location specified in their TOP issued voltage schedule by allowing the GOP to monitor at a different location by applying a methodology for converting the voltage monitored; however, the conversion method should be communicated and agreed to by the Transmission Operator. There is not a one for one conversion between grid voltage and terminal voltage and both parties should agree on the conversion method and monitoring point to avoid any future audit or implementation issues.VAR-002-3 R3Exelon agrees with the fifteen (15) minutes to allow a GOP time to resolve an issue before having to notify the TOP of a status or capability change; however, postponing the notification by 15 minutes to alleviate short term / nuisance notifications has the effect, as written, of shortening the notification window to 15 minutes. Fifteen minutes is not a reasonable timeframe for such notifications to occur, especially in large dispersed fleet operators where the GOPs do not communicate directly to their TOP and must notify via a third party (e.g., an independent generation dispatching organization). Exelon suggests that the 30 minute notification timeframe for a status change on the AVR, PPS or alternative voltage controlling device be started following the inability to restore within 15 minutes.VAR-002-3 R4Exelon suggests that the VAR SDT provide guidance to the industry on examples of reactive capability changes that would require notification to the TOP within 30 minutes after becoming aware of a change. The only guidance provided to date is in the VAR-002 Compliance Analysis Report dated August, 2010.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the	

Organization	Question 3 Comment
entire standard before posting it for another 45-day comment/ballot.	
Florida Municipal Power Agency	FMPA appreciates these changes. However, VAR-002-3 remains duplicative of other requirements within the standardsVAR-002-3 R2, bullet 2.3 is duplicative of TOP-001-2 R1. Both require the GOP to follow the direction of the TOP. Bullet 2.3 should be deleted.VAR-002-3 R5 is duplicative of TOP-003-2 and should be deleted. VAR-002-3 R5 requires the GO to provide the TOP information about the GSU. TOP-003-2 R5 requires the GO to submit data as specified by the TOP. The TOP cannot perform their obligations of VAR-001-4 R6 to specify GSU tap positions without the data of VAR-002-3 R5; however, the TOP will ask for that data in accordance with TOP-003-2 R3. Hence, these requirements are redundant and VAR-002-3 R5 ought to be deleted.FMPA also wonders how duplication between TOP-003-2 that gives TOPs a carte blanche opportunity to develop data requests on any information they need and the notification requirements of VAR-002-3 will be managed. In other words, the TOP can develop their TOP-003-2 data specification to include the notification requirements of VAR-002-3 and as such GOPs would be subject to double jeopardy risk.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Utility System Efficiencies, Inc.	For R2, what about the situation where the generator cannot actually influence the voltage? There may be a significant amount of hours where they can't keep the voltage in range. For M2, for a generator that does not have an AVR, what type of evidence is required to show compliance for 8760 hours per year? Sounds like a lot of evidence potentially.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Tri-State Generation and	For VAR-002-3 R5 TSGT believes the TOP should consult with the GOP rather than

Organization	Question 3 Comment
Transmission Association, Inc.	the GO to better align requirement R5 with its subrequirement R5.1.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Consolidated Edison Co. of NY, Inc.	Generators may be asked by their TOP to operate in other modes. Reword Requirement R1 as follows: R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless the Generator Operator 1) is exempted by the Transmission Operator, [delete: or] 2) is notified by the Transmission Operator to operate in a different viable operating mode (e.g., constant VAR output mode), or 3) has notified the Transmission Operator of one of the following:
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Consumers Energyu	It is important to clarify the statement of "notification requirements." In the context of VAR-002 this term refers to the notification from the GOP to the TOP on status of the AVR, Ability to follow the voltage schedule or the status of the unit.We would suggest the timing on VAR-002 R3 be similar to R4 in that the clock starts at the awareness of the GOP of a status change.VAR-001 clearly defines a Voltage or Reactive Power schedule. We suggest this be done in VAR-002 for consistency rather than the footnotes provided.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Luminant Generation	Luminant appreciates the work of the SDT and agrees that most of the revisions are appropriate, and that the intent of the SDT to allow for more than one method of voltage support is correct. However, as written, VAR-002, R2, does not clearly

Organization	Question 3 Comment
	identify that generators can provide voltage support by a method other than maintaining a voltage schedule, continuously monitoring voltage and reporting deviations from the voltage schedule. In some areas of the country, the TOP monitors the voltage at all busses in it area, including the busses connecting generators, and directs generators to modify reactive output as the TOP requests. Luminant believes the language of VAR-002, R2 should be modified to provide clarity as follows:R2. Unless exempted by the Transmission Operator, each Generator Operator shall provide generator voltage support or Reactive Power support (within each generating Facility's capabilities4) as follows: [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] 2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to provide voltage or Reactive Power support directed by the Transmission Operator. 2.2. When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the request cannot be met. 2.3. When directed by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule3 (within each generating Facility's capabilities4) provided by the Transmission Operator, and shall meet the conditions of notification for deviations from the voltage schedule provided by the Transmission Operator. 2..3.1 Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator. With this proposed language, the GOP would have to maintain a voltage schedule and report deviations only if that is the normal method of voltage support requested by the TOP. 2.3 and 2.3.1 would only apply to a GOP that maintains a voltage schedule. The measures for 2.1 and 2.2 would include operator logs, voice recordings, etc.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	

Organization	Question 3 Comment
Duke Energy	No. Duke Energy does not agree with the revisions made.Duke Energy is unclear whether the exemptions referenced in R1 and R2 in VAR-002-3 are the same as the exemptions created in VAR-001-4 R4. We believe using the word "exempted" in multiple requirements without identifying the origin of the exemption is a cause of confusion. Requirement 2 - Revise R2.1 to read," When a generator's AVR is out of service, the generator does not have an AVR, or is not in a TOP approved mode of AVR operation as specified in R1, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator. "The VRF/VSL for Requirement 2 would need to be modified if this change is made.Requirement 3 - Duke Energy is unclear as to what is considered an alternative voltage controlling device. Duke Energy prefers the language in the previous draft of this standard which states, "Each Generator Operator shall notify its associated Transmission Operator of a status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability within 30 minutes of the change. If the status has been restored within the first 15 minutes of such change, then there is no need to call the TOP. "The language in the previous draft provides more clarity on what would prompt notification from a GOP to a TOP based on status or capability change.Requirement 5 - Duke Energy would like the SDT to review and verify that the Transmission Planner, and not the Planning Authority or Planning Coordinator, is the correct functional entity for this requirement. Lastly, Duke Energy would like to clarify that we encouraged our ballot body members to vote "Negative" on this ballot for reasons stipulated above. However, one of our ballot body members mistakenly voted "Affirmative" which was in error. Our decision to vote "Negative" on this ballot was unanimous among all those involved. We apologize for any confusion this may have caused.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	

Organization	Question 3 Comment
Kansas City Power & Light	NO. R2 is the part of VAR-002 that I disagree with because the Transmission System Operator is monitoring the system voltage and notifies each generating facility when they need to raise/lower voltage in that particular area of the system. If the voltage at the generating facility is high/low the TSO has received an alarm and will be notifying the plants control operator to correct the voltage and there already is a requirement for the control operators to comply with the TSO request.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Portland General Electric Co	PGE appreciates NERC's efforts to revise VAR-002. The standard as whole is a significant improvement from the previous version. However, R3 still requires a 30 minute notification for notifying the transmission operator (TOP). The 30 minute limit is a challenge for generator operations to meet. The SDT should consider increasing this limit to 60 minutes. In addition, the requirement should allow registered entities to set up an alternative method to provide real-time AVR/PSS/voltage control device telemetry. This method would eliminate a need for notifying the transmission operator within 30 minutes. Also, the NERC glossary should fully define the term, 'voltage controlling device', as stated in R3.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
American Electric Power	R5: Rather than allowing only 30 days, we instead recommend that the Generator Owner be allowed to provide the data within the timeframe agreed upon by the GO and either the Transmission Operator or Transmission Planner. This data is often part of larger data submission that may stretch beyond the proposed time horizon. In addition, providing this data to the TP appears to be duplicative of the MOD standards currently being updated. As a result, we recommend removing the TP from this requirement.R6: We recommend that Requirement 6 and its subrequirement be applicable only to the Generator Owner and not split between the Generator Owner

Organization	Question 3 Comment
	and Generator Operator. If both are to be retained, we recommend that the subrequirement be changed to state "*If* the Generator Owner cannot provide tap setting changes as requested, the Generator Owner or Generator Operator should notify the Transmission Operator..."
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Bureau of Reclamation	Reclamation believes that the notification requirements in R2 and R3 should provide the continent-wide standard. Reclamation suggests that the bullet points in R1 should be relabeled as sub-requirements R1.1 and R1.2.Reclamation requests that the drafting team clarify the timeframe for notifications required by R1. Reclamation suggests that the drafting team update VAR-002-3 R2 to allow Generator Operators to notify Transmission Operators that a voltage schedule cannot be met for equipment or other reasons, so that the Transmission Operator can alter the voltage schedule accordingly. R2.2 recognizes that a Generator Operator can provide an explanation that a voltage schedule cannot be met "when directed to modify voltage" but does not address the planning horizon. Reclamation appreciates that R2 recognizes that generators only need to comply with voltage schedules within facility capabilities, and that footnote 6 recognizes that generating facility capability may not be sufficient at times to pull the system voltage within scheduled tolerance bands. Nevertheless, Reclamation believes that R2 subrequirements should more clearly articulate that (1) Generator Operators should provide Transmission Operators with feedback that they cannot meet voltage schedules in the planning horizon, and (2) generators may not always be capable of modifying system voltage.Reclamation notes that R2.3 applies to real-time operations, and suggests that R2.3 should be updated to require Generator Operators and Transmission Operators to monitor voltage at mutually-agreed upon locations to avoid confusion in real-time communications. Reclamation suggests that the drafting team update VAR-002-3 R3 to specify that the "Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative

Organization	Question 3 Comment
	voltage controlling device within 30 minutes of becoming aware of the change." Reclamation also suggests that M3 should be updated to specify that the GOP must notify its associated Transmission Operator "within 30 minutes of becoming aware of the change" rather than "within 30 minutes of when the change first occurred." Reclamation notes that VAR-002-3 R4 specifies that the "Generator Operator shall notify its associated Transmission Operator within 30 minutes after becoming aware of a change in reactive capability... ." Reclamation suggests that M4 should be updated to match this language and specify that the GOP must notify its associated Transmission Operator "within 30 minutes of becoming aware of the change" rather than "within 30 minutes of when the change first occurred." Reclamation requests clarification on types of "changes in reactive capability" that could trigger the notification requirement in R4. Reclamation notes that the time horizon for VAR-002-3 R6 should probably be changed from "Real-Time Operations" to "Operations Planning" to match VAR-001-4 R6 and reflect that tap setting changes are agreed upon in advance rather than in real-time. Reclamation suggests that VAR-002-3 R6 should be updated to match VAR-001-4 R6 and to specify that the Transmission Operator must coordinate outages to accommodate required step-up transformer tap changes. Reclamation suggests the drafting team update the requirement to read "After consultation with the Generator Owner regarding necessary step-up transformer tap changes, associated outages, and the implementation schedule...".
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Northeast Power Coordinating Council	Suggest the following changes to more effectively convey the intents of Measure M3 and Requirement R6.Suggest that Measure M3 be reworded to require demonstration of compliance rather than to require actions which should have been stipulated in the requirement. Specifically, we proposed the last part in Measure M3 be revised to:"...therefore, if a status change lasts more than 15 minutes, the GOP shall provide evidence such as system log, electronic message or a transmittal letter that it notified its associated Transmission Operator within 30 minutes of when the

Organization	Question 3 Comment
	change first occurred."Regarding R6, the wording "the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator..." is not a direct action and may not be measurable. Suggest revising it to read:"the Generator Owner shall implement the transformer tap positions according to the specifications provided by the Transmission Operator...."We further propose that the SDT insert the evidence language into the first sentence of Measure M3 which asks for evidence that the Generator notified its associated Transmission Operator within 30 minutes of the change identified in Requirement R3.Generators may be asked by their TOP to operate in other modes. Reword Requirement R1 as follows: R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) unless the Generator Operator 1) is exempted by the Transmission Operator, 2) is notified by the Transmission Operator to operate in a different viable operating mode (e.g., constant VAR output mode), or 3) has notified the Transmission Operator of one of the following:... The comments in Question 2 regarding Hydro-Quebec regarding the word "schedule" apply.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
PacifiCorp	The following change to requirement R4 is recommended: "Reactive capability changes due to change in the wind speed for wind generators or a change in the solar resource for solar facilities do not require Transmission Operator notification." Given the variable nature of wind, the reliance of weather forecasting does not rest explicitly with the GOP. The TOP has access to weather forecasting that would make the need of notification by the GOP unnecessary.Additionally, PacifiCorp supports the following comments from MidAmerican:We support the deletion of the language regarding notification of the expected duration of a change in status. At the time a status change occurs it is often difficult to provide a meaningful estimate of the duration of the change. Requirement 3 should be revised to state - Notification must

Organization	Question 3 Comment
	be made within 30 minutes of becoming aware of the change from automatic controlling voltage for the AVR, and from in-service of the PSS. Measure 3 should be revised to reflect this as well.The revised VAR-002 R2.1 removes the 15 minute deviation criteria for notification by Generator Operators to Transmission Operators. The revised VAR-001-4 requires Transmission Operators to provide notification requirements. The drafting team in the consideration of comments explained "In an effort to remove prescriptive notification requirements for the entire continent" the change was made. This leaves the Generator Operators at the mercy of Transmission Operators who could potentially set a no deviation criteria. It is recommended that a comprise be struck by specifying a limit on the criteria such as "no less than 15 minutes".
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
MRO NSRF	The revised VAR-002 R2.1 removes the 15 minute deviation criteria for notification by Generator Operators to Transmission Operators. The revised VAR-001-4 requires Transmission Operators to provide notification requirements. The drafting team in the consideration of comments explained "In an effort to remove prescriptive notification requirements for the entire continent" the change was made. This leaves the Generator Operators at the mercy of Transmission Operators who could potentially set a no deviation criteria. It is recommended that a compromise be struck by specifying a limit on the criteria such as "no less than 15 minutes".For clarification it is recommended that the word "generator" be added before the word "stability" in the last sentence of footnote 6. [Note to NSRF: a comment on this was submitted previously but it did not have a recommended language change]In M2 it is recommended that "alarm logs" be added to the list of evidence. We support the deletion of the language regarding notification of the expected duration of a change in status. At the time a status change occurs it is often difficult to provide a meaningful estimate of the duration of the change. Requirement 3 should be revised to state - Notification must be made within 30 minutes of becoming aware of the

Organization	Question 3 Comment
	change from automatic controlling voltage for the AVR, and from in-service of the PSS. Measure 3 should be revised to reflect this as well.The following change to requirement R4 is recommended: "Reactive capability changes due to factors such as a change in the wind speed for wind generators or a change in the solar resource for solar facilities do not require Transmission Operator notification"Measure 4 should be revised to reflect the wording in Requirement 4 - Notification must be made within 30 minutes of becoming aware of the change of state of the AVR.For the same reason described above for VAR-001 (NERC IGVT Report), R1 should be modified as follows:"R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) or plant-level volt/var regulator in service and controlling voltage) unless the Generator Operator 1) is exempted by the Transmission Operator, or 2) has notified the Transmission Operator of one of the following:" A similar addition should be made where the AVR is referred to in the other requirements of VAR-002.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Independent Electricity System Operator	We agree with most of the proposed changes, but would suggest the following changes to more effective convey the intent of Requirement R3 and Measure M3.a. R3: The wording "the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator" is not a direct action and may not be measurable. We suggest to revise it to read:"the Generator Owner shall implement the transformer tap positions according to the specifications provided by the Transmission Operator...."b. M3: We suggest it be reworded to require demonstration of compliance rather than to require actions which should have been stipulated in the requirement. Specifically, we proposed the last part in Measure M3 be revised to:"...therefore, if a status change lasts more than 15 minutes, the GOP shall provide evidence such as system log, electronic message or a transmittal letter that it notified its associated Transmission Operator within 30

Organization	Question 3 Comment
	minutes of when the change first occurred."We further propose that the SDT insert the evidence language into the first sentence of Measure M3 which asks for evidence that the Generator notified its associated Transmission Operator within 30 minutes of the change identified in Requirement R3.We assess the changes proposed under Q2 and Q 3, above, are not substantive and do not materially change the intent or content of the standards. Therefore, if the standards receives 2/3 majority approval at the ballot, these changes can be implemented and posted for recirculating ballot without having to post and ballot the standards for a successive ballot.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
ISO/RTO Standards Review Committee	We assess the changes proposed under Q2 and Q 3, above, are not substantive and do not materially change the intent or content of the standards. Therefore, if the standards receives 2/3 majority approval at the ballot, these changes can be implemented and posted for recirculating ballot without having to post and ballot the standards for a successive ballot.We agree with most of the proposed changes, but would suggest the following changes to more effective convey the intent of Requirement R3 and Measure M3.a. R3: The wording "the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator" is not a direct action and may not be measurable. We suggest to revise it to read:"the Generator Owner shall implement the transformer tap positions according to the specifications provided by the Transmission Operator...."b. M3: We suggest it be reworded to require demonstration of compliance rather than to require actions which should have been stipulated in the requirement. Specifically, we proposed the last part in Measure M3 be revised to:"...therefore, if a status change lasts more than 15 minutes, the GOP shall provide evidence such as system log, electronic message or a transmittal letter that it notified its associated Transmission Operator within 30 minutes of when the change first occurred."We further propose that the SDT insert the evidence language into the first sentence of Measure M3 which asks for evidence that the Generator

Organization	Question 3 Comment
	notified its associated Transmission Operator within 30 minutes of the change identified in Requirement R3.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Ameren	We request that the SDT support adding to R3 the "...after becoming aware of..." language now proposed for R4. This will help reduce the number of unnecessary GOP notifications to the TOP.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Arizona Public Service Company	Yes
Salt River Project	Yes
Tennessee Valley Authority	Yes
The United Illuminating Company	Yes
CenterPoint Energy, Houston Electric LLC.	Yes, CenterPoint Energy agrees with these revisions to VAR-002 removing compliance issues that address burdensome notification requirements, allowing the Transmission Operator, through VAR-001 to tailor notification requirements based on system/area needs.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	

Organization	Question 3 Comment
Idaho Power Company	Yes, exempting the intermittent outages of AVR's and only requiring notification for extended interruptions is an improvement and lessens the documentation necessary to show compliance.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Ingleside Cogeneration LP	Yes,Ingleside Cogeneration agrees that there must be reasonable notification criteria controlled by TOPs that allows them to specify when notification of change in AVR or reactive resource status is necessary. In many cases, the status is telemetered in real-time, but a call is required anyways to specify the expected duration of the status change. This is overcommunication in most cases, and only serves to tie up resources at the GOP and TOP.The same is true of notifications when the GOP cannot maintain the voltage at the interconnection point. Many GOPs do not control interconnection voltage and could actually resist an adjustment that the TOP is trying to make in response to system conditions. Again, some reasonable notification criteria could stop a lot of nuisance calls under these circumstances.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
City of Austin dba Austin Energy	Yes.
PJM Interconnection	Yes.
EDP Renewables North America LLC	Yes. EDPR NA believes it is important for TOPs to have the flexibility to tailor its requirements, as long as there is sufficient coordination among affected entities. We also offer the following comment:VAR-002 R1: We support the concept that a GOP need not notify its TOP that its AVR is out of service if it has previously advised its TOP that it will not have its AVR in service during start-up and shut-down. We

Organization	Question 3 Comment
	recommend that similar provision be made for variable energy resources which are not able to provide voltage support when operating in similar circumstances. Wind farms, for example, generally have equipment limitations that can affect their ability to follow voltage schedules when operating at low levels. Wind farms will not telemeter a different status in that circumstance, however. We propose that, if a variable energy resource has notified its TOP of equipment limitations that affect its ability to follow a voltage schedule until it achieves a certain level of production, also not be required to notify the TOP that its AVR is out of service.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Bonneville Power Administration	Yes. Comments: BPA requests further clarification of VAR-002-3 R3 and M3, to be revised such that a status or capability change in generator Reactive Power should be reported within 30 minutes from an entity becoming aware of the change in condition, rather than the current form, which is 30 minutes from the change in condition.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
SPP Standards Review Group	Yes. We also offer the following comments on the two standards.Generic Comments on VAR-001-4We recommend changing 'real time' in the Purpose to 'Real-time' as defined in the NERC Glossary of Terms.We suggest rewording R1.1 to the following: 'Each Transmission Operator shall provide a copy of the voltage schedules as specified in R1 to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of such a request.' Although we have proposed deleting R2, if the drafting team decides to keep it, we recommend deleting the last sentence in R2. It is really an example and doesn't contribute substantially to the requirement.We also recommended deleting R3 but if the drafting team decides to keep it, we suggest adding 'to operate within SOLs and IROLs' following 'as necessary' at the end of the

Organization	Question 3 Comment
	requirement.The use of the term 'direct' in R3 and R5.1 lead to implications of issuing directives. To get away from this situation, we suggest substituting 'instruct' for 'direct'. This change will also need to be reflected in the Measures and the VSLs.Since R4 contains an exemption for R5, we suggest reordering requirements R4 and R5 such that R5 becomes R4 and R4 becomes R5. That way the exemption follows the requirement.We suggest the drafting team delete the phrase '...at the Transmission Operator's discretion.' at the end of R5. We suggest changing 'associated' to 'applicable' in and deleting the redundant phrase at the end of R5.1. The requirement would then read: 'The Transmission Operator shall provide the voltage or Reactive Power schedule to the applicable Generator Operator.' The Measure will also need to be revised to correspond with the revised requirement.We recommend adding 'for that criteria' following 'request' at the end of R5.3.We recommend changing the Time Horizon in R6 to Long-Term Planning since the Transmission Planner is typically the entity that will determine when a tap change is necessary and will notify the Transmission Operator that it needs to be done.In the Rationale Box for R6 there is a reference to VAR capability and tap setting. We suggest rewording that sentence to the following: 'If the tap setting is not properly set, then the VARs available from that unit can be affected.'The Severe VSL for R3 contains 'real-time'. It needs to be 'Real-time'.Generic Comments on VAR-002-3The use of the term 'direct' in R2.2 lead to implications of issuing directives. To get away from this situation, we suggest substituting 'instruct' for 'direct'. This change would need to be reflected in the Measure 2.1 and 2.2 and the VSL also.We suggest changing the notification timing requirements in R3 to the Generator Operator must notify the Transmission Operator within 30 minutes of the change of AVR status unless the AVR has been restored to service.In the second sentence in the Rationale Box for R3, use 'provide' instead of 'provided.'In the Rationale Boxes for R5 and R6 there is a reference to VAR capability and tap setting. We suggest rewording that sentence to the following: 'If the tap setting is not properly set, then the VARs available from that unit can be affected.'
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire	

Organization	Question 3 Comment
standard before posting it for another 45-day comment/ballot.	
Xcel Energy	Yes. Xcel Energy appreciates the hard work of the Standard Drafting Team. We recognize that significant effort has been put into the modifications of the VAR-001 and VAR-002 standards and we applaud the direction the team is moving. We are voting Negative on VAR-002 for one reason which we explain below.Xcel Energy understands that the existing language in the VAR-002 standard uses the term "status change" but believe that this term is not well defined and is subject to different interpretations. AVRs and PSSs are designed to cycle based on the parameters being monitored by the devices. This as-designed cycling may be interpreted as a status change. We note here that the drafting team does not use the term status change in its rationale statement. Instead, the rationale statement is much clearer in meaning than the proposed requirement language. To address Xcel Energy's concern, we request that the drafting team replace the first sentence in Requirement R3 with the following sentence. (We believe that this change does not constitute a significant modification but is instead providing more clarity in the requirement language based on the wording of the Rationale for Requirement R3.)"Each Generator Operator shall notify its associated Transmission Operator when the AVR, power system stabilizer, or alternative voltage controlling device goes out of service within 30 minutes of the change."
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Electric Reliability Council of Texas, Inc.	Yes.ERCOT supports the revisions but recommends that the SDT consider the following additional issues:A. Consider revising R2 as follows: "The generator shall follow the voltage schedule assigned by its TOP." Otherwise this is effectively a "fill in the blank" standard.As drafted, R2 also establishes "how" entities are required to meet their obligations. The standards should establish what is required and leave it to the discretion of the functional entity to determine how to meet the relevant objective. R3 provides the needed notification.B. VAR-002 R2 requires GOs to notify

Organization	Question 3 Comment
	TOPs of voltage. This seems to create an unnecessary requirement given that TOPs are obligated to monitor system voltage.C. VAR-002 R2.1 appears to require that GOs maintain the voltage assigned. Consistent with the general principle that the standards should establish what is required, how GOs maintain voltage assignments should be within the discretion of the entity.D. VAR-002 R2.2 is redundant. If GOs have to maintain the voltage assigned, this is unnecessary.E. VAR-002 R2.3 is redundant if a GO has to maintain the voltage assigned.F. VAR-002 M2 includes a statement that has a "will" in it. This effectively establishes a requirement. Measures are means of demonstrating compliance, they are not requirements. The measure should be revised accordingly.G. VAR-002 R3 should state that the notification is not required during startup or shutdown. A TOP can determine from telemetered information when a unit is operating below their lower stability limit. Requiring reporting of AVR/PSS status coming on/going off line is not necessary and creates unnecessary distractions that could undermine reliability.H. The 2nd sentence of R3 is redundant with the 1st. If notification is required within 30 minutes it is implicit that the entity does not have to notify within 15 minutes? I. If a GO maintains the assigned voltage, the status of a GO's AVR is irrelevant. If a GO failed to maintain the assigned voltage they are in violation of R2 regardless of the reason. M3 seems to unnecessarily create the potential for double violation issue on a reporting obligation.J. The standard should make clear that telemetry on status of AVRs and PSSs to TOPs meets this notification obligation. The term 'notify' seems to imply a manual written or verbal communication.K. VAR-002 R4 second sentence dealing with 15 min language- - please refer to R3/M3 comments.L. VAR-002 R5 - This requirement is unnecessary if GOs have to respond to any reasonable data request from their TOP.M. VAR-002 R6 is redundant with R2. If a GO has to maintain assigned voltage, and adjusting taps is necessary to do that, then this instructional requirement is not needed. If R6 is kept, in VAR-002-3 Standard the entity changes in R6.1. VAR-001-4 states the TOP will work with the GO in R6. Then in VAR-002-3 it states the following:R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that

Organization	Question 3 Comment
	transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. [Violation Risk Factor: Lower] [Time Horizon: Real-time Operations] 6.1. If the Generator Operator cannot comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification. Why does it change from the GO to the GOP? The SDT should address the differences within VAR-002-3 to mirror R6 in the VAR-001-4 Standard.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Dominion	Yes.In order to be consistent, Dominion also suggests reviewing the need to use "its associated Transmission Operator" throughout the entire standard (i.e. R1 - "has notified the Transmission Operator", R2/M2 - "provided by the Transmission Operator", R6 - "specifications provided by the Transmission Operator", etc).
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
DTE Electric Co.	YesComments: Adding the 15 minute window in VAR-002 is a great improvement.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	

4. The VRFs/VSLs for VAR-002 were modified to remove arbitrary time requirements. Do you have any specific comments or questions about the new VSLs/VRFs?

Organization	Question 4 Comment
Southern Company: Southern Company Services, Inc.; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing	The removal of "up to 45 minutes for the R2 VSL was a major improvement.The comma in the second and third OR statements of the Severe VSL for VAR-002 R2 is not needed. The comma in the second OR statement of the Severe VSL for VAR-002 R6 is not needed.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Manitoba Hydro	(1) VSLs, - not clear why the references throughout the VSLs are to 'responsible entity' when the requirements are clear as to an obligation on either the Generator Owner or Generator Operator. Those entities should be listed in the VSLs as they are in the requirements and standards. (2) VSLs, R2, Severe VSL - the word 'Power' is missing after 'Reactive'. Also doesn't mention that the Generator Operator 'did not have an exemption'. (3) VSLs, R3 and R4 - would read better if stated 'the Generator Operator did not make the notification of a change that lasted more than 15 minutes within 30 minutes of the first occurrence of the change as required'.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	

Organization	Question 4 Comment
CenterPoint Energy, Houston Electric LLC.	CenterPoint Energy believes the VSLs associated with VAR-001 R2 and R3 do not consider changes in Real-Time topography such as forced outages, Resource inadequacy, or changes in weather that can drastically change the outcome of any planned or studied environment in both normal and emergency operations. A transmission operator could have scheduled sufficient reactive resources as necessary and have them available to mitigate known and identified SOLs or IROLs, but cannot schedule sufficient reactive resources for the unknown. CenterPoint energy suggests adding "identified" to the VSL language. "The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an identified SOL or IROL". CenterPoint energy believes that the High VSL for R4 is inappropriate and is indicative of a zero tolerance environment. If a Transmission Operator has an exemption criteria established, notifies the Generator Operator of such exemption, and captures evidence for compliance to prove notification 99 times out of 100, then the one instance in which the TOP notified the Generator Operator, but failed to capture evidence would warrant a High VSL possible violation.
Response: Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, the SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Xcel Energy	If the drafting team makes the requested modifications to the requirements, Xcel Energy has no concerns with either the VSLs or VRFs.
Response: Thank you for your comments.	
Utility System Efficiencies, Inc.	No
Idaho Power Company	No
Tennessee Valley Authority	No comments

Organization	Question 4 Comment
Salt River Project	No.
Bonneville Power Administration	No.
Kansas City Power & Light	No.
EDP Renewables North America LLC	No.
City of Austin dba Austin Energy	No.Because NERC has not provided an area for "Additional Comments," we are adding them here.The City of Austin dba Austin Energy (AE) commends the Standard Drafting Team's efforts related to Project 2013-04. The quality of the standard is enhanced over previous approved versions, providing additional clarity and compliance sensitivity. AE respectfully submits the following comments on VAR-001-4 and VAR-002-3 to the Standard Drafting Team (SDT):VAR-002-3, R1, Pertaining to the phrase "... unless the Generator Operator 1) is exempted by the Transmission Operator, or 2) has notified the Transmission Operator..." AE recommends the SDT clarify whether the TOP may exempt all the units represented by a GOP, or instead, specific generating facilities or a generator bus. AE suggests altering the language to read "... unless 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator..." This change will make the language in VAR-002-3 R1 consistent with the language in VAR-001-4 R4.VAR-002-3, R2.3: The requirement makes it mandatory for Generator Operators to monitor the voltage at the location specified in the voltage schedule or have a methodology for converting the scheduled voltage specified by the TOP. This may imply that the Generator Operator should make voltage corrections independent from the TOP. AE believes that maintaining the appropriate transmission level voltage is the key for sustaining system stability and that responsibility falls on the TOP. Because the TOP already monitors the transmission level voltages, the R2.3

Organization	Question 4 Comment
	requirement for GOPs to monitor voltage is redundant and may create a situation where the TOP and GOP do not agree on the monitored value (i.e. the voltage readings can be different due to step-up voltage equipment). To avoid confusion and potential compliance ambiguities, AE suggests the standard specifically state TOPs are responsible for monitoring the system voltage schedule and notifying the GOP when voltage drifts outside acceptable parameters. This appears to be a common practice of operating the grid. The GOP will be responsible for meeting the reactive support requested by the TOP. If the GOP cannot meet the reactive support requested by the TOP, the GOP should have to notify the TOP. AE suggests the following: Add "Transmission Operators" under R4 - "4.3 Transmission Operators", and alter R2.3 to: "Each Transmission Operator shall monitor the system voltage and notify its associated GOPs for additional voltage support if system voltage fails to meet the voltage schedule. If the GOP cannot meet the reactive support requested by the TOP due to equipment limitations, it shall notify the TOP of the limitations within 15 minutes.VAR-002-3, R4: AE believes the phrase "a change in reactive capability" is vague. As written, even the slightest change in reactive capability must be reported to the TOP. Is it the SDT intent the TOP be notified if a reactive capability (leading or lagging) of a generation resource changes by 1 MVAR? Detecting and reporting small reductions in reactive capability will create onerous reporting. AE recommends the following for R4: "Each Generator Operator shall notify its associated Transmission Operator within 30 minutes that a resource's reactive capability changed by 20 MVAR or 10%, whichever is greater, of the previously provided reactive capability due to factors other than a status change described in Requirement R3."
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, so the VAR SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
American Electric Power	R3 & R4 do not require communications for all instances. As a result, the severe VSL text must be qualified so that it only applies to those situations where notification is actually necessary.

Organization	Question 4 Comment
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, so the VAR SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Bureau of Reclamation	Reclamation suggests that the VSLs for VAR-002-3 R3 and R4 should reflect a range of noncompliance like in VAR-002-2. A failure to notify the Transmission Operator of an AVR, power system stabilizer, or reactive capability change for 35 minutes should not be treated the same as a failure to notify the Transmission Operator of the status change for 75 minutes.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, so the VAR SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Duke Energy	See our comments on VAR-002 Requirement 2.
Arizona Public Service Company	The VRF of "high" is not justified for any of the requirements. We would suggest a VRF of "medium" or "low". If the drafting team thinks a VRF of "high " is justified, some reasoning should be provided by the team. Lack of documented voltage schedules does not mean the system is being operated unreliably. Units are still being operated in AVR mode as required by other schedules and transmission operators coordinate the voltage schedules as needed.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, so the VAR SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
PPL NERC Registered Affiliates	Time requirements are not necessarily arbitrary, and it is in fact important to establish explicit and meaningful criteria regarding the acceptable time (and magnitude) of voltage schedule deviations. The principal reason that VAR-002 has been so troublesome in the past is that one could interpret a 10 MW hydro unit being out of the bandwidth by 0.1 kV for 1 minute as constituting a violation, despite there being no meaningful impact on BES reliability. There are moreover many occasions when a the system voltage unavoidably strays briefly outside the bandwidth due to a

Organization	Question 4 Comment
	disturbance or because there are step-changes in the TOP's voltage schedule. VAR-002-3 makes a slight movement in the right direction by stating in R2 that a unit must keep within the bandwidth or, "meet the conditions of notification," but there is nothing in VAR-001 or 002 to require TOPs to create justifiable requirements in this respect. We presently suffer under a system in which meaningless violations are spawned by abusive practices, such as establishing a bandwidth of only +/- 0.5%, and VAR-001 and 002 should be revised in a fashion that prohibits such practices.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, so the VAR SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
ACES Standards Collaborators	We do not support the VSLs for R5 because it meets P81 criteria and should be removed. We also do not support the VSLs for requirements that need modifications as identified in question 3.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, so the VAR SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
SPP Standards Review Group	We suggest the following change for the High VSL for R2. The responsible entity did not have a conversion methodology when it monitored voltage...'We recommend replacing the word 'directive' with 'specification' in the Severe VSL for R6.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, so the VAR SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	
Northeast Power Coordinating Council	We support the proposed VRFs and VSLs.
ISO/RTO Standards Review Committee	We support the proposed VRFs and VSLs.

Organization	Question 4 Comment
Independent Electricity System Operator	We support the proposed VRFs and VSLs.
Exelon Companies	We understand that R3 and R4 are binary requirements, (did or did not notify in 30 minutes), but it seems unreasonable that a complete failure to notify would have the same VSL as a notification that is one or five minutes late.
Response: Thank you for your comments. Since VAR-002 did not pass successive ballot, so the VAR SDT will revisit the entire standard before posting it for another 45-day comment/ballot.	

Additional Comments:

Seminole Electric
Bret T. Galbraith

VAR-001-4 Comments

(1) Requirement R2 states the following:

"Each Transmission Operator shall schedule '**sufficient reactive resources to regulate voltage levels'** under normal and Contingency conditions." (emphasis added)

Seminole requires clarification concerning the phrase "sufficient reactive resources to regulate voltage levels." Seminole requests additional clarity as to what it means to regulate voltage levels, e.g., does this mean to operate within SOLs? Please add clarity to the language of the Requirement, and not in guidance documents. Seminole believes adding clarity will assist auditors in determining what is "sufficient."

(2) Requirement R3 states the following:

"Each Transmission Operator shall operate or direct the Real-time operation of devices to '**regulate transmission voltage and reactive flow as necessary'**." (emphasis added)

Seminole believes that the language "as necessary" does not provide enough due process notification of what is required. Seminole would like clarification as to what is necessary, for example, "necessary to ensure sufficient voltage support to prevent …"

VAR-002-3 Comments

(1) Requirement R1. defines "start-up" as ending "when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation." The drafting also defines "shutdown" as beginning "when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline." Seminole reasons that these definitions for "start-up" and "shutdown" inaccurately describe generator start-up and shutdown in the traditional meaning of these terms. For example, operators may consider start-up to cover the generator load above the minimum sustainable load value to base load for environmental permitting regulations. It appears that the drafting team is attempting to define a unique generator operational region, and therefore, Seminole suggests that the drafting team utilize different terms than "start-up" and "shutdown" in order to prevent confusion.

However, the drafting team does not define "testing mode," and Seminole reasons that without additional guidelines, such as qualitative and quantitative factors, the misinterpretation of "testing mode" is a concern. Therefore, Seminole requests the drafting team to describe in greater detail "testing mode."

(2) Requirement R3 states the following:

"Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within **'30 minutes'** of the change. If the status has been restored within the first '**15 minutes'** of such change, then there is no need to notify the Transmission Operator." (emphasis added)

Reviewing the timeframes listed, it appears the numbers are significant to the whole number value. Therefore, if an entity has an AVR status change that lasts 15 minutes and 29 seconds, that AVR status change does not need to be reported, because proper significant digits rounding will round that value to 15 minutes and not 16 minutes. Please clarify the significant digit in these timeframes, i.e., is it 15, 15.0, 15.00, 15.0000, etc.?

Response: Thank you for your comments. The phrase "as necessary" is retained because the Transmission Operator is not expected to always operate or direct the actions of a Generator Operator. This allows the TOP to intervene as necessary to avoid system events or instances of high or low voltage. Also, since VAR-002 did not pass successive ballot, so the VAR SDT will revisit the entire standard before posting it for another 45-day comment/ballot.

Santee Cooper
Rene' Free

1. The rationale statement for R1 of VAR-001 says that it, "will allow each Transmission Operator (TOP) to establish its own policies and procedures," regarding voltage schedules and tolerance bands. This wording does nothing to prevent specifying an unreasonably-tight bandwidth (e.g. +/- 0.5%). We suggest that R1.1 end as follows, "…voltage schedules along with associated tolerance bands of not less than 1.5% of the schedule voltage unless technically justified." There may be some resistance to making the standard prescriptive, but it's not a burdensome requirement.
2. VAR-002, R5 should be revised to state; "For generator step-up and auxiliary transformers with nominal primary voltages equal to the generator terminal voltage:" This is to clarify that R4 is N/A to startup transformers and other station auxiliary transformers connected to a HV bus at a plant.

Response: Thank you for your comments. The industry could not reach a consensus on a minimum tolerance band, and some TOPs provided feedback that some tolerance bands are very narrow due to the area's voltage constraints. Also, since VAR-002 did not pass successive ballot, so the VAR SDT will revisit the entire standard before posting it for another 45-day comment/ballot.

END OF REPORT

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR and supporting package posted for comment on July 19, 2013.
2. Draft standard posted for initial comments and ballot from July 19, 2013 to September 3, 2013.
3. Draft standard posted for an additional comment and ballot from November 15, 2013 to November 26, 2013.

Description of Current Draft

This is the third posting of the proposed draft standard. This proposed draft standard will be posted for a 10-day final ballot.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period with Ballot	October/November 2013
Final Ballot	December 2013
NERC Board of Trustees Adoption	February 2014
Filing to Applicable Regulatory Authorities	February 2014

Version History

Version	Date	Action	Change Tracking
1	6/18/2007	Initial Standard is FERC approved	
2	1/10/2011	FERC approved added LSEs and Controllable Load to the standard.	
3	6/20/2013	WECC Variance is approved by FERC	

Definitions of Terms Used in the Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None.

A. Introduction

1. **Title:** Voltage and Reactive Control

2. **Number:** VAR-001-4

3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in Real-time to protect equipment and the reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators

   4.2. Generator Operators within the Western Interconnection (for the WECC Variance)

5. **Effective Date:**

   5.1. The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

Rationale for R1: Paragraph 1868 of Order No. 693 requires NERC to add more "detailed and definitive requirements on “established limits” and “sufficient reactive resources”, and identify acceptable margins (i.e. voltage and/or reactive power margins)." Since Order No. 693 was issued, however, several FAC and TOP standards have become enforceable to add more requirements around voltage limits. More specifically, FAC-011 and FAC-014 require that System Operating Limits (SOLs) and reliability margins are established. The NERC Glossary definition of SOLs includes both: 1) Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) and 2*)* System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits). Therefore, for reliability reasons Requirement R1 now requires a Transmission Operator (TOP) to set voltage or Reactive Power schedules with associated tolerance bands. Further, since neighboring areas can affect each other greatly, each TOP must also provide a copy of these schedules to its Reliability Coordinator (RC) and adjacent TOP upon request.

R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits. *[Violation Risk Factor: High] [Time Horizon: Operational Planning]*

1.1. Each Transmission Operator shall provide a copy of the voltage schedules (which is either a range or a target value with an associated tolerance band) to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.

M1. The Transmission Operator shall have evidence that it specified system voltage schedules using either a range or a target value with an associated tolerance band.

For part 1.1, the Transmission Operator shall have evidence that the voltage schedules (which is either a range or a target value with an associated tolerance band) were provided to its Reliability Coordinator and adjacent Transmission Operators within 30 days of a request. Evidence may include, but is not limited to, emails, website postings, and meeting minutes.

Rationale for R2:

Paragraph 1875 from Order No. 693 directed NERC to include requirements to run voltage stability analysis periodically, using online techniques where commercially available and offline tools when online tools are not available. This standard does not explicitly require the periodic voltage stability analysis because such analysis would be performed pursuant to the SOL methodology developed under the FAC standards. TOP standards also require the TOP to operate within SOLs and Interconnection Reliability Operating Limits (IROL). The VAR standard drafting team (SDT) and industry participants also concluded that the best models and tools are the ones that have been proven and the standard should not add a requirement for a responsible entity to purchase new online simulations tools. Thus, the VAR SDT simplified the requirements to ensuring sufficient reactive resources are online or scheduled. Controllable load is specifically included to answer FERC's directive in Order No. 693 at Paragraph 1879.

R2. Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operational Planning]*

M2. Each Transmission Operator shall have evidence of scheduling sufficient reactive resources based on their assessments of the system. For the operational planning time horizon, Transmission Operators shall have evidence of assessments used as the basis for how resources were scheduled.

Rationale for R3:

Similar to Requirement R2, the VAR SDT determined that for reliability purposes, the TOP must ensure sufficient voltage support is provided in Real-time in order to operate within an SOL.

R3. Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operational Planning]*

M3. Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as necessary in Real-time. This may include instructions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments.

Rationale for R4:

The VAR SDT received significant feedback on instances when a TOP would need the flexibility for defining exemptions for generators. These exemptions can be tailored as the TOP deems necessary for the specific area's needs. The goal of this requirement is to provide a TOP the ability to exempt a Generator Operator (GOP) from: 1) a voltage or Reactive Power schedule, 2) a setting on the AVR, or 3) any VAR-002 notifications based on the TOP's criteria. Feedback from the industry detailed many system events that would require these types of exemptions which included, but are not limited to: 1) maintenance during shoulder months, 2) scenarios where two units are located within close proximity and both cannot be in voltage control mode, and 3) large system voltage swings where it would harm reliability if all GOP were to notify their respective TOP of deviations at one time. Also, in an effort to improve the requirement, the sub-requirements containing an exemption list were removed from the currently enforceable standard because this created more compliance issues with regard to how often the list would be updated and maintained.

R4. The Transmission Operator shall specify the criteria that will exempt generators from: 1) following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any associated notifications. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

4.1 If a Transmission Operator determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.

M4. Each Transmission Operator shall have evidence of the documented criteria for generator exemptions.

For part 4.1, the Transmission Operator shall also have evidence to show that, for each generator in its area that is exempt from: 1) following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any notifications, the associated Generator Operator was notified of this exemption.

Rationale for R5:

The new requirement provides transparency regarding the criteria used by the TOP to establish the voltage schedule. This requirement also provides a vehicle for the TOP to use appropriate granularity when setting notification requirements for deviation from the voltage or Reactive Power schedule. Additionally, this requirement provides clarity regarding a "tolerance band" as specified in the voltage schedule and the control dead-band in the generator's excitation system.

Voltage Schedule tolerances are the bandwidth that accompanies the voltage target in a voltage schedule, should reflect the anticipated fluctuation in voltage at the Generation Operator's facility during normal operations, and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a Generation Operator's automatic voltage regulator's control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the generator step-up transformer at the Transmission Operator's discretion. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

5.1. The Transmission Operator shall provide the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).

5.2. The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).

5.3. The Transmission Operator shall provide the criteria used to develop voltage schedules Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the Generator Operator within 30 days of receiving a request.

M5. The Transmission Operator shall have evidence of a documented voltage or Reactive Power Schedule (which is either a range or a target value with an associated tolerance band).

For part 5.1, the Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the applicable Generator Operators, and that the Generator Operator was directed to comply with the schedule in automatic voltage control mode, unless exempted.

For part 5.2, the Transmission Operator shall have evidence it provided notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band). For part 5.3, the Transmission Operator shall have evidence it provided the criteria used to develop voltage schedules or Reactive Power schedule

(which is either a range or a target value with an associated tolerance band) within 30 days of receiving a request by a Generator Operator.

Rationale for R6:

Although tap settings are first established prior to interconnection, this requirement could not be deleted because no other standard addresses when a tap setting must be adjusted. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

R6. After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with the requirement and that it consulted with the Generator Owner.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Transmission Operator shall retain evidence for Measures 1 through 6 for 12 months. The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operational Planning**	**High**	N/A	N/A	N/A	The Transmission Operator does not specify a system voltage schedule (which is either a range or a target value with an associated tolerance band).
R2	**Real-time Operations, Same-day Operations, and Operational Planning**	**High**	N/A	N/A	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an SOL.	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an IROL.
R3	**Real-time Operations, Same-day Operations, and Operational Planning**	**High**	N/A	N/A	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an SOL.	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an IROL.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Operations Planning**	**Lower**	N/A	N/A	The Transmission Operator has exemption criteria and notified the Generator Operator, but the Transmission Operator does not have evidence of the notification to the Generator Operator.	The Transmission Operator does not have exemption criteria.
R5	**Operations Planning**	**Medium**	N/A	The Transmission Operator does not provide the criteria for voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) after 30 days of a request.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) to all Generator Operators.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) to any Generator Operators. Or The Transmission Operator does not provide the Generator Operator with the notification requirements for deviations from the

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).
R6	**Operations Planning**	**Lower**	The Transmission Operator does not provide either the technical justification or timeframe for changing generator step-up tap settings.	N/A	N/A	The Transmission Operator does not provide the technical justification and the timeframe for changing generator step-up tap settings.

D. Regional Variances

The following Interconnection-wide variance shall be applicable in the Western Electricity Coordinating Council (WECC) and replaces, in their entirety, Requirements R4 and R5. Please note that Requirement R4 is deleted and R5 is replaced with the following requirements.

Requirements

E.A.13 Each Transmission Operator shall issue any one of the following types of voltage schedules to the Generator Operators for each of their generation resources that are on-line and part of the Bulk Electric System within the Transmission Operator Area: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- A voltage set point with a voltage tolerance band and a specified period.
- An initial volt-ampere reactive output or initial power factor output with a voltage tolerance band for a specified period that the Generator Operator uses to establish a generator bus voltage set point.
- A voltage band for a specified period.

E.A.14 Each Transmission Operator shall provide one of the following voltage schedule reference points for each generation resource in its Area to the Generator Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- The generator terminals.
- The high side of the generator step-up transformer.
- The point of interconnection.
- A location designated by mutual agreement between the Transmission Operator and Generator Operator.

E.A.15 Each Generator Operator shall convert each voltage schedule specified in Requirement E.A.13 into the voltage set point for the generator excitation system. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

E.A.16 Each Generator Operator shall provide its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals within 30 calendar days of request by its Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

E.A.17 Each Transmission Operator shall provide to the Generator Operator, within 30 calendar days of a request for data by the Generator Operator, its transmission equipment data and operating data that supports development of the voltage set point conversion methodology. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

E.A.18 Each Generator Operator shall meet the following control loop specifications if the Generator Operator uses control loops external to the Automatic Voltage Regulators (AVR) to manage MVar loading: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

E.A.18.1. Each control loop's design incorporates the AVR's automatic voltage controlled response to voltage deviations during System Disturbances.

E.A.18.2. Each control loop is only used by mutual agreement between the Generator Operator and the Transmission Operator affected by the control loop.

Measures[1]

M.A.13 Each Transmission Operator shall have and provide upon request, evidence that it provided the voltage schedules to the Generator Operator. Dated spreadsheets, reports, voice recordings, or other documentation containing the voltage schedule including set points, tolerance bands, and specified periods as required in Requirement E.A.13 are acceptable as evidence.

M.A.14 The Transmission Operator shall have and provide upon request, evidence that it provided one of the voltage schedule reference points in Requirement E.A.14 for each generation resource in its Area to the Generator Operator. Dated letters, e-mail, or other documentation that contains notification to the Generator Operator of the voltage schedule reference point for each generation resource are acceptable as evidence.

M.A.15 Each Generator Operator shall have and provide upon request, evidence that it converted a voltage schedule as described in Requirement E.A.13 into a voltage set point for the AVR. Dated spreadsheets, logs, reports, or other documentation are acceptable as evidence.

M.A.16 The Generator Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Transmission Operator it provided its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.A.17 The Transmission Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Generator Operator it provided data to support development of the voltage set point conversion methodology. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.A.18 If the Generator Operator uses outside control loops to manage MVar loading, the Generator Operator shall have and provide upon request, evidence that it met the control loop specifications in sub-parts E.A.18.1 through E.A.18.2. Design specifications with identified agreed-upon control loops, system reports, or other dated documentation are acceptable as evidence.

[1] The number for each measure corresponds with the number for each requirement, i.e. M.E.A.13 means the measure for Requirement E.A.13.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR and supporting package posted for comment on July 19, 2013.
2. Draft standard posted for initial comments and ballot from July 19, 2013 to September 3, 2013.
~~2.~~3. Draft standard posted for an additional comment and ballot from November 15, 2013 to November 26, 2013.

Description of Current Draft

This is the ~~second~~ third posting of the proposed draft standard. This proposed draft standard will be posted for a ~~45~~10-day ~~formal comment period and parallel~~final ballot.

Anticipated Actions	Anticipated Date
Additional 45-Day Comment Period with Ballot	October/November 2013
Final Ballot	December 2013
NERC Board of Trustees Adoption	~~December~~ February 2014~~3~~
Filing to Applicable Regulatory Authorities	~~December~~ February 2014~~3~~

Version History

Version	Date	Action	Change Tracking
1	6/18/2007	Initial Standard is FERC approved	
2	1/10/2011	FERC approved added LSEs and Controllable Load to the standard.	
3	6/20/2013	WECC Variance is approved by FERC	

Definitions of Terms Used in the Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None.

A. Introduction

1. **Title:** Voltage and Reactive Control

2. **Number:** VAR-001-4

3. **Purpose:** To ensure that voltage levels, reactive flows, and reactive resources are monitored, controlled, and maintained within limits in ~~r~~Real-time to protect equipment and the reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Transmission Operators

   4.2. Generator Operators within the Western Interconnection (for the WECC Variance)

5. **Effective Date:**

   5.1. The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

Rationale for R1: Paragraph 1868 of Order No. 693 requires NERC to add more "detailed and definitive requirements on “established limits” and “sufficient reactive resources”, and identify acceptable margins (i.e. voltage and/or reactive power margins)." Since Order No. 693 was issued, however, several FAC and TOP standards have become enforceable to add more requirements around voltage limits. More specifically, FAC-011 and FAC-014 require that System Operating Limits (~~“~~SOLs~~”~~) and reliability margins are established. The NERC Glossary definition of SOLs ~~must~~ includes both: 1) Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) and 2*)* System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits). Therefore, for reliability reasons Requirement R1 now requires a Transmission Operator (TOP) to set voltage or Reactive Power schedules with associated tolerance bands. Further, since neighboring areas can affect each other greatly, each TOP must also provide a copy of these schedules to its Reliability Coordinator (RC) and adjacent TOP upon request.

R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits. *[Violation Risk Factor: High] [Time Horizon: Operational Planning]*

1.1. Each Transmission Operator shall provide a copy of the voltage schedules (which is either a range or a target value with an associated tolerance band) ~~and associated tolerance bands~~ to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.

M1. The Transmission Operator shall have evidence that it specified system voltage schedules using either a range or a target value with an associated tolerance band.

For part 1.1, the Transmission Operator shall have evidence that the voltage schedules (which is either a range or a target value with an associated tolerance band) were provided to its Reliability Coordinator and adjacent Transmission Operators within 30 days of a request. Evidence may include, but is not limited to, emails, website postings, and meeting minutes.

Rationale for R2:

Paragraph 1875 from Order No. 693 directed NERC to include requirements to run voltage stability analysis periodically, using online techniques where commercially available and offline tools when online tools are not available. This standard does not explicitly require the periodic voltage stability analysis because such analysis ~~is now required~~ would be performed ~~-~~pursuant to the SOL methodology developed under~~in~~ the FAC standards. TOP standards also require the TOP to operate within SOLs and Interconnection Reliability Operating Limits (~~"~~IROL~~"~~). The VAR standard drafting team (~~"~~SDT~~"~~) and industry participants also concluded that the best models and tools are the ones that have been proven and the standard should not add a requirement for a responsible entity to purchase new online simulations tools. Thus, the VAR SDT simplified the requirements to ensuring sufficient reactive resources are online or scheduled. Controllable load is specifically included to answer FERC's directive in Order No. 693 at Paragraph 1879.

R2. Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operational Planning]*

M2. Each Transmission Operator shall have evidence of scheduling sufficient reactive resources based on their assessments of the system. For the operational planning time horizon, Transmission Operators shall ~~provide copies~~ have evidence of assessments used as the basis for how resources were scheduled.

Rationale for R3:

Similar to Requirement R2, the VAR SDT determined that for reliability purposes, the TOP must ensure sufficient voltage support is provided in Real-time in order to operate within an SOL.

R3. Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary. *[Violation Risk Factor: High] [Time Horizon: Real-time Operations, Same-day Operations, and Operational Planning]*

M3. Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as ~~needed~~ necessary in Real-time. This may include ~~directions~~ instructions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments.

Rationale for R4:

The VAR SDT received significant feedback on instances when a TOP would need the flexibility for defining exemptions for generators. These exemptions can be tailored as the TOP deems necessary for the specific area's needs. The goal of this requirement is to provide a TOP the ability to exempt a Generator Operator (GOP) from: 1) a voltage or Reactive Power schedule, 2) a setting on the AVR, or 3) any VAR-002 notifications based on the TOP's criteria. Feedback from the industry detailed many system events that would require these types of exemptions which included, but are not limited to: 1) maintenance during shoulder months, 2) scenarios where two units are located within close proximity and both cannot be in voltage control mode, and 3) large system voltage swings where it would harm reliability if all GOP were to notify their respective TOP of deviations at one time. Also, in an effort to improve the requirement, the sub-requirements containing an exemption list were removed from the currently enforceable standard because this created more compliance issues with regard to how often the list would be updated and maintained.

R4. The Transmission Operator shall specify the criteria that will exempt generators from: ~~compliance with the requirements defined in Requirement R5, part 5.1, and any associated notification requirements~~ 1) following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any associated notifications. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

4.1 If a Transmission Operator determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.

M4. Each Transmission Operator shall have evidence of the documented criteria for generator exemptions.

For part 4.1, the Transmission Operator shall also have evidence to show that, for each ~~generating unit~~generator in its area that is exempt from: 1) following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any notifications, the associated Generator Operator was notified of this exemption.

Rationale for R5:

The new requirement provides transparency regarding the criteria used by the TOP to establish the voltage schedule. This requirement also provides a vehicle for the TOP to use appropriate granularity when setting notification requirements for deviation from the voltage or Reactive Power schedule. Additionally, this requirement provides clarity regarding a "tolerance band" as specified in the voltage schedule and the control dead-band in the generator's excitation system.

Voltage Schedule tolerances are the bandwidth that accompanies the voltage target in a voltage schedule, should reflect the anticipated fluctuation in voltage at the Generation Operator's facility during normal operations, and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a Generation Operator's automatic voltage regulator's control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the ~~Generator Step-Up~~ generator step-up transformer at the Transmission Operator's discretion. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

5.1. The Transmission Operator shall provide the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).

5.2. The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).

5.3. The Transmission Operator shall provide the criteria used to develop voltage schedules Reactive Power schedule (which is either a range or a target value with an associated tolerance band) ~~and associated tolerance bands~~ to the Generator Operator within 30 days of receiving a request.

M5. The Transmission Operator shall have evidence of a documented voltage or Reactive Power Schedule (which is either a range or a target value with an associated tolerance band)~~and tolerance band~~.

For part 5.1, the Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band)~~and tolerance band~~ to the applicable Generator Operators, and that the Generator Operator was directed to comply with the schedule in automatic voltage control mode, unless exempted. ~~The evidence shall include written records, email, or voice recordings.~~

For part 5.2, the Transmission Operator shall have evidence it provided notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target

value with an associated tolerance band) ~~and associated tolerance band~~. ~~The evidence shall include written records, email, or voice recordings.~~

For part 5.3, the Transmission Operator shall have evidence it provided the criteria used to develop voltage schedules or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) ~~and associated tolerance bands~~ within 30 days of receiving a request by a Generator Operator.

Rationale for R6:

Although tap settings are first established prior to interconnection, this requirement could not be deleted because no other standard addresses when a tap setting must be adjusted. If the tap setting is not properly set, then the amount of VARs produced by a unit can be affected.

R6. After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with the requirement and that it consulted with the Generator Owner.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Transmission Operator shall retain evidence for Measures 1 through ~~4~~ 6 for 12 months. The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

~~As defined in the NERC Rules of Procedure,~~ "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operational Planning**	**High**	N/A	N/A	N/A	The Transmission Operator ~~has~~does not specify~~ied~~ a system voltage schedule (which is either a range or a target value with an associated tolerance band)~~and associated tolerance bands~~.
R2	**Real-time Operations, Same-day Operations, and Operational Planning**	**High**	N/A	N/A	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an SOL.	The Transmission Operator does not schedule sufficient reactive resources as necessary to avoid violating an IROL.
R3	**Real-time Operations, Same-day Operations, and Operational Planning**	**High**	N/A	N/A	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an SOL.	The Transmission Operator does not operate or direct any real-time operation of devices as necessary to avoid violating an IROL.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Operations Planning**	**Lower**	N/A	N/A	The Transmission Operator has exemption criteria and notified the Generator Operator, but the Transmission Operator does not have evidence of the notification to the Generator Operator.	The Transmission Operator does not have exemption criteria.
R5	**Operations Planning**	**Medium**	N/A	The Transmission ~~Operator~~ Operator does not provide~~s~~ the criteria for voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) ~~-~~after 30 days of a request.	The Transmission Operator does not provide~~s~~ voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band ~~to~~) to ~~some, but not~~ all~~,~~ Generator Operators.	The Transmission Operator does not provide voltage or Reactive Power schedules (which is either a range or a target value with an associated tolerance band) ~~and tolerance bands~~ to any Generator Operators.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Or The Transmission Operator ~~did~~ does not provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).
R6	**Operations Planning**	**Lower**	The Transmission Operator does not provide ~~E~~either the technical justification or timeframe for changing generator step-up tap settings~~are not provided~~.	N/A	N/A	The Transmission Operator does not provide ~~Neither~~ the technical justification ~~nor~~ and the timeframe for changing generator step-up tap settings ~~are provided.~~.

D. Regional Variances

The following Interconnection-wide variance shall be applicable in the Western Electricity Coordinating Council (WECC) and replaces, in their entirety, Requirements R~~3~~4 and R~~4~~5. Please note that Requirement R~~3~~4 is deleted and R~~4~~5 is replaced with the following requirements.

Requirements

E.A.13 Each Transmission Operator shall issue any one of the following types of voltage schedules to the Generator Operators for each of their generation resources that are on-line and part of the Bulk Electric System within the Transmission Operator Area: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- A voltage set point with a voltage tolerance band and a specified period.
- An initial volt-ampere reactive output or initial power factor output with a voltage tolerance band for a specified period that the Generator Operator uses to establish a generator bus voltage set point.
- A voltage band for a specified period.

E.A.14 Each Transmission Operator shall provide one of the following voltage schedule reference points for each generation resource in its Area to the Generator Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

- The generator terminals.
- The high side of the generator step-up transformer.
- The point of interconnection.
- A location designated by mutual agreement between the Transmission Operator and Generator Operator.

E.A.15 Each Generator Operator shall convert each voltage schedule specified in Requirement E.A.13 into the voltage set point for the generator excitation system. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same-day Operations]*

E.A.16 Each Generator Operator shall provide its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals within 30 calendar days of request by its Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

E.A.17 Each Transmission Operator shall provide to the Generator Operator, within 30 calendar days of a request for data by the Generator Operator, its transmission equipment data and operating data that supports development of the voltage set point conversion methodology. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

E.A.18 Each Generator Operator shall meet the following control loop specifications if the Generator Operator uses control loops external to the Automatic Voltage Regulators (AVR) to manage MVar loading: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

E.A.18.1. Each control loop's design incorporates the AVR's automatic voltage controlled response to voltage deviations during System Disturbances.

E.A.18.2. Each control loop is only used by mutual agreement between the Generator Operator and the Transmission Operator affected by the control loop.

Measures[1]

M.A.13 Each Transmission Operator shall have and provide upon request, evidence that it provided the voltage schedules to the Generator Operator. Dated spreadsheets, reports, voice recordings, or other documentation containing the voltage schedule including set points, tolerance bands, and specified periods as required in Requirement E.A.13 are acceptable as evidence.

M.A.14 The Transmission Operator shall have and provide upon request, evidence that it provided one of the voltage schedule reference points in Requirement E.A.14 for each generation resource in its Area to the Generator Operator. Dated letters, e-mail, or other documentation that contains notification to the Generator Operator of the voltage schedule reference point for each generation resource are acceptable as evidence.

M.A.15 Each Generator Operator shall have and provide upon request, evidence that it converted a voltage schedule as described in Requirement E.A.13 into a voltage set point for the AVR. Dated spreadsheets, logs, reports, or other documentation are acceptable as evidence.

M.A.16 The Generator Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Transmission Operator it provided its voltage set point conversion methodology from the point in Requirement E.A.14 to the generator terminals. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.A.17 The Transmission Operator shall have and provide upon request, evidence that within 30 calendar days of request by its Generator Operator it provided data to support development of the voltage set point conversion methodology. Dated reports, spreadsheets, or other documentation are acceptable as evidence.

M.A.18 If the Generator Operator uses outside control loops to manage MVar loading, the Generator Operator shall have and provide upon request, evidence that it met the control loop specifications in sub-parts E.A.18.1 through E.A.18.2. Design specifications with identified agreed-upon control loops, system reports, or other dated documentation are acceptable as evidence.

[1] The number for each measure corresponds with the number for each requirement, i.e. M.E.A.13 means the measure for Requirement E.A.13.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

VAR Directives Project

Implementation Plan for VAR-001-4

Approvals Required

VAR-001-4 – Voltage and Reactive Control

Prerequisite Approvals

There are no other standards that must receive approval prior to the approval of this standard.

Revisions to Glossary Terms

None

Applicable Entities

Transmission Operators (VAR-001-4)

Applicable Facilities

N/A

Conforming Changes to Other Standards

None

Effective Dates

VAR-001-4shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-001-4 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Justification

Because VAR-001 now requires determining voltage and reactive power schedules with associated tolerance bands in addition to any notification requirements, the Transmission Operators need a quarter to prepare documentation. Additionally, the Transmission Operators that do not already provide tolerance bands with voltage schedules will need some time to adjust to providing new data (more specifically, the criteria for schedules) to Generator Operators.

Retirements

VAR-001-3 will be retired at midnight of the day immediately prior to the Effective Date of VAR-001-4 in the particular jurisdiction in which the new standard becomes effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

VAR Directives Project

Implementation Plan for VAR-001-4 ~~and VAR-002-3~~

Approvals Required

VAR-001-4 – Voltage and Reactive Control

~~VAR-002-3 — Generator Operation for Maintaining Network Voltage Schedules~~

Prerequisite Approvals

There are no other standards that must receive approval prior to the approval of this standard.

Revisions to Glossary Terms

None

Applicable Entities

~~Generator Operators (VAR-002-3)~~

~~Generator Owners (VAR-002-3)~~

Transmission Operators (VAR-001-4)

Applicable Facilities

N/A

Conforming Changes to Other Standards

None

Effective Dates

VAR-001-4 ~~and VAR-002-3 – All requirements~~ shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-001-4 ~~and VAR-002-3~~ shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Justification

~~The currently effective VAR-002 standard is one of the most violated standards; however, the industry argues these violations do not address any reliability gaps. Instead, Generator Operators and Transmission Operators are required to handle many nuisance phone calls for slight deviations from a voltage schedule. The nuisance phone calls can be a distraction during a scheduled maintenance or a system event; thus, the industry would support making the changes as soon as possible. However, since~~ Because VAR-001 now requires determining voltage and reactive power schedules with associated tolerance bands in addition to any notification requirements, the Transmission Operators need a quarter to prepare documentation. ~~The VAR-002 standards cannot go into effect without the new TOP schedules and notification requirements. Also for~~ Additionally, the Transmission Operators that do not already provide tolerance bands with voltage schedules~~, those Transmission Operators~~ will need some time to adjust to providing new data (more specifically, the criteria for schedules) to Generator Operators.

Retirements

VAR-001-3 ~~and VAR-002-2b~~ will be retired at midnight of the day immediately prior to the Effective Date of VAR-001-4 ~~and VAR-002-3~~ in the particular jurisdiction in which the new standard~~s are becoming~~ becomes effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Operations

Draft Reliability Standard Compliance Guidance for VAR-001-4 and VAR-002-3
October 21, 2013

Introduction

The NERC Compliance department (Compliance) worked with the VAR standard drafting team (SDT) to review the proposed standards VAR-001-4 and VAR-002-3. The purpose of the review was to discuss the requirements of the proposed standard to obtain an understanding of its intended purpose and the evidence necessary to support compliance. The purpose of this document is to address specific questions posed by the VAR SDT in order to aid in the drafting of the requirements and provide a level of understanding regarding evidentiary support necessary to demonstrate compliance.

While all compliance evaluations require levels of auditor judgment, participating in these reviews allows Compliance to develop training and approaches to support a high level of consistency in audits conducted by the Regional Entities. The following questions and answers are intended to assist the SDT in further refining the standard and to serve as a resource in the development of training for auditors.

VAR-001 and VAR-002 Questions

Question 1

How will compliance determine if sufficient reactive resources were scheduled as part of VAR-001-4 Requirement R2?

Compliance Response to Question 1

For VAR-001-4 Requirement R2, an auditor would review the studies that a TOP used to schedule resources to see that the studies show whether new resources should be brought online, or if the resources online are sufficient to regulate voltage levels. An auditor may observe a TOP reviewing the study and scheduling live and may pull samples from various time periods to determine whether a TOP scheduled resources as required in the study.

Question 2

Is it clear that VAR-001-4 Requirement R4 allows for exemptions, for any duration, from: 1) voltage schedules, 2) being in automatic voltage control mode, or 3) any notification requirements?

Compliance Response to Question

It is clear that VAR-001 Requirement R4 allows for any combination of exemptions for generator operators from 1) voltage schedules, 2) being in automatic voltage control mode, or 3) any notification requirements, as long as the

exemption meets the criteria specified by the TOP. An auditor will not look for any pre-authorization from the TOP; rather an auditor will verify that the generator operator has met the criteria set forth by the TOP.

Question 3

Tolerance bands apply to a set voltage or Reactive Power number with a +/- percentage as the tolerance band. The voltage range or Reactive Power range is a high and low number that a Generator Operator is expected to operate within for reliability purposes. With regard to VAR-001-4 Requirement R5, is it clear that when a voltage range or Reactive Power range is provided as a schedule, a tolerance band is not expected to also be provided?

Compliance Response to Question 3

Yes, it is clear based on VAR-001-4 Requirement R5 that a voltage or Reactive power schedule can be either: 1) a target number with a tolerance band, OR 2) a voltage or Reactive Power range to operate within. An auditor would not expect to see a tolerance band provided with an operating range for voltage or Reactive Power.

Question 4

With regard to VAR-002-3, will generators receive a violation for instances where a system event is affecting system voltage, but the generators made the appropriate conversions and set the AVRs to meet the original schedule provided by the TOP?

Compliance Response to Question 4

No, the generator operators can only be responsible for maintaining the schedule provided by the TOP based on existing facility equipment. In the event that a generator operator does not have the equipment to have visibility of high-side system voltage, the GOP will not have the ability to adjust VARs to maintain system voltage. An auditor is not to determine that, where the GOP does not have the high side monitoring equipment and where the AVR is set appropriately based on existing facility equipment, the generator operator is non-compliant. However, if the TOP provides a new directive or schedule, the GOP is required to follow the new directive. This directive can include modifying an AVR setting or providing more voltage support, and the generator operator is expected to comply pursuant to VAR-002-3.

Question 5

Related to VAR-002-3, generators can monitor voltage on either the low side and high side of the GSU (depending on equipment limitation) and the “number” being monitored by the Generator will not always equate to the number provided by the TOP. Is it clear that VAR-002 Requirement R2, part 2.3 only wants a conversion of the schedule provided to the number monitored? Is it clear that there should not be a violation if the schedule does not match the number being monitored on the low side as long as there is a documented conversion?

Compliance Response to Question 5

The Generator should be able to provide documentation that identifies the "number" being monitored and the calculation demonstrating how the "number" equates to the schedule provided by the TOP. The measure for VAR-002-3 Requirement R2, part 2.3 is clear on what evidence should be able to demonstrate this during an audit.

Question 6

VAR-002-3, Requirement R4 was added because generators cannot report a capability change until they are aware of the change. The currently enforceable standard requires a notification as soon as the capability change occurs; however, many times the change occurred well before the generators were aware of the problem. Is it clear that VAR-002-3 Requirement R4 is only violated after the generator is made aware of the change?

Compliance Response to Question 6

It is clear that VAR-002-3, Requirement R4 will only be a violation if the change is not reported after 30 minutes of becoming aware of the reactive capability change. An auditor will ask an entity for evidence to demonstrate when it became aware of the change in reactive capability. This will not be purely subjective; there are technical instances where it will be clear that an entity would have been made aware of the change in reactive capability. For example, one instance is where a unit is ramping to an expected VAR output, and it cannot reach it; a reactive capability change has occurred.

Conclusion

Following final approval of the Reliability Standard, Compliance will develop the final Reliability Standards Auditor Worksheet (RSAW) and associated training.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VAR Mapping Document
Transition of VAR-001-3

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R1	Requirement R1	This requirement is duplicated in other standards, and the new requirement has been simplified to require the specification of the voltage and Reactive Power schedules and associated tolerance bands. A new part 1.1 has been added to allow for voltage coordination with adjacent TOPs and applicable RCs. In the currently enforceable standards, the TOP-004-2 Requirements R1, R2, and R3 duplicate monitoring and controlling voltage requirements. The same requirements that make the TOP operate within the IROLs and SOLs also require the monitoring and controlling of voltage as a necessary action. The pending TOP-002-3 Requirement R2 and TOP-001-2 Requirements R7 and R9 also cover this function because collectively those requirements mandate: 1) having a plan to operate within IROLs and SOLs and 2) operating within IROLs and SOLs.
VAR-001-3 R2	Requirement R2	The new requirement has been updated to just reflect the scheduling of resources. It eliminates the need for the existing R7, R8, and R9. It also maintains a list of sufficient reactive resources.

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R3	Requirement R4	The new requirement has been simplified by removing the need to maintain an exemption list. Instead, the standard focuses on whether the exemption criteria are known and whether a granted exemption was communicated to the applicable Generator.
VAR-001-3 R4	Requirement R5	The new requirements have been updated to allow the TOP to provide the voltage or Reactive Power schedule at either the high side or the low side of the GSU. Also a tolerance band is now required under the new requirement. New parts have also been added to direct a GOP to operate in AVR, to require the TOP to provide notification requirements, and to provide the criteria for developing schedules and tolerance bands upon request.
VAR-001-3 R5	Deleted	This requirement was proposed to be retired in the P81 NOPR. Therefore, pending a final rulemaking on P81, this requirement has been deleted.
VAR-001-3 R6	Deleted	This requirement is deleted because the TOP standards require knowing the status of Reactive Power resources. In the pending TOP-006-3 R1 and the currently enforceable TOP-006-2 R1, the TOP and BA must know the status of all generating and transmission resources available for use. Although power system stabilizers are not specifically named in either of the TOP standards, the areas that rely on PSS equipment will require monitoring the PSS status under the data specifications of the TOP standards.

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R7	Deleted	This has moved into the new R3.
VAR-001-3 R8	Deleted	This has moved into the new R3.
VAR-001-3 R9	Deleted	See comments for new R2.
VAR-001-3 R10	Deleted	This is duplicative of the pending TOP-001-2 Requirements R9, R10, and R11 before FERC and the Glossary Tv definition which states that IROL and SOL violations must be corrected within 30 minutes. The currently enforceable TOP-004-2 R4 also duplicates this requirement to correct IROLs and SOLs within 30 minutes.
VAR-001-3 R11	Requirement R6	The requirement has been updated to allow for scheduling consultation.
VAR-001-3 R12	Deleted	This requirement was deleted because the EOP standards address taking any corrective action including load-shedding. Also the pending TOP-002-3 Requirement R2 and TOP-001-2 Requirement R11 address the TOP taking corrective actions. The currently enforceable TOP-004-2 R4 also duplicates this requirement to take corrective action.

VAR Mapping Document

Transition of VAR-001-3 ~~and VAR-002-2b~~

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R1	Requirement R1	This requirement is duplicated in other standards, and the new requirement has been simplified to require the specification of the voltage and Reactive Power schedules and associated tolerance bands. A new part 1.1 has been added to allow for voltage coordination with adjacent TOPs and applicable RCs. In the currently enforceable standards, the TOP-004-2 Requirements R1, R2, and R3 duplicate monitoring and controlling voltage requirements. The same requirements that make the TOP operate within the IROLs and SOLs also require the monitoring and controlling of voltage as a necessary action. ~~The pending TOP-002-3 Requirement R2 and TOP-001-2 Requirements R7 and R9 also cover this function because collectively those requirements mandate: 1) having a plan to operate within IROLs and SOLs and 2) operating within IROLs and SOLs.~~

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R2	Requirement R2	The new requirement has been updated to just reflect the scheduling of resources.- Scheduling is a more accurate term for TOP operations. It eliminates the need for the existing ~~R7, R8, and~~ R9. It also maintains a list of sufficient reactive resources.
VAR-001-3 R3	Requirement R4	The new requirement has been simplified by removing the need to maintain an exemption list. Instead, the standard focuses on whether the exemption criteria are known and whether a granted exemption was communicated to the applicable Generator. It eliminates the need for the existing R7 and R8.
VAR-001-3 R4	Requirement R5	The new requirements have been updated to allow the TOP to provide the voltage or Reactive Power schedule at either the high side or the low side of the GSU. Also a tolerance band is now required under the new requirement. New parts have also been added to direct a GOP to operate in AVR, to require the TOP to provide notification requirements, and to provide the criteria for developing schedules and tolerance bands upon request.
VAR-001-3 R5	Deleted	This requirement was proposed to be retired in the P81 NOPR. Therefore, pending a final rulemaking on P81, this requirement has been deleted.

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R6	Deleted	This requirement is deleted because the TOP standards require knowing the status of Reactive Power resources. In the pending TOP-006-3 R1 and the currently enforceable TOP-006-2 R1, the TOP and BA must know the status of all generating and transmission resources available for use. Although power system stabilizers are not specifically named in either of the TOP standards, the areas that rely on PSS equipment will require monitoring the PSS status under the data specifications of the TOP standards.
VAR-001-3 R7	Deleted	This has moved into the new R3.
VAR-001-3 R8	Deleted	This has moved into the new R3.
VAR-001-3 R9	Deleted	See comments for new R2.
VAR-001-3 R10	Deleted	This is duplicative of the pending TOP-001-2 Requirements R9, R10, and R11 before FERC and the Glossary Tv definition which states that IROL and SOL violations must be corrected within 30 minutes. The currently enforceable TOP-004-2 R4 also duplicates this requirement to correct IROLs and SOLs within 30 minutes.
VAR-001-3 R11	Requirement R6	The requirement has been updated to allow for scheduling consultation.

Standard: VAR-001-4 – Voltage and Reactive Control		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-001-3 R12	Deleted	This requirement was deleted because the EOP standards address taking any corrective action including load-shedding. ~~Also the pending TOP-002-3 Requirement R2 and TOP-001-2 Requirement R11 address the TOP taking corrective actions.~~ The currently enforceable TOP-004-2 R4 ~~also~~ duplicates this requirement to take corrective action.

~~Standard: VAR-001-2 — Capacity Benefit Margin~~		
~~**Requirement in Approved Standard**~~	~~**Transitions to the below Requirement in New Standard or Other Action**~~	~~**Description and Change Justification**~~
~~VAR-002-2b R1~~	~~Requirement R1~~	~~The requirement has been modified to allow for testing and exemptions for other AVR modes when necessary.~~
~~VAR-002-2b R2~~	~~Requirement R2~~	~~The new requirement has been updated to allow for the TOP to define notification requirements. The requirement also adds parts to allow for the conversion of a high side schedule to a low side number for monitoring purposes.~~
~~VAR-002-2b R3~~	~~Requirement R3 and R4.~~	~~The old requirement has been broken into two requirements: 1) one for AVR/PSS status, and 2) one for reactive capability. Both allow 15 minutes to correct an issue before having to notify the TOP.~~
~~VAR-002-2b R3~~	Requirement ~~R4~~R5	~~The requirement has not been modified.~~The original sub-requirement 4.1.4 (the +/- voltage range with step-change in % for load-tap changing transformers) has been removed because other data specifications in MOD-10-0 requirement R2 duplicate this requirement.
~~VAR-002-2b R4~~	~~Requirement R5~~	~~The requirement has not been modified.~~

Formatted: Highlight

VAR Revisions

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Reliability Standard Audit Worksheet[1]

VAR-001-4 – Voltage and Reactive Control

This section to be completed by the Compliance Enforcement Authority.

Audit ID: Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity: Registered name of entity being audited
NCR Number: NCRnnnnn
Compliance Enforcement Authority: Region or NERC performing audit
Compliance Assessment Date(s)[2]: Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method: Audit
Names of Auditors: Supplied by CEA

Applicability of Requirements *[RSAW developer to insert correct applicability]*

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1													X		
R2													X		
R3													X		
R4													X		
R5													X		
R6													X		

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Subject Matter Experts

Identify Subject Matter Expert(s) responsible for this Reliability Standard. (Insert additional rows if necessary)

Registered Entity Response (Required):

SME Name	Title	Organization	Requirement(s)

DRAFT

R1 Supporting Evidence and Documentation

R1. Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.

1.1. Each Transmission Operator shall provide a copy of the voltage schedules and associated tolerance bands to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.

M1. The Transmission Operator shall have evidence that it specified system voltage schedules using either a range or a target value with an associated tolerance band.

For part 1.1, the Transmission Operator shall have evidence that the voltage schedules were provided to its Reliability Coordinator and adjacent Transmission Operators within 30 days of a request. Evidence may include, but is not limited to, emails, website postings, and meeting minutes.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[3]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M1.
Documentation of request made per Part 1.1 from Reliability Coordinator and/or adjacent Transmission Operators, if applicable and requested by auditor.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

[3] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-001-4, R1
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R1) Review evidence provided and ensure it meets the requirements outlined in Requirement R1.
	(Part 1.1) Examine evidence to verify that voltage schedules were provided within 30 days of request per Part 1.1.

Note to Auditor: Auditors, at their discretion and based on the risk of the entity's compliance with this requirement to the BES, may communicate with Balancing Authorities and other Transmission Operators to determine if data requests were made of the entity. Auditors may also accept entity assertions regarding whether data requests made.

Entity assertions that no data requests were made do not have to be in writing.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load.

M2. Each Transmission Operator shall have evidence of scheduling sufficient reactive resources based on their assessments of the system. For the operational planning time horizon, Transmission Operators shall provide copies of assessments used as the basis for how resources were scheduled.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[4]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M2.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-001-4, R2
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Review the studies/assessments that entity used to schedule resources to determine that the studies show whether new resources should be brought online, or if the resources online are sufficient to regulate voltage levels. Auditors should verify that actual scheduling reflected the results of the studies/assessments.

[4] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound, only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough instances, per above, to gain reasonable assurance that entity is complying with Requirement R2.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary.

M3. Each Transmission Operator shall have evidence that actions were taken to operate capacitive and inductive resources as needed in Real-time. This may include directions to Generator Operators to: 1) provide additional voltage support; 2) bring resources on-line; or 3) make manual adjustments.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[5]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
Any written policies, procedures or protocols describing how the entity operates or directs devices to regulate transmission voltage and reactive flow as necessary, if the entity has such documents.
Evidence as outlined in M3 as requested by auditor.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location

[5] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-001-4, R3
This section to be completed by the Compliance Enforcement Authority

	Review evidence to understand how entity operates or directs devices to regulate transmission voltage and reactive flow as necessary. Auditors may sample system events or other instances of voltage irregularities to verify that operations or directions occurred as required per Requirement R2.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound, only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough events or other instances of voltage irregularities, per above, to gain reasonable assurance that entity is complying with Requirement R2.

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. The Transmission Operator shall specify the criteria that will exempt generators from compliance with the requirements defined in Requirement R5, part 5.1, and any associated notification requirements.

4.1 If a Transmission Operator determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.

M4. Each Transmission Operator shall have evidence of the documented criteria for generator exemptions.

For part 4.1, the Transmission Operator shall also have evidence to show that, for each generating unit in its area that is exempt from: 1) following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any notifications, the associated Generator Operator was notified of this exemption.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[6]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M4.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-001-4, R4
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R4) Review evidence and note existence of exemption criteria per Requirement R4. For a sample of exempted generators, verify that exemption was granted in accordance with criteria.

[6] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

	(Part 1.1) For a sample of exempted generators, ensure exempted generator was notified.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound, only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough generators, per above, to gain reasonable assurance that entity is complying with Requirement R4.

Requirement R4 allows for any combination of exemptions for generator operators from 1) voltage schedules, 2) being in automatic voltage control mode, or 3) any notification requirements, as long as the exemption meets the criteria specified by the entity. An auditor will not look for any pre-authorization from the entity; rather an auditor will verify that the generator operator has met the criteria set forth by the entity.

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the Generator Step-Up transformer at the Transmission Operator's discretion.

5.1. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).

5.2. The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule.

5.3. The Transmission Operator shall provide the criteria used to develop voltage schedules and associated tolerance bands to the Generator Operator within 30 days of receiving a request.

M5. The Transmission Operator shall have evidence of a documented voltage or Reactive Power Schedule and tolerance band.

For part 5.1, the Transmission Operator shall have evidence it provided a voltage or Reactive Power schedule and tolerance band to the applicable Generator Operators, and that the Generator Operator was directed to comply with the schedule in automatic voltage control mode, unless exempted. The evidence shall include written records, email, or voice recordings.

For part 5.2, the Transmission Operator shall have evidence it provided notification requirements for deviations from the voltage or Reactive Power schedule and associated tolerance band. The evidence shall include written records, email, or voice recordings.

For part 5.3, the Transmission Operator shall have evidence it provided the criteria used to develop voltage schedules and associated tolerance bands within 30 days of receiving a request by a Generator Operator.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[7]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M5.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-001-4, R5
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R5) Verify existence of voltage or Reactive Power schedule and that it meets the requirements of Requirement R5.
	(Part 5.1) For a sample of Generator Operators, verify voltage or Reactive Power schedule was provided

[7] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

	per Part 5.1.
	(Part 5.2) For a sample of Generator Operators, verify the notification requirements for deviations from the voltage or Reactive Power schedule was provided per Part 5.2.
	(Part 5.3) For a sample of Generator Operators, verify criteria was provided as requested per Part 5.3.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound, only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough notifications, per above, to gain reasonable assurance that entity is complying with Requirement R5.

It is clear based on VAR-001-4 Requirement R5 that a voltage or Reactive power schedule can be either: 1) a target number with a tolerance band, Or 2) a voltage or Reactive Power range to operate within. An auditor would not expect to see a tolerance band provided with an operating range for voltage or Reactive Power.

Auditor Notes:

R6 Supporting Evidence and Documentation

R6. After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.

M6. The Transmission Operator shall have evidence that it provided documentation to the Generator Owner when a change was needed to a generating unit's step-up transformer tap in accordance with the requirement and that it consulted with the Generator Owner.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[8]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.

[8] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

See M6.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-001-4, R6
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Understand entity's procedures concerning coordinating tap settings with Generator Owners per Requirement R6.
	For a sample of Generator Owners, verify tap setting changes were executed per Requirement R6.
Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound, only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough tap setting communications, per above, to gain reasonable assurance that entity is complying with Requirement R6.	

Auditor Notes:

Revision History

Version	Date	Reviewers	Revision Description
1	11/07/2013	NERC compliance, Standards	New Document

DRAFT

Violation Risk Factor and Violation Severity Level Justifications

VAR-001-4 – Voltage and Reactive Control

This document provides the Standard Drafting Team's (SDT) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in VAR-001-4 – Voltage and Reactive Control. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project. A copy of the standard with the associated VRFs and VSLs is available here.

NERC Criteria - Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Violation Risk Factor Guidelines

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

The Commission seeks to ensure that Violation Risk Factors assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities

• Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

Guideline (3) – Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) –Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria - Violation Severity Levels

Violation Severity Levels (VSLs) define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

Violation severity levels should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

FERC's VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline 1 – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline 2 – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3 – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline 4 – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the

Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification – VAR-001-4 Requirement R1	
Proposed VRF	**High**
NERC VRF Discussion	A VRF of High is necessary because this requirement ensures that a system voltage schedule is created to ensure system stability.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: This High VRF is consistent with the Blackout Report because Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The VRF applies to the entire requirement. The sub-part within Requirement R1 is consistent and considered a High VRF.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: Because maintaining a voltage schedule is critical to preventing a violation of a System Operating Limit, this VRF was drafted to be consistent with the VRFs for other standards (e.g., TOP, FAC, etc.) addressing operating within the appropriate limits.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because voltage instability will cause "Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures."
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More Than One Obligation: This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level.

VSL Justification – VAR-001-4 Requirement R1	
NERC VSL Guidelines	Consistent with NERC's VSL Guideline, this VSL acknowledges the criticality of this requirement and whether or not a system voltage schedule was created.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The current level of compliance is not lowered with the proposed VSL because this is a new requirement, and it only has a "severe" VSL.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary, and therefore, a single severe VSL is necessary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the	The proposed VSL is consistent with the corresponding requirements.

Corresponding Requirement	
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on a cumulative number of violations.

VRF Justification – VAR-001-2 Requirement R2	
Proposed VRF	**High**
NERC VRF Discussion	A VRF of High is consistent with the NERC VRF definition. Requirement R2 focuses on ensuring there are enough reactive resources online to regulate voltage levels, and a High VRF represents the criticality of making sure the system resources are adjusted to meeting normal and Contingency conditions.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: This High VRF is consistent with the Blackout Report because Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System. Therefore, ensuring the proper resources are online for voltage support warrants a High VRF.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: There is no sub-part to Requirement R2; therefore, it is consistent.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: Because scheduling resources is critical to preventing a system operating limit, this VRF is drafted to be consistent with other standards (e.g., TOP, FAC, etc.) that address operating within the appropriate limits.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs:

	This VRF is consistent with the NERC Definition because not scheduling enough resources to support system conditions will cause "Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures."
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation: This VRF does not co-mingle multiple objectives, nor does it water down the requirement to reflect a lower risk level.

VSL Justification – VAR-001-4 Requirement R2	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines, the VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

"Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

VRF Justification – VAR-001-4 Requirement R3	
Proposed VRF	**High**
NERC VRF Discussion	This requirement warrants a High VRF and is consistent with the NERC definition because this requirement represents a critical step that TOPs should take in order to avoid an SOL violation in Real-time.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: This High VRF is consistent with the Blackout Report because Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System. Therefore, ensuring that the TOP directs the Real-time devices as necessary to regulate voltage and reactive flow warrants a High VRF.

FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: There is no sub-part to Requirement 3; therefore, the requirement is consistent.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: Because directing other Real-time devices for voltage and reactive flows is critical to preventing a system operating limit, this VRF is drafted to be consistent with other standards (e.g., TOP, FAC, etc.) that address operating within the appropriate limit.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because not directing Real-time operation of devices as necessary could directly cause "Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures."
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level

VSL Justification – VAR-001-4 Requirement R3	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The current level of compliance is not lowered with the proposed VSL.

FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

VRF Justification – VAR-001-4 Requirement R4	
Proposed VRF	**Lower**
NERC VRF Discussion	This requirement is Lower because it focuses on whether a TOP has created an exemption criteria. The Lower VRF is warranted because many entities will not have any exemptions allowed generators within their system. Additionally, a violation of this requirement would not adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: This VRF is consistent with the Blackout Report because although Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, a violation of the requirements to have exemption criteria would result in the GOPs being held to a more stringent performance requirement and is unlikely to severely affect the reliability of the bulk Power System. Therefore, a lower VRF is warranted.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The sub-part within Requirement R4 is consistent with R4 and is considered a Lower VRF.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: Other standards do not address exemptions from 1) voltage schedules; 2) AVR settings; or 3) any associated notifications.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because if the GOP is not exempted, a higher performance expectation maintained for GOPs. This does more to protect against events that could cause “Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures.”
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation:

	This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a Lower risk level.

VSL Justification – VAR-001-4 Requirement R4	
NERC VSL Guidelines	This VSL is consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The current level of compliance is not lowered with the proposed VSL.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3:	The proposed VSL is worded consistently with the corresponding requirement.

Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

VRF Justification – VAR-001-4 Requirement R5	
Proposed VRF	**Medium**
NERC VRF Discussion	This requirement is a Medium because even if a TOP does not provide the voltage or Reactive Power schedules to all GOPs, the TOP is still monitoring the system and will direct the GOPs within an area to provide voltage support as necessary.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: This VRF is consistent with the Blackout Report because although Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, the TOP standards and Requirements R1-4, still require the TOP to monitor voltage to operate within System Operating Limits. Therefore, a Medium VRF is warranted.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The parts within Requirement R5 are consistent with Requirement R5 and is considered a Medium VRF.

FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: As explained in Guideline 1, this requirement is consistent with other standards, namely TOP standards.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a violation "could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System." However, due to the TOP standards, a violation is unlikely to like to a lead "to Bulk Electric System instability, separation, or cascading failures."
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation: This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level.

VSL Justification – VAR-001-4 Requirement R5	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2:	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties.

Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	Guideline 2a: The proposed VSL is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

VRF Justification – VAR-001-4 Requirement R6

Proposed VRF	Lower
NERC VRF Discussion	This requirement ensures there is coordination for making TOP-directed tap setting changes. A violation of this requirement would not lead to a system event, but the coordination must happen in order for a TOP to know when a generator is going offline. The proper tap settings also ensures Max VAR capability of a unit is maintained.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: This VRF is consistent with the Blackout Report because although Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, this requirement is aimed at improving the max VARs put into the system. If this requirement were violated, the system would still operate at the level it was prior to making the tap changes.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: There is no sub-part to Requirement R6, and a TOP would still be monitoring the system in order to prevent a system event. Therefore, this requirement is consistent and considered a Medium VRF.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: This requirement is not addressed by other standards.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a violation "could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System." However, due to the TOP standards, a violation of this requirement alone is unlikely to like to a lead "to Bulk Electric System instability, separation, or cascading failures."
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation:

	This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level.

VSL Justification – VAR-001-4 Requirement R6	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3:	The proposed VSL is worded consistently with the corresponding requirement.

Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

DRAFT-Consideration of Issues and Directives

Project 2013-04 – Voltage and Reactive Control

Voltage and Reactive Control		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Summary of Directives from FERC: **1.** VAR-001: FERC ordered that the standard be developed to: (1) expand the applicability to include reliability coordinators and LSEs; (2) include detailed and definitive requirements on "established limits" and "sufficient reactive resources", and identifies acceptable margins above the voltage instability points; (3) include Requirements to perform voltage stability analysis periodically, using online techniques where commercially available and offline techniques where online techniques are not available, to assist real-time operations, for areas susceptible to voltage instability; (4) include controllable load among the reactive resources to satisfy reactive requirements and (5) addresses the power factor range at the interface between LSEs and the transmission grid. **2.** VAR-001: FERC clarified that voltage schedules must have a technical basis and remanded an interpretation of VAR-001 back to NERC for reconsideration. **3.** VAR-002: FERC directed NERC to consider Dynegy's suggestions to improve the standard by providing more detailed and definitive requirements for establishing time frames associated with an incident of non-compliance.		
Accordingly, the ERO should modify VAR-001-1 to include reliability coordinators as applicable entities and	Order No. 693, P 1855	FERC recently issued a Notice of Proposed Rulemaking on the IRO family of standards.[1] Although FERC recommended a remand of the IRO filing, the monitoring role of the Reliability

[1] *Monitoring System Conditions - Transmission Operations Reliability Standard Transmission Operations Reliability Standards Interconnection Reliability Operations and Coordination Reliability Standards*, 145 FERC ¶ 61,158 (2013).

Voltage and Reactive Control		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
include a new requirement(s) that identifies the reliability coordinator's monitoring responsibilities.		Coordinator is best addressed in the IRO standards generally. Therefore, this directive will be addressed by a future IRO project.
The Commission directs the ERO to address the reactive power requirements for LSEs on a comparable basis with purchasing-selling entities.	Order No. 693, P 1858	This directive has been met, and is effectively retired. This directive has already been addressed and reviewed by FERC in a prior version VAR-001-2.[2] However, the applicable requirement (R5 of the currently effective VAR-001-3) that initially addressed this directive has been removed from the VAR standards due to overlap with the *pro forma* Open Access Transmission Tariff ("OATT).[3] Thus, this directive is no longer needed for reliability and should be withdrawn or retired.
In the NOPR, the Commission asked for comments on acceptable ranges of net power factor at the interface at which the LSEs receive service from the Bulk-Power System during normal and extreme load conditions... The Commission believes that Reliability Standard VAR-001-1 is an appropriate place for the ERO to take steps to address these concerns by setting out requirements for transmission owners and LSEs to maintain an appropriate power factor range at their interface. **We direct the ERO**	Order No. 693, P 1861	This directive is no longer needed for reliability and should be withdrawn. Power factor ranges/requirements are established by contract, and to include such ranges/requirements in the VAR standard would be duplicative. The TPL-001-4 has now been approved and will address requirements for power factors. TPL-001-4, Requirement R1, part 1.1.4 requires system models to include Real and reactive Load forecasts. These two inputs in the TOP's models ultimately provide the appropriate power factors that should be maintained.

[2] *See* FERC letter order, *NERC Petition for Approval of Proposed Modifications to Reliability Standards BAL-002-1; EOP-002-3; FAC-002-1; MOD-021-2; PRC-004-2; and VAR-001-2,* 134 FERC ¶ 61,015 (2011).

[3] *Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards,* Order No. 788, 145 FERC ¶ 61,147 (2013).

Voltage and Reactive Control		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
to develop appropriate modifications to this Reliability Standard to address the power factor range at the interface between LSEs and the Bulk- Power System.		In addition, the FAC-001-0 standard requires Transmission Owners (TOs) to set interconnection requirements including "Voltage, Reactive Power, and power factor control" (emphasis added). Thus, the power factor controls and requirements are outlined as part of the interconnection studies/process. Finally, as markets have matured the RTO's have addressed the reliability issues regarding wholesale LSE's through various governance agreements. These agreements speak to the reliable planning, operation, and coordination between the BPS and LSE's.
We direct the ERO to include APPA's concern in the Reliability Standards development process. We note that transmission operators currently have access to data through their energy management systems to determine a range of power factors at which load operates during various conditions, and **we suggest that the ERO use this type of data as a starting point for developing this modification.**	Order No. 693, P 1862	The directive has been addressed by the VAR SDT, and APPA's concerns were discussed early in Project 2013-04. In Order No. 693 APPA stated, "it may be difficult to reach an agreement on acceptable ranges of net power factors at the interfaces where LSEs receive service from the Bulk-Power System because the acceptable range of power factors at any particular point on the electrical system varies based on many location-specific factors. APPA further states that system power factors will be affected by the transmission infrastructure used to supply the load."[4]

[4] *See Mandatory Reliability Standards for the Bulk-Power System,* Order No. 693, FERC Stats. & Regs. ¶31,242 at P 1861, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

Voltage and Reactive Control		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		As stated above, the VAR SDT determined the power factor will be addressed by interconnection agreements, the OATT, and other standards. In light of how the directives for PP 1858 and 1863 are addressed, the VAR SDT determined the appropriate power factor range is addressed through the OATT and the interconnection process. Therefore, the VAR SDT determined that it was not necessary to add VAR requirements to access power factor data because that would be duplicative, and FERC determined these types of requirement are not needed for reliability, as stated in Order No. 788 which approved certain P81 retirements.[5]
The Commission expects that the appropriate power factor range developed for the interface between the bulk electric system and the LSE from VAR-001-1 would be used as an input to the transmission and operations planning Reliability Standards. The range of power factors developed in this Reliability Standard provides the input to the range of power factors identified in the modifications to the TPL Reliability Standards.	Order No. 693, P 1863	The Commission clarified that this is not a directive to change or modify a standard.[6]
In the NOPR, the Commission expressed concern that the technical requirements containing terms such as	Order No. 693, P1868	This directive on established limits is being addressed in an equally effective and efficient manner through the TOP and FAC

[5] *See* Order No. 788.

[6] *Id.* at Attachment A.

Voltage and Reactive Control		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
"established limits" or "sufficient reactive resources" are not definitive enough to address voltage instability and ensure reliable operations. To address this concern, the NOPR proposed directing the ERO to modify VAR-001-1 to include more detailed and definitive requirements on "established limits" and "sufficient reactive resources" and identify acceptable margins (i.e. voltage and/or reactive power margins) above voltage instability points to prevent voltage instability and to ensure reliable operations. **We will keep this direction, and direct the ERO to include this modification in this Reliability Standard**.		family of standards. After Order No. 693 was issued, several standards were approved by FERC providing specific requirements on "established limits" and associated margins. FAC-011 and FAC-014 both address SOLs which by definition must include both voltage stability ratings and system voltage limits. An SOL is the value (such as MW, MVar, Amperes, Frequency or Volts) that satisfies the most limiting of the prescribed operating criteria for a specified system configuration to ensure operation within acceptable reliability criteria. System Operating Limits are based upon certain operating criteria. These include, but are not limited to: • Facility Ratings (Applicable pre- and post-Contingency equipment or facility ratings) • Transient Stability Ratings (Applicable pre- and post-Contingency Stability Limits) • Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) • System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits). [7] Further, FAC-014-2 Requirement R2 demands "[t]he Transmission Operator shall establish SOLs (as directed by its

[7] *See NERC Glossary of Terms Used in Reliability Standards,* available at *http://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.*

Voltage and Reactive Control		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Reliability Coordinator) for its portion of the Reliability Coordinator Area that are consistent with its Reliability Coordinator's SOL Methodology." FAC-011-2 Requirement R2 states "[t]he Reliability Coordinator's SOL Methodology shall include a requirement that SOLs provide BES performance consistent with the following: R2.1. In the pre-contingency state, the BES shall demonstrate transient, dynamic and voltage stability; all Facilities shall be within their Facility Ratings and within their thermal, voltage and stability limits. In the determination of SOLs, the BES condition used shall reflect current or expected system conditions and shall reflect changes to system topology such as Facility outages. R2.2. Following the single Contingencies identified in Requirement 2.2.1 through Requirement 2.2.3, the system shall demonstrate transient, dynamic and voltage stability; all Facilities shall be operating within their Facility Ratings and within their thermal, voltage and stability limits; and Cascading or uncontrolled separation shall not occur." (emphases added). FAC-011-2, R3 states: "The Reliability Coordinator's methodology for determining SOLs, shall include, as a minimum,

Voltage and Reactive Control		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		a description of the following, along with any reliability margins…" (emphasis added). Although FAC standards require the establishment and criteria of SOLs, the TOP standards require operations within SOLs and IROLs. The currently enforceable TOP-002-2.1b requires that "Each Balancing Authority and Transmission Operator shall plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs)." TOP-004-2 R1 states "Each Transmission Operator shall operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs)." Thus, the TOP and FAC standards provide sufficient details on established limits and acceptable margins for voltage by providing vehicles for monitoring and operating within SOLs and IROLs. If a system event were to occur due to voltage, the TOP and FAC standards would be the appropriate place for a violation because a limit would have been violated. With regard to the directive on sufficient reactive resources, VAR-001 R2 has been modified to state the TOP will "schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means

Voltage and Reactive Control		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load." As explained in the rationale for the new requirement ensures sufficient reactive resources are online or scheduled to regulate voltage levels. The old requirement used the term "acquire" instead of schedule, and there was industry confusion on how to acquire sufficient reactive resources.
We recognize that our proposed modification does not identify what definitive requirements the Reliability Standard should use for "established limits" and "sufficient reactive resources." **Rather, the ERO should develop appropriate requirements that address the Commission's concerns through the ERO Reliability Standards development process.**	Order No. 693, P 1869	The Commission clarified that this is not a directive to change or modify a standard.[8]
In response to the concerns of APPA, SDG&E and EEI on the availability of tools, the Commission recognizes that transient voltage stability analysis is often conducted as an offline study, and that steady-state voltage stability analysis can be done online. The Commission clarifies that it does not wish to require anyone to use tools that are not validated for real-time operations. Taking these comments into consideration, the Commission clarifies its	Order No. 693, P 1875	Analytical tools or online techniques in general will be addressed in Project 2009-02, Real-time Monitoring and Analysis Capabilities. Therefore, this directive will be addressed in that project. Further, the VAR SDT determined that the Commission is not requiring TOPs to purchase new online models or to implement tools that will not adequately study a TOP's reactive power requirements. The VAR SDT also

[8] *See* Order No. 788 at Attachment A.

Voltage and Reactive Control		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
proposed modification from the NOPR. For the Final Rule, **we direct the ERO, through its Reliability Standards development process, to modify Reliability Standard VAR-001-1 to include Requirements to perform voltage stability analysis periodically, using online techniques where commercially-available, and offline simulation tools where online tools are not available, to assist real-time operations. The ERO should consider the available technologies and software as it develops this modification to VAR-001-1 and identify a process to assure that the Reliability Standard is not limiting the application of validated software or other tools.**		determined that the most reliable models are the ones proven over time to correctly model the system. Further, the VAR SDT also determined the TOP standards require periodic voltage stability analysis. The currently enforceable standards: TOP-004-2 and TOP-006-2 require actively monitoring voltage in order to operate within SOLs.
The Commission noted in the NOPR that in many cases, load response and demand-side investment can reduce the need for reactive power capability in the system. Based on this assertion, the Commission proposed to direct the ERO to include controllable load among the reactive resources to satisfy reactive requirements for incorporation into Reliability Standard VAR-001-1. **While we affirm this requirement, we expect the ERO to consider the comments of SoCal Edison with regard to**	Order No. 693, P 1879	NERC addressed this directive in a prior version of the VAR standard, but as mentioned above, examples of sufficient reactive resources including controllable load are listed in VAR-001 R2.[9]

[9] *supra* at note 2.

Voltage and Reactive Control		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
reliability and SMA in its process for developing the technical capability requirements for using controllable load as a reactive resource in the applicable Reliability Standards.		
Dynegy has suggested an improvement to Reliability Standard VAR-002-1, and NERC should consider this in its Reliability Standards development process.	Order No. 693, P 1885	Dynegy stated that VAR-002-1 should be modified to require detailed and definitive requirements when defining the timeframe associated with an "incident" of non-compliance. The VAR SDT, NERC staff, and industry participants could not agree on an appropriate number for creating a non-compliance window for the continent. Instead, VAR-001 was modified to require TOPs to create notification requirements for their GOPs in VAR-001-4 Requirement 5, part 5.2. The TOPs can then tailor their notification requirements based on their area's reliability needs/voltage constraints.
The Commission remands to the ERO the proposed interpretation of VAR-001-1, Requirement R4 and directs the ERO to revise the interpretation consistent with the Commission's discussion below.	Order No. 724, P 47.	P 49 of Order No. 724 explains this directive by stating "the Commission adopts its NOPR proposal, and finds that a voltage schedule should reflect sound engineering, as well as operating judgment and experience. The Commission remands NERC's proposed VAR-001-1, Requirement R4 interpretation, in order

Voltage and Reactive Control		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		that NERC may reconsider its interpretation consistent with this order."[10] NERC staff and TOPs expressed concern that having to justify a schedule could provide a forum for disputing voltage schedules in general. This could harm reliability if GOPs were permitted to not implement a schedule until there was consensus on the technical merits of a voltage schedule. Therefore, in order to maintain a TOPs authority for setting schedules, the VAR SDT determined the standard should require sharing study data for how a voltage schedule was determined. The VAR SDT determined that in order to show voltage schedules reflect sound engineering and judgment, a TOP should provide the criteria for developing schedules and tolerance bands when requested by a GOP. This is reflected in VAR-001-4 Requirement 5, part 5.3. This requirement allows the GOP to understand the technical basis for a voltage schedule, but it does not create a vehicle for the GOPs to approve the voltage schedule.

[10] *Electric Reliability Organization Interpretations of Specific Requirements of Frequency Response and Bias and Voltage and Reactive Control Reliability Standards*, 127 FERC ¶ 61,158 at P 49 (2009).

Voltage and Reactive Control		
Issue or Directive	**Source**	**Consideration of Issue or Directive**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement Update

Project 2013-04 Voltage and Reactive Control
VAR-001-4

Final Ballot Now Open through December 23, 2013

Now Available

It has come to NERC's attention that an administrative error resulted in incorrect votes being carried forward for the VAR-001-4 final ballot that opened on December 11, 2013. The final ballot for VAR-001-4 is being restarted today with the appropriate votes carried forward and will end on Monday, December 23, 2013. Anyone who has logged in during the incorrect final ballot period to change their vote will need to log in again to revote in this ballot. We recognize that this ballot now closes the Monday of a holiday week and apologize for the inconvenience.

As this final ballot needed to be restarted due to the administrative error, the following two additional clarifying changes were made to the standard:

- **The language in Requirement R4 regarding criteria for generator exemptions was clarified to match the language in the measure.**
- **Requirement references in the WECC Regional Variance were updated to match the corresponding requirements in VAR-001-4.**

Background information for this project can be found on the project page.

Instructions for Balloting

In the final ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their previously cast votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the final ballot window. If a ballot pool member does not participate in the final ballot, that member's vote cast in the previous ballot will be carried over as that member's vote in the final ballot.

Members of the ballot pool associated with this project may log in and submit their vote for the standard by clicking here.

Next Steps

Voting results for the standard will be posted and announced after the ballot window closes. If approved, it will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-001-4

Final Ballot Now Open through December 20, 2013

Now Available

A final ballot for **VAR-001-4** is open through **8 p.m. Eastern on Friday, December 20, 2013.**

Background information for this project can be found on the project page.

Instructions for Balloting

In the final ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their previously cast votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the final ballot window. If a ballot pool member does not participate in the final ballot, that member's vote cast in the previous ballot will be carried over as that member's vote in the final ballot.

Members of the ballot pool associated with this project may log in and submit their vote for the standard by clicking here.

Next Steps

Voting results for the standard will be posted and announced after the ballot window closes. If approved, it will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-001-4 and VAR-002-3

Final Ballot Results

Now Available

A final ballot for **VAR-001-4** concluded at **8 p.m. Eastern on Monday, December 23, 2013.**

The standard achieved a quorum and sufficient affirmative votes for approval. Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results for the ballots.

Standard	Quorum /Approval
VAR-001-4	84.34% / 75.35%

Background information for this project can be found on the project page.

Next Steps

The standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results	
Ballot Name:	Project 2013-04 Voltage and Reactive Control VAR-001-4 _
Ballot Period:	12/13/2013 - 12/23/2013
Ballot Type:	Final Ballot
Total # Votes:	334
Total Ballot Pool:	396
Quorum:	**84.34 % The Quorum has been reached**
Weighted Segment Vote:	75.35 %
Ballot Results:	**A quorum was reached and there were sufficient affirmative votes for approval.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	106	1	57	0.695	25	0.305	0	8	16
2 - Segment 2	9	0.9	7	0.7	2	0.2	0	0	0
3 - Segment 3	86	1	48	0.727	18	0.273	0	8	12
4 - Segment 4	30	1	15	0.789	4	0.211	0	7	4
5 - Segment 5	98	1	42	0.656	22	0.344	0	13	21
6 - Segment 6	52	1	28	0.683	13	0.317	0	4	7
7 - Segment 7	0	0	0	0	0	0	0	0	0
8 - Segment 8	4	0.3	3	0.3	0	0	0	0	1
9 - Segment 9	3	0.2	2	0.2	0	0	0	0	1
10 - Segment 10	8	0.7	6	0.6	1	0.1	0	1	0
Totals	**396**	**7.1**	**208**	**5.35**	**85**	**1.75**	**0**	**41**	**62**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Negative	SUPPORTS THIRD PARTY COMMENTS
1	American Electric Power	Paul B Johnson		
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Negative	COMMENT RECEIVED
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Negative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel		
1	Colorado Springs Utilities	Paul Morland	Negative	SUPPORTS THIRD PARTY COMMENTS - FMPA
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	El Paso Electric Company	Pablo Onate	Abstain	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Abstain	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Hydro One Networks, Inc.	Ajay Garg		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JDRJC Associates	Jim D Cyrulewski	Negative	SUPPORTS THIRD PARTY COMMENTS
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Jennifer Flandermeyer		
1	Lakeland Electric	Larry E Watt	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Long Island Power Authority	Robert Ganley		
1	Los Angeles Department of Water & Power	John Burnett		
1	Lower Colorado River Authority	Martyn Turner	Negative	

1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger	Negative	SUPPORTS THIRD PARTY COMMENTS
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	SUPPORTS THIRD PARTY COMMENTS
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	SUPPORTS THIRD PARTY COMMENTS
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Oncor Electric Delivery	Jen Fiegel		
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Abstain	
1	Otter Tail Power Company	Daryl Hanson	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Abstain	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Abstain	
1	SaskPower	Wayne Guttormson		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Abstain	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Texas Municipal Power Agency	Brent J Hebert		
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Western Area Power Administration	Lloyd A Linke	Negative	COMMENT RECEIVED
				SUPPORTS

1	Xcel Energy, Inc.	Gregory L Pieper	Negative	THIRD PARTY COMMENTS
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Negative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Negative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Services	Mark Peters		
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blue Ridge Electric	James L Layton		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	SUPPORTS THIRD PARTY COMMENTS
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS
3	City of Farmington	Linda R Jacobson		
3	City of Garland	Ronnie C Hoeinghaus	Negative	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Negative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley		
3	Colorado Springs Utilities	Charles Morgan	Negative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Negative	COMMENT RECEIVED
3	CPS Energy	Jose Escamilla	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	Entergy	Joel T Plessinger		
3	FirstEnergy Corp.	Cindy E Stewart	Abstain	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia System Operations Corporation	Scott McGough	Abstain	
3	Great River Energy	Brian Glover	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Hydro One Networks, Inc.	David Kiguel	Abstain	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke		
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Lakeland Electric	Mace D Hunter	Negative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Abstain	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
				SUPPORTS

3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	THIRD PARTY COMMENTS
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	SUPPORTS THIRD PARTY COMMENTS
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	David R Rivera	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Abstain	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-County Electric Cooperative, Inc.	Mike Swearingen	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache		
4	City of Clewiston	Kevin McCarthy		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell	Affirmative	
4	Consumers Energy Company	Tracy Goble	Negative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Abstain	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Cairo Vanegas	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Georgia System Operations Corporation	Guy Andrews	Abstain	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	

4	Modesto Irrigation District	Spencer Tacke		
4	Ohio Edison Company	Douglas Hohlbaugh	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	Amerenue	Sam Dwyer	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Arizona Public Service Co.	Scott Takinen	Negative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Abstain	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Negative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman		
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Negative	SUPPORTS THIRD PARTY COMMENTS - FMPA
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Detroit Edison Company	Alexander Eizans	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Negative	
5	Dynegy Inc.	Dan Roethemeyer	Abstain	- (SERC OC)
5	El Paso Electric Company	Gustavo Estrada		
5	Electric Power Supply Association	John R Cashin		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Essential Power, LLC	Patrick Brown		
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Abstain	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Hydro-Québec Production	Roger Dufresne	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lafayette Utilities System	Jamie B Webb	Affirmative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	

5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Karin Schweitzer	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Abstain	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing		
5	Nebraska Public Power District	Don Schmit	Negative	SUPPORTS THIRD PARTY COMMENTS
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	NiSource	Huston Ferguson		
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Occidental Chemical	Michelle R DAntuono		
5	Oglethorpe Power Corporation	Bernard Johnson		
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Abstain	
5	PacifiCorp	Bonnie Marino-Blair	Negative	COMMENT RECEIVED
5	Pattern Gulf Wind LLC	Grit Schmieder-Copeland		
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Abstain	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Public Utility District No. 1 of Chelan County	John Yale		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Raven Power	Scott A Etnoyer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Feather Power Project	Kathryn Zancanella	Affirmative	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State G & T Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	SUPPORTS THIRD PARTY COMMENTS
5	USDI Bureau of Reclamation	Erika Doot	Negative	
5	Utility System Effeciencies, Inc. (USE)	Robert L Dintelman	Negative	
5	Vandolah Power Company L.L.C.	Douglas A. Jensen	Abstain	
5	Westar Energy	Bryan Taggart	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Western Farmers Electric Coop.	Clem Cassmeyer		
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Negative	SUPPORTS THIRD PARTY COMMENTS

6	AEP Marketing	Edward P. Cox		
6	Ameren Energy Marketing Co.	Jennifer Richardson		
6	APS	Randy A. Young	Negative	COMMENT RECEIVED
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak		
6	Colorado Springs Utilities	Shannon Fair	Negative	COMMENT RECEIVED
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Negative	SUPPORTS THIRD PARTY COMMENTS
6	FirstEnergy Solutions	Kevin Querry	Abstain	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brenda Hampton	Abstain	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley		
6	New York Power Authority	Saul Rojas	Affirmative	
6	Northern California Power Agency	Steve C Hill	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson		
6	Oklahoma Gas & Electric Services	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Negative	SUPPORTS THIRD PARTY COMMENTS
6	PacifiCorp	Kelly Cumiskey	Negative	COMMENT RECEIVED
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	Southern California Edison Company	Lujuanna Medina		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Wisconsin Public Service Corp.	David Hathaway	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Negative	SUPPORTS THIRD PARTY COMMENTS
8		Edward C Stein		
8		Roger C Zaklukiewicz	Affirmative	

8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney		
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	COMMENT RECEIVED
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR and supporting package posted for comment on July 19, 2013.
2. Draft standard posted for initial comments and ballot from July 19, 2013 to September 3, 2013.
3. Draft standard posted for additional comments and ballot from October 11, 2013 to November 26, 2013.

Description of Current Draft

This is the third posting of the proposed draft standard. This proposed draft standard will be posted for a 45-day formal comment period and parallel ballot.

Anticipated Actions	Anticipated Date
Additional 45-Day SAR Comment Period with Ballot	February/March
Final Ballot	April 2014
NERC Board of Trustees Adoption	May 2014
Filing to Applicable Regulatory Authorities	May 2014

Version History

Version	Date	Action	Change Tracking
1	5/1/2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and 2.4.3.	July 5, 2006
1a	12/19/2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	1/16/2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	Errata
1.1a	10/29/2008	BOT adopted errata changes; updated version number to "1.1a"	Errata
1.1b	3/3/2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	Revised
2b	4/16/2013	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4. FERC Order issued approving VAR-002-2b.	Revised

Definitions of Terms Used in the Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None.

A. Introduction

1. Title: **Generator Operation for Maintaining Network Voltage Schedules**

2. Number: VAR-002-3

3. Purpose: To ensure generators provide reactive support and voltage control, within generating Facility capabilities, in order to protect equipment and maintain reliable operation of the Interconnection.

4. Applicability:

4.1. Generator Operator

4.2. Generator Owner

5. Effective Dates

The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

Rationale for R1: This requirement has been maintained due to the importance of running a unit with its automatic voltage regulator (AVR) in service and in either voltage controlling mode or the mode instructed by the TOP. However, the requirement has been modified to allow for testing, and the measure has been updated to include some of the evidence that can be used for compliance purposes.

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode, as instructed by the Transmission Operator unless: 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- That the generator is being operated in start-up,[1] shutdown,[2] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in the control mode that was instructed by the Transmission Operatorfor a reason other than start-up, shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If a generator is exempted, the Generator Operator shall also have evidence that the generator is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.
[2] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

Rationale for R2:

Requirement R2 details how a Generator Operator (GOP) operates its generator(s) to provide voltage support and when the GOP is expected to notify the Transmission Operator (TOP). In an effort to remove prescriptive notification requirements for the entire continent, the VAR-002-3 standard drafting team (SDT) opted to allow each TOP to determine the notification requirements for each of its respective GOPs based on system requirements. Additionally, a new part 2.3 has been added to detail that each GOP may monitor voltage by using its existing facility equipment.

Conversion Methodology: There are many ways to convert the voltage schedule from one voltage level to another. Some entities may choose to develop voltage regulation curves for their transformers; others may choose to do a straight ratio conversion; others may choose an entirely different methodology. All of these methods have technical challenges, but the studies performed by the TOP, which consider N-1 and credible N-2 contingencies, should compensate for the error introduced by these methodologies, and the TOP possesses the authority to direct the GOP to modify its output if its performance is not satisfactory. During a significant system event, such as a voltage collapse, even a generation unit in automatic voltage control that controls based on the low-side of the generator step-up transformer should see the event on the low-side of the generator step-up transformer and respond accordingly.

Voltage Schedule Tolerances: The bandwidth that accompanies the voltage target in a voltage schedule should reflect the anticipated fluctuation in voltage at the GOP's Facility during normal operations and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a GOP's AVR control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within each generating Facility's capabilities[4]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

[3] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.

[4] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a generator is operating in manual control, reactive power capability may change based on stability considerations.

2.2. When instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage or Reactive Power schedule.

For part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

For part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's instructions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the instruction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For part 2.3, for Generator Operators that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall document or be able to demonstrate the method of conversion from the voltage level monitored to the voltage level specified on the voltage schedule.

Rationale for R3:

This requirement has been modified to limit the notifications required when an AVR goes out of service and quickly comes back in service. Such notifications provide little to no benefit to reliability. Thirty (30) minutes have been built into the requirement to allow a GOP time to resolve an issue before having to notify the TOP of a status or capability change. The requirement has also been amended to remove the sub-requirement to provide an estimate for the expected duration of the status change. The 30-minute window should resolve most issues.

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the

change. If the status has been restored within 30 minutes of such change, then to the Generator Operator is not required to notify the Transmission Operator of the status change *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any status change identified in Requirement R3. If the status has been restored within the first 30 minutes, no notification is necessary.

Rationale for R4:

This requirement has been bifurcated from the prior version VAR-00202b Requirement R3. This requirement allows GOPs to report reactive capability changes after they are made aware of the change. The current standard requires notification as soon as the change occurs, but many GOPs are not aware of a reactive capability change until it has taken place.

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within 30 minutes of such change, then to the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability in accordance with Requirement R4. If the capability has been restored within the first 30 minutes, no notification is necessary.

Rationale for R5:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected. The prior version of VAR-002-2b subpart 4.1.4 (the +/- voltage range with step-change in % for load-tap changing transformers) has been removed. The percentage information was not needed because the tap settings, ranges and impedance are required. Those inputs can be used to calculate the step-change percentage if needed.

R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

5.1. For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

5.1.1. Tap settings.

5.1.2. Available fixed tap ranges.

5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirement R5 part 5.1.1 through part 5.1.3 within 30 calendar days.

Rationale for R6:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected.

R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

6.1. If the Generator Owner cannot comply with the Transmission Operator's specifications, the Generator Owner shall notify the Transmission Operator and shall provide the technical justification.

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation in accordance with Requirement R6. The Generator Owner shall have evidence that it notified its associated Transmission Operator when it could not comply with the Transmission Operator's step-up transformer tap specifications in accordance with Requirement R6 part 6.1.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. The Generator Operator shall maintain all other evidence for the current and previous calendar year.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Real-time Operations**	**Medium**	N/A	N/A	N/A	Unless exempted, the Generator Operator did not operate each generator in the automatic voltage control mode or in a different control mode, as instructed by the Transmission Operator, and failed to provide the required notifications to Transmission Operator as identified in Requirement R1.
R2	**Real-time Operations**	**Medium**	N/A	N/A	The Generator Operator did not have conversion methodology when it monitors voltage at a location different from the schedule provided by the Transmission Operator.	The Generator Operator did not maintain voltage or Reactive Power schedule as directed by the Transmission Operator and did not make the necessary notifications required by the Transmission Operator. OR The Generator Operator did not have an operating AVR, and the responsible entity did not use an alternative method for controlling voltage. OR The Generator Operator did not modify voltage when directed, and the responsible entity did not provide any explanation.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes.
R4	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes.
R5	**Real-time Operations**	**Lower**	N/A	N/A	The Generator Operator failed to provide its associated Transmission Operator and Transmission Planner one of the types of data specified in Requirement R5 parts 5.1.1, 5.1.2, and 5.1.3.	The Generator Operator failed to provide to its associated Transmission Operator and Transmission Planner two or more of the types of data specified in Requirement R5 parts 5.1.1, 5.1.2, and 5.1.3.
R6	**Real-time Operations**	**Lower**	N/A	N/A	N/A	The Generator Owner did not ensure the tap changes were made according the Transmission Operator's specifications. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Generator Owner failed to perform the tap changes, and the Generator Owner did not provide technical justification for why it cannot comply with the Transmission Operator specifications.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR and supporting package posted for comment on July 19, 2013.
2. Draft standard posted for initial comments and ballot from July 19, 2013 to September 3, 2013.
3. Draft standard posted for additional comments and ballot from October 11, 2013 to November 26, 2013.

Description of Current Draft

This is the ~~second~~ third posting of the proposed draft standard. This proposed draft standard will be posted for a 45-day formal comment period and parallel ballot.

Anticipated Actions	Anticipated Date
Additional 45-Day SAR Comment Period with Ballot	~~October/November 2013~~February/March
Final Ballot	~~December 2013~~April 2014
NERC Board of Trustees Adoption	~~December 2013~~May 2014
Filing to Applicable Regulatory Authorities	~~December 2013~~May 2014

Version History

Version	Date	Action	Change Tracking
1	5/1/2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and 2.4.3.	July 5, 2006
1a	12/19/2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	1/16/2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	Errata
1.1a	10/29/2008	BOT adopted errata changes; updated version number to "1.1a"	Errata
1.1b	3/3/2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	Revised
2b	4/16/2013	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4. FERC Order issued approving VAR-002-2b.	Revised

Definitions of Terms Used in the Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None.

A. Introduction

1. Title: **Generator Operation for Maintaining Network Voltage Schedules**

2. Number: VAR-002-3

3. Purpose: To ensure generators provide reactive support and voltage control, within generating Facility capabilities, in order to protect equipment and maintain reliable operation of the Interconnection.

4. Applicability:

4.1. Generator Operator

4.2. Generator Owner

5. Effective Dates

The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

Rationale for R1: This requirement has been maintained due to the importance of running a unit with its automatic voltage regulator (AVR) in service and in either voltage controlling mode or the mode instructed by the TOP. However, the requirement has been modified to allow for testing, and the measure has been updated to include some of the evidence that can be used for compliance purposes.

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode, as instructed by the Transmission Operator unless ~~the Generator Operator~~: 1) the generator is exempted by the Transmission Operator, ~~-~~or 2) the Generator Operator has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- That the generator is being operated in start-up,[1] shutdown,[2] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in the ~~automatic voltage~~ control mode that was instructed by the Transmission Operator ~~-~~for a reason other than start-up, shutdown, or ~~-~~ testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence ~~must~~ may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If a generator is exempted, the Generator Operator shall also have evidence that the generator ~~it~~ is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.
[2] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

Rationale for R2:

Requirement R2 details how a Generator Operator (GOP) operates ~~the~~ its generator(s) ~~system~~ to ~~maintain~~ provide ~~a~~ voltage ~~schedule~~ support and when the GOP is expected to notify the Transmission Operator (TOP). In an effort to remove prescriptive notification requirements for the entire continent, the VAR-002-3 standard drafting team (SDT) opted to allow each TOP to determine the notification requirements for each of its respective GOPs based on system requirements. Additionally, a new part 2.3 has been added to detail that each GOP ~~shall~~ may monitor voltage ~~based~~ by using ~~on~~ its existing facility equipment.

Conversion Methodology: There are many ways to convert the voltage schedule from one voltage level to another. Some entities may choose to develop voltage regulation curves for their transformers; others may choose to do a straight ratio conversion; others may choose an entirely different methodology. All of these methods have technical challenges, but the studies performed by the TOP, which consider N-1 and credible N-2 contingencies, should compensate for the error introduced by these methodologies, and the TOP possesses the authority to direct the GOP to modify its output if its performance is not satisfactory. During a significant system event, such as a voltage collapse, even a generation unit in automatic voltage control that controls based on the low-side of the generator step-up transformer should see the event on the low-side of the generator step-up transformer and respond accordingly.

Voltage Schedule Tolerances: The bandwidth that accompanies the voltage target in a voltage schedule should reflect the anticipated fluctuation in voltage at the GOP's Facility during normal operations and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a GOP's AVR control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within each generating Facility's capabilities[4]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule ~~directed~~ provided by the Transmission Operator.

[3] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.

[4] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a ~~Generator~~ generator is operating in manual control, reactive power capability may change based on stability considerations.

2.2. When ~~directed~~ instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a ~~unit~~ generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage or Reactive Power schedule.

For part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule ~~directed~~ provided by the Transmission Operator.

For part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's ~~directions~~ instructions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the ~~direction~~instruction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For part 2.3, for ~~units~~ Generator Operators that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall document or be able to demonstrate the method of conversion from the voltage level monitored to the voltage level specified on the voltage schedule.

Rationale for R3:

This requirement has been modified to limit the notifications required when an AVR goes out of service and quickly comes back in service. Such notifications provide~~d~~ little to no benefit to reliability. ~~Fifteen~~ Thirty (~~15~~30) minutes have been built into the requirement to allow a GOP time to resolve an issue before having to notify the TOP of a status or capability change. The requirement has also been amended to remove the sub-requirement to provide an estimate for the expected duration of the status change. The 30~~15~~-minute window should resolve most issues.

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the

change. If the status has been restored within ~~the first 15~~ 30 minutes of such change, then ~~there is no need to~~to the Generator Operator is not required to notify the Transmission Operator of the status change~~.~~ *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of ~~the~~ any status change identified in Requirement R3. If the status has been restored within the first ~~15~~ 30 minutes, no notification is necessary~~; therefore, if a status change lasts more than 15 minutes, the GOP must notify its associated Transmission Operator within 30 minutes of when the change first occurred~~.

Rationale for R4:

This requirement has been bifurcated from the ~~earlier~~ prior version VAR-00202b Requirement R3. This requirement allows GOPs to report reactive capability changes after they are made aware of the change. The current standard requires notification as soon as the change occurs, but many GOPs ~~are already in non-compliance situations by the time it is known that~~are not aware of a reactive capability change until it has taken place.

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes ~~after~~ of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within ~~the first 15~~ 30 minutes of such change, then ~~there is no need to~~to the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes ~~of the recognition~~ of becoming aware of a change in reactive capability ~~change identified~~ in accordance with Requirement R4. If the capability has been restored within the first ~~15~~ 30 minutes, no notification is necessary~~; therefore, if a capability change lasts more than 15 minutes, the Generator Operator must notify its associated Transmission Operator within 30 minutes of when the change first occurred~~.

Rationale for R5:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the ~~amount of~~ VARs ~~produced by a~~ available from that unit can be affected. The ~~original~~ prior version of VAR-002-2b sub~~-requirement~~part 4.1.4 (the +/- voltage range with step-change in % for load-tap changing transformers) has been removed. The percentage information was not needed ~~since~~ because the tap settings, ranges and impedance are required. Those inputs can be used to calculate the step-change percentage if needed.

R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

5.1. For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

5.1.1. Tap settings.

5.1.2. Available fixed tap ranges.

5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirement~~s~~ R5 part 5.1.1 through part 5.1.3 within 30 calendar days.

Rationale for R6:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the ~~amount of~~ VARs ~~produced by~~ available from that ~~a~~ unit can be affected.

R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

6.1. If the Generator ~~Operator~~ Owner cannot comply with the Transmission Operator's specifications, the Generator ~~Operator~~ Owner shall notify the Transmission Operator and shall provide the technical justification.

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation ~~as identified~~ in accordance with Requirement R6. The Generator ~~Operator~~ Owner shall have evidence that it notified its associated Transmission

Operator when it could not comply with the Transmission Operator's step-up transformer tap specifications ~~as identified~~ in accordance with Requirement R6 part 6.1.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. The Generator Operator shall maintain all other evidence for the current and previous calendar year.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

~~As defined in the NERC Rules of Procedure, "Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.~~

1.4. Additional Compliance Information:

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Real-time Operations**	**Medium**	N/A	N/A	N/A	Unless exempted, the ~~responsible entity~~Generator Operator did not operate each generator in the automatic voltage control mode or in a different control mode, as instructed by the Transmission Operator, and failed to ~~notify~~ provide the required notifications to Transmission Operator as identified in Requirement R1.
R2	**Real-time Operations**	**Medium**	N/A	N/A	The ~~responsible entity~~Generator Operator did not have conversion methodology when it monitors voltage at a location different from the schedule provided by the Transmission Operator.	The Generator Operator ~~responsible entity~~ did not maintain voltage or Reactive Power schedule as directed by the Transmission Operator and did not make the necessary notifications required by the Transmission Operator. OR The Generator Operator ~~responsible entity~~ did not have an operating AVR, and the responsible entity did not use an alternative method for controlling voltage. OR The Generator Operator ~~responsible entity~~ did not modify voltage when directed, and the responsible entity did not provide any explanation.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator ~~responsible entity~~ did not make the required notification within 30 minutes.
R4	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator ~~responsible entity~~ did not make the required notification within 30 minutes.
R5	**Real-time Operations**	**Lower**	N/A	N/A	The Generator Operator ~~responsible entity~~ failed to provide ~~to~~ its associated Transmission Operator and Transmission Planner one of the types of data specified in Requirement~~s~~ R5 parts 5.1.1 ~~and~~ , 5.1.2, and 5.1.3.	The Generator Operator ~~responsible entity~~ failed to provide to its associated Transmission Operator and Transmission Planner two or more of the types of data specified in Requirement~~s~~ R5 parts 5.1.1, ~~and~~ 5.1.2, and 5.1.3.
R6	**Real-time Operations**	**Lower**	N/A	N/A	N/A	The Generator Owner did not ensure the tap changes were made according the Transmission Operator's specifications.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Generator ~~Operator~~ Owner failed to perform the tap changes, and the Generator ~~Operator~~ Owner did not provide technical justification for why it cannot comply with the Transmission Operator ~~directive~~specifications.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

VAR Directives Project

Implementation Plan for VAR-001-4 and VAR-002-3

Approvals Required

VAR-001-4 – Voltage and Reactive Control
VAR-002-3 — Generator Operation for Maintaining Network Voltage Schedules

Prerequisite Approvals

There are no other standards that must receive approval prior to the approval of this standard.

Revisions to Glossary Terms

None

Applicable Entities

Generator Operators (VAR-002-3)

Generator Owners (VAR-002-3)

Transmission Operators (VAR-001-4)

Applicable Facilities

N/A

Conforming Changes to Other Standards

None

Effective Dates

VAR-001-4 and VAR-002-3 – All requirements shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-001-4 and VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Justification

The currently effective VAR-002 standard is one of the most violated standards; however, the industry argues these violations do not address any reliability gaps. Instead, Generator Operators and Transmission Operators are required to handle many nuisance phone calls for slight deviations from a voltage schedule. The nuisance phone calls can be a distraction during a scheduled maintenance or a system event; thus, the industry would support making the changes as soon as possible. However, since VAR-001 now requires determining voltage and reactive power schedules with associated tolerance bands in addition to any notification requirements, the Transmission Operators need a quarter to prepare documentation. The VAR-002 standards cannot go into effect without the new TOP schedules and notification requirements. Also for Transmission Operators that do not already provide tolerance bands with voltage schedules, those Transmission Operators will need some time to adjust to providing new data (more specifically, the criteria for schedules) to Generator Operators.

Retirements

VAR-001-3 and VAR-002-2b will be retired at midnight of the day immediately prior to the Effective Date of VAR-001-4 and VAR-002-3 in the particular jurisdiction in which the new standards are becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

VAR Directives Project

Implementation Plan for VAR-001 and VAR-002

Approvals Required

VAR-001-4 – Voltage and Reactive Control
VAR-002-3 — Generator Operation for Maintaining Network Voltage Schedules

Prerequisite Approvals

There are no other standards that must receive approval prior to the approval of this standard.

Revisions to Glossary Terms

None

Applicable Entities

Generator Operators (VAR-002-3)

Generator Owners (VAR-002-3)

Transmission Operators (VAR-001-4)

~~Reliability Coordinators~~

Applicable Facilities

N/A

Conforming Changes to Other Standards

None

Effective Dates

VAR-001-4 and VAR-002-3 – All requirements ~~- In those jurisdictions where regulatory approval is required, this standard~~ shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority ~~regulatory approval~~ or as otherwise provided for in a jurisdiction where approval by an~~made effective pursuant to the laws~~ applicable ~~to such ERO~~ governmental authority~~authorities. In those jurisdictions where no regulatory approval~~ is required for a~~, this~~ standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-001-4 and VAR-002-3 shall become effective on the first

day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction~~approval~~.

Justification

The currently effective VAR-002 standard is one of the most violated standards; however, the industry argues these violations do not address any reliability gaps. Instead, Generator Operators and Transmission Operators are required to handle many nuisance phone calls for slight deviations from a voltage schedule. The nuisance phone calls can be a distraction during a scheduled maintenance or a system event; thus, the industry would support making the changes as soon as possible. However, since VAR-001 now requires determining voltage and reactive power schedules with associated tolerance bands in addition to any notification requirements~~a documented policy or procedure for assessments~~,~~;~~ the Transmission Operators need a quarter to prepare documentation. The VAR-002 standards cannot go into effect without the new TOP schedules and notification requirements. Also for Transmission Operators that do not already provide tolerance bands with voltage schedules, those Transmission Operators will need some time to adjust to providing new data (more specifically, the criteria for schedules) to Generator Operators.

Retirements

VAR-001-3 and VAR-002-2b will be retired at midnight of the day immediately prior to the Effective Date of VAR-001-4 and VAR-002-3 in the particular j~~J~~urisdiction in which the new standards are becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2013-04 Voltage and Reactive Control (VAR) Revisions

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments on the draft VAR-002-3 standard. The electronic comment form must be completed by 8:00 p.m. ET by **April 14, 2014**.

If you have questions please contact Soo Jin Kim via email or by telephone at 404-446-9742.

The project page may be accessed by clicking here.

Background Information

When the first versions of the VAR standards were approved in FERC Order No. 693,[1] the Commission also issued FERC issued several directives with regard to how to improve the standard. Each of the outstanding directives are explained in detail in the technical white paper (see project page).

The informal consensus building for VAR began in February 2013. Specifically, the ad hoc group engaged stakeholders on how best to address the FERC directives, remove paragraph 81 candidates, and implement results-based approaches. A discussion of the ad hoc group's consensus building and collaborative activities are also included in the technical white paper.

Project 2013-04 posted an initial draft for comment and ballot from July 19, 2013 to September 3, 2013. Although the VAR standards did not pass, the industry provided numerous helpful coments, and the standard drafting team made significant revisions based on the stakeholder input. Both VAR-001 and VAR-002 were posted for another comment and ballot from October 11, 2013 to November 26, 2013. VAR-001 successfully passed, but VAR-002 did not receive the necessary votes. This posting is now soliciting comment on the revised VAR-002 standard.

Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

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

Question

1. Please provide your comments on the proposed VAR-002-3 below:

Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Operations

Draft Reliability Standard Compliance Guidance for VAR-001-4 and VAR-002-3
October 21, 2013

Introduction

The NERC Compliance department (Compliance) worked with the VAR standard drafting team (SDT) to review the proposed standards VAR-001-4 and VAR-002-3. The purpose of the review was to discuss the requirements of the proposed standard to obtain an understanding of its intended purpose and the evidence necessary to support compliance. The purpose of this document is to address specific questions posed by the VAR SDT in order to aid in the drafting of the requirements and provide a level of understanding regarding evidentiary support necessary to demonstrate compliance.

While all compliance evaluations require levels of auditor judgment, participating in these reviews allows Compliance to develop training and approaches to support a high level of consistency in audits conducted by the Regional Entities. The following questions and answers are intended to assist the SDT in further refining the standard and to serve as a resource in the development of training for auditors.

VAR-001 and VAR-002 Questions

Question 1

How will compliance determine if sufficient reactive resources were scheduled as part of VAR-001-4 Requirement R2?

Compliance Response to Question 1

For VAR-001-4 Requirement R2, an auditor would review the studies that a TOP used to schedule resources to see that the studies show whether new resources should be brought online, or if the resources online are sufficient to regulate voltage levels. An auditor may observe a TOP reviewing the study and scheduling live and may pull samples from various time periods to determine whether a TOP scheduled resources as required in the study.

Question 2

Is it clear that VAR-001-4 Requirement R4 allows for exemptions, for any duration, from: 1) voltage schedules, 2) being in automatic voltage control mode, or 3) any notification requirements?

Compliance Response to Question

It is clear that VAR-001 Requirement R4 allows for any combination of exemptions for generator operators from 1) voltage schedules, 2) being in automatic voltage control mode, or 3) any notification requirements, as long as the

exemption meets the criteria specified by the TOP. An auditor will not look for any pre-authorization from the TOP; rather an auditor will verify that the generator operator has met the criteria set forth by the TOP.

Question 3

Tolerance bands apply to a set voltage or Reactive Power number with a +/- percentage as the tolerance band. The voltage range or Reactive Power range is a high and low number that a Generator Operator is expected to operate within for reliability purposes. With regard to VAR-001-4 Requirement R5, is it clear that when a voltage range or Reactive Power range is provided as a schedule, a tolerance band is not expected to also be provided?

Compliance Response to Question 3

Yes, it is clear based on VAR-001-4 Requirement R5 that a voltage or Reactive power schedule can be either: 1) a target number with a tolerance band, OR 2) a voltage or Reactive Power range to operate within. An auditor would not expect to see a tolerance band provided with an operating range for voltage or Reactive Power.

Question 4

With regard to VAR-002-3, will generators receive a violation for instances where a system event is affecting system voltage, but the generators made the appropriate conversions and set the AVRs to meet the original schedule provided by the TOP?

Compliance Response to Question 4

No, the generator operators can only be responsible for maintaining the schedule provided by the TOP based on existing facility equipment. In the event that a generator operator does not have the equipment to have visibility of high-side system voltage, the GOP will not have the ability to adjust VARs to maintain system voltage. An auditor is not to determine that, where the GOP does not have the high side monitoring equipment and where the AVR is set appropriately based on existing facility equipment, the generator operator is non-compliant. However, if the TOP provides a new directive or schedule, the GOP is required to follow the new directive. This directive can include modifying an AVR setting or providing more voltage support, and the generator operator is expected to comply pursuant to VAR-002-3.

Question 5

Related to VAR-002-3, generators can monitor voltage on either the low side and high side of the GSU (depending on equipment limitation) and the “number” being monitored by the Generator will not always equate to the number provided by the TOP. Is it clear that VAR-002 Requirement R2, part 2.3 only wants a conversion of the schedule provided to the number monitored? Is it clear that there should not be a violation if the schedule does not match the number being monitored on the low side as long as there is a documented conversion?

Compliance Response to Question 5

The Generator should be able to provide documentation that identifies the "number" being monitored and the calculation demonstrating how the "number" equates to the schedule provided by the TOP. The measure for VAR-002-3 Requirement R2, part 2.3 is clear on what evidence should be able to demonstrate this during an audit.

Question 6

VAR-002-3, Requirement R4 was added because generators cannot report a capability change until they are aware of the change. The currently enforceable standard requires a notification as soon as the capability change occurs; however, many times the change occurred well before the generators were aware of the problem. Is it clear that VAR-002-3 Requirement R4 is only violated after the generator is made aware of the change?

Compliance Response to Question 6

It is clear that VAR-002-3, Requirement R4 will only be a violation if the change is not reported after 30 minutes of becoming aware of the reactive capability change. An auditor will ask an entity for evidence to demonstrate when it became aware of the change in reactive capability. This will not be purely subjective; there are technical instances where it will be clear that an entity would have been made aware of the change in reactive capability. For example, one instance is where a unit is ramping to an expected VAR output, and it cannot reach it; a reactive capability change has occurred.

Conclusion

Following final approval of the Reliability Standard, Compliance will develop the final Reliability Standards Auditor Worksheet (RSAW) and associated training.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VAR-002 Mapping Document

Transition of VAR-002-2b

Standard: VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b, R1	Requirement R1	The requirement has been modified to allow for testing and exemptions for other AVR modes when necessary. This requirement was also modified to allow GOPs to operate in a different control mode as instructed by the TOP.
VAR-002-2b, R2	Requirement R2	The new requirement has been updated to allow for the TOP to define notification requirements. The requirement also adds parts to allow for the conversion of a high side schedule to a low side number for monitoring purposes. Reactive Power schedules have been added for generators that use those schedules, and for consistency purposes "unit" has been changed to "generator".

Standard: VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b, R3	Requirement R3 and R4.	The old requirement has been broken into two requirements: 1) one for AVR/PSS status, and 2) one for reactive capability. Both allow 30 minutes to correct an issue before having to notify the TOP.
VAR-002-2b, R3	Requirement R5	The requirement has been modified to remove the sub-part that requires the GOP to provide "[t]he +/- voltage range with step-change in % for load-tap changing transformers." The measure was also modified to add that a GOP must provide the data "within 30 calendar days"
VAR-002-2b, R4	Requirement R6	The requirement has been updated to apply to the same functional entity for the Requirement and sub-part.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VAR-002 Mapping Document

Transition of VAR-002-2b

Standard: VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b, R1	Requirement R1	The requirement has been modified to allow for testing and exemptions for other AVR modes when necessary. This requirement was also modified to allow GOPs to operate in a different control mode as instructed by the TOP.
VAR-002-2b, R2	Requirement R2	The new requirement has been updated to allow for the TOP to define notification requirements. The requirement also adds parts to allow for the conversion of a high side schedule to a low side number for monitoring purposes. Reactive Power schedules have been added for generators that use those schedules, and for consistency purposes "unit" has been changed to "generator".

Standard: VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b, R3	Requirement R3 and R4.	The old requirement has been broken into two requirements: 1) one for AVR/PSS status, and 2) one for reactive capability. Both allow ~~15~~ 30 minutes to correct an issue before having to notify the TOP.
VAR-002-2b, R3	Requirement R5	The requirement has ~~not been modified~~been modified to remove the sub-part that requires the GOP to provide "[t]he +/- voltage range with step-change in % for load-tap changing transformers." The measure was also modified to add that a GOP must provide the data "within 30 calendar days"~~.~~
VAR-002-2b, R4	Requirement R6	The requirement has ~~not been modified.~~been updated to apply to the same functional entity for the Requirement and sub-part.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Reliability Standard Audit Worksheet[1]

VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	Audit
Names of Auditors:	Supplied by CEA

Applicability of Requirements *[RSAW developer to insert correct applicability]*

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1				X											
R2				X											
R3				X											
R4				X											
R5			X												
R6			X												

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Subject Matter Experts

Identify Subject Matter Expert(s) responsible for this Reliability Standard. (Insert additional rows if necessary)

Registered Entity Response (Required):

SME Name	Title	Organization	Requirement(s)

DRAFT

R1 Supporting Evidence and Documentation

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode, as instructed by the Transmission Operator unless ~~the Generator Operator~~ 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following:

- That the generator is being operated in start-up,[3] shutdown,[4] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in the ~~automatic voltage~~ control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence ~~must~~ may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If a generator is exempted, the Generator Operator shall also have evidence that the generator ~~it~~ is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

Registered Entity Response to Question (Required):

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[5]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this

[3] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.
[4] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.
[5] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M1.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R1
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	For instances where entity did not operate a generator in automatic voltage control mode or in a different control mode, as instructed by the Transmission Operator, ensure notification was given to the Transmission Operator in accordance with Requirement R1.

Note to Auditor: Auditors can identify instances where entities did not operate~~d~~ generators ~~outside of~~in automatic voltage control mode, or in a different control mode, as instructed by the Transmission Operator, through their general knowledge of the interconnected transmission system in the entity's area. Auditor knowledge is obtained through activities such as conversations with the entity under audit or the Transmission Operator, and an awareness of events occurring on the interconnected transmission system. In situations where the entity's compliance with this requirement poses little risk to the BES, conversations with other entities, such as Transmission Operators, is most likely not necessary.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[6] (within each generating Facility's capabilities[7]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator.

2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule ~~directed~~ provided by the Transmission Operator.

2.2. When ~~directed~~ instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a ~~unit~~ generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage or Reactive Power schedule.

For part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule ~~directed~~ provided by the Transmission Operator.

For part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's ~~directions~~ instructions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the

[6] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.

[7] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a ~~Generator~~ generator is operating in manual control, reactive power capability may change based on stability considerations.

~~direction~~instruction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For part 2.3, for ~~units~~ Generator Operators that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall document or be able to demonstrate the method of conversion from the voltage level monitored to the voltage level specified on the voltage schedule.

Question: As a Generation Operator, have you operated the generator with the AVR out of service?

Registered Entity Response to Question (Required):

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[8]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M2.
Any written policies, procedures or protocols describing how the entity maintains the generator voltage or Reactive Power schedule provided by Transmission Operator, if the entity has such documents.
Generator voltage or Reactive Power schedule provided to entity by Transmission Operator, or entity's record thereof, for timeframes selected by the auditor.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

[8] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

Compliance Assessment Approach Specific to VAR-002-3, R2

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Interview entity staff and/or review documentation provided by the entity to understand how they maintain the generator voltage or Reactive Power schedule or authorized exemption per Requirement R2.
	Read entity's response to compliance Question above and understand how entity complies with Requirement R2, when they operate a generator with AVR in not in service.
	Select a sample of timeframes during the audit period and have entity walkthrough how they complied with Requirement R2 for those timeframes.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough timeframes, per above, to gain reasonable assurance that entity is complying with Requirement R2.

For part 2.3, the entity should be able to provide documentation that identifies the voltage number being monitored and the calculation demonstrating how it equates to the schedule provided by the Transmission Operator. The measure for VAR-002-3 Requirement R2, part 2.3 is clear on what evidence should be able to demonstrate this during an audit. The entity can only be responsible for maintaining the schedule provided by the Transmission Operator based on existing facility equipment. In the event that an entity does not have the equipment to have visibility of high-side system voltage, the entity will not have the ability to adjust VARs to maintain system voltage. An auditor is not to determine that, where the entity does not have the high side monitoring equipment and where the AVR is set appropriately based on existing facility equipment, the entity is non-compliant. However, if the Transmission Operator provides a new directive or schedule, the entity is required to follow the new directive. This directive can include modifying an AVR setting or providing more voltage support, and the entity is expected to comply pursuant to VAR-002-3.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within ~~the first 15~~30 minutes of such change, then the Generator Operator is not required to ~~there is no need to~~ notify the Transmission Operator of the status change.

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of ~~the~~ any status change identified in Requirement R3. If the status has been restored within the first ~~15~~ 30 minutes, no notification is necessary~~; therefore, if a status change lasts more than 15 minutes, the GOP must notify its associated Transmission Operator within 30 minutes of when the change first occurred~~.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[9]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
Any written policies, procedures or protocols describing how the entity responds to a status change on AVR, if the entity has such documents. An example of entity's response to a status change on AVR provided by entity, if applicable.
Auditor may select certain instances where entity had a status change on AVR. In such instances, provide associated evidence of awareness and resolution/notification.
Evidence as outlined in M3.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

[9] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

Compliance Assessment Approach Specific to VAR-002-3, R3
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Interview entity staff and/or review documentation provided by the entity to understand how they respond to status changes on AVR.
	Review evidence provided to determine if entity responded to status change on AVR in accordance with Requirement R3.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough timeframes, per above, to gain reasonable assurance that entity is complying with Requirement R3.

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes after becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within the first 15 minutes of such change, then there is no need to notify the Transmission Operator.

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of the recognition of a reactive capability change identified in Requirement R4. If the capability has been restored within the first 15 minutes, no notification is necessary; therefore, if a capability change lasts more than 15 minutes, the Generator Operator must notify its associated Transmission Operator within 30 minutes of when the change first occurred.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[10]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
Any written policies, procedures or protocols describing how the entity responds to a change in reactive capability, if the entity has such documents. An example of entity's response to a change in reactive capability provided by entity, if applicable.
Auditor may select certain instances where entity ~~should~~ may have been aware of a status change in reactive capability. In such instances, provide associated evidence of awareness and resolution/notification. See Note to Auditor for additional details.
Evidence as outlined in M4.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R4
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Interview entity staff and/or review documentation provided by the entity to understand how they respond to change in reactive capability.
	Review evidence provided to determine if entity responded to change in reactive capability in accordance with Requirement R4.
Note to Auditor: It is clear that VAR-002-3, Requirement R4 will only be a violation if the change is not reported after 30 minutes of becoming aware of the status change in reactive capability. An auditor will ask an entity for evidence to demonstrate when it became aware of the change. This will not be purely	

[10] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

subjective; there are technical instances (e.g. unit trips, ramping, equipment/AVR failures) where it ~~will be~~is ~~clear~~ likely that an entity ~~would have been~~was made aware of the change in reactive capability. ~~For example, one instance is where a unit is ramping to an expected VAR output, and it cannot reach it; a reactive capability change has occurred.~~

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request.

5.1. For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

5.1.1. Tap settings.

5.1.2. Available fixed tap ranges.

5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirements R5 part 5.1.1 through part 5.1.3.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[11]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
Evidence as outlined in M4. Evidence of transmittal of the data could include, but is not limited to, items such as an electronic message or a transmittal letter with the information included or attached.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted:

[11] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R5
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Review evidence (documented date of request and reply) to determine if entity responded to information request(s) as required in Requirement R5 within 30 days of receiving a request from associated Transmission Operator.
Note to Auditor: Based on the auditors professional judgment, he or she may confirm with Transmission Operators to determine if requests for data were made or simply confirm the existence of such requests with the entity under audit.	

Auditor Notes:

R6 Supporting Evidence and Documentation

R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement.

6.1. If the Generator Operator cannot comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation as identified in Requirement R6. The Generator Operator shall have evidence that it notified its associated Transmission Operator when it could not comply with the Transmission Operator's step-up transformer tap specifications as identified in Requirement R6 part 6.1.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[12]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M6.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R6
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Review evidence (documented date of request and response) to determine if entity responded to change(s) as required in Requirement R6.
Note to Auditor: Based on the auditors professional judgment, he or she may confirm with Transmission Operators to determine if requests for changes to transformer tap positions were made or simply confirm the existence of such requests with the entity under audit.	

[12] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

Auditor Notes:

Revision History

Version	Date	Reviewers	Revision Description
1	11/XX/2013	NERC Ceompliance, Standards	New Document
2	3/14/2014	NERC Compliance, Standards	Revisions based on changes to underlying Reliability Standard.

DRAFT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules

This document provides the Standard Drafting Team's (SDT) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project. A copy of the standard with the associated VRFs and VSLs is available here.

NERC Criteria - Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Violation Risk Factor Guidelines

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

The Commission seeks to ensure that Violation Risk Factors assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities

• Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

Guideline (3) – Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) –Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria - Violation Severity Levels

Violation Severity Levels (VSLs) define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

Violation severity levels should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

FERC's VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline 1 – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline 2 – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3 – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline 4 – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the

Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification – VAR-002-3 Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium is necessary because this requirement could affect the stability of the BES, but the requirement itself addresses instances where a GOP will not necessarily operate in with the AVR in different control modes or when the TOP will instruct a GOP to operate in other modes.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although the Blackout Report list Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, the GOP control modes are not as critical because the TOP is monitoring the system. The companion requirement to VAR-002-3 (in VAR-001-4) are properly designated with a HIGH VRF to ensure voltage schedules are provided as part of the TOPs plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The VRF applies to the entire requirement.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: Because maintaining a voltage schedule is critical to preventing a violation of a System Operating Limit, this VRF was drafted to be the same VRFs for VAR-001-4 Requirement R5. VAR-001-4 Requirement R5 requires the TOP to specify a schedule and notification requirements that the GOP must follow.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a GOP not operating in the proper control mode can affect the BES, but a single violation is unlikely to lead to instability, separation, or cascading failure. This is especially the case since a TOP will also be monitoring for voltage deviations.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More Than One Obligation:

	This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level.

VSL Justification – VAR-002-3 Requirement R1	
NERC VSL Guidelines	Consistent with NERC's VSL Guideline, this VSL acknowledges the criticality of this requirement and whether or not a system voltage schedule was created.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The current level of compliance is not lowered with the proposed VSL because this requirement only has a "severe" VSL.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary, and therefore, a single severe VSL is necessary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is consistent with the corresponding requirements.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on a cumulative number of violations.

VRF Justification – VAR-002-3 Requirement R2	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium is consistent with the NERC VRF definition. Requirement R2 focuses on GOPs maintaining a schedule, but there could be system events that will pull a GOP out of schedule. Also, late at night and early in the morning, the system may experience instances of low or high voltage. This could impact the BES, but a single instance is unlikely to lead to instability, separation, or cascading failure. The sub-requirements also require the GOP to modify the voltage schedule when directed by the TOP.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although the Blackout Report lists Reactive Power and voltage control as critical areas where a violation could severely affect the reliability of the Bulk-Power System, there are general times when a GOP will be unable to maintain a voltage schedule due to system condition. These instances occur frequently during the early morning and late at night. The companion requirement to VAR-002-3 (in VAR-001-4) are properly designated

	with a HIGH VRF to ensure voltage schedules are provided as part of the TOP's plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The VRF applies to the entire requirement, including all sub-parts.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: Because maintaining a voltage schedule is critical to preventing a violation of a System Operating Limit, this VRF was drafted to be the same VRFs for VAR-001-4 Requirement R5. VAR-001-4 Requirement R5 requires the TOP to specify a schedule and notification requirements that the GOP must follow.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a GOP not maintaining a schedule can affect the BES, but a single violation is unlikely to lead to instability, separation, or cascading failures. This is especially the case since a TOP will also be monitoring for voltage deviations
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation: This VRF does not co-mingle multiple objectives, nor does it water down the requirement to reflect a lower risk level.

VSL Justification – VAR-002-3 Requirement R2	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines, the VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering	There is no prior compliance obligation related to the subject of this standard.

the Current Level of Compliance	
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation,	The proposed VSL is not based on cumulative number of violations.

Not on A Cumulative Number of Violations	

VRF Justification – VAR-002-3 Requirement R3	
Proposed VRF	**Medium**
NERC VRF Discussion	This requirement warrants a Medium VRF and is consistent with the NERC definition because this requirement is whether the GOP made the required notifications to the TOP within the appropriate timeframes.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although the Blackout Report list Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, the GOP notifications are unlikely to lead to system instability, separation, or cascading failures. This is particularly the case because the TOP is still operating the system to stay within System Operating Limits and Interconnection Reliability Operating Limits.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: There is no sub-part to Requirement 3; therefore, the requirement is consistent.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: This VRF is drafted to be consistent with other standards (e.g., BAL) that address making appropriate notifications.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because not making the appropriate notifications can impact the grid, but the TOPs are still effectively monitoring the system; thus, instability, separation, or cascading failures are unlikely due to a single violation.
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level

VSL Justification – VAR-002-3 Requirement R3	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The current level of compliance is not lowered with the proposed VSL.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary because the standard is violated only when a notification is not made to the TOP; therefore, a severe VSL is warranted. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be	The proposed VSL is worded consistently with the corresponding requirement.

Consistent with the Corresponding Requirement	
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

VRF Justification – VAR-002-3 Requirement R4	
Proposed VRF	**Medium**
NERC VRF Discussion	This requirement warrants a Medium VRF and is consistent with the NERC definition because this requirement is whether the GOP made the required notifications to the TOP within the appropriate timeframes.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although the Blackout Report list Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, the GOP notifications are unlikely to lead to system instability, separation, or cascading failures. This is particularly the case because the TOP is still operating the system to stay within System Operating Limits and Interconnection Reliability Operating Limits.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: There is no sub-part to Requirement 3; therefore, the requirement is consistent.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: This VRF is drafted to be consistent with other standards (e.g., BAL) that address making appropriate notifications.

FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because not making the appropriate notifications can impact the grid, but the TOPs are still effectively monitoring the system; thus, instability, separation, or cascading failures are unlikely due to a single violation.
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level

VSL Justification – VAR-002-3 Requirement R4	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The current level of compliance is not lowered with the proposed VSL.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary because the standard is violated only when a notification is not made to the TOP; therefore, a severe VSL is warranted.

"Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

VRF Justification – VAR-002-3 Requirement R5	
Proposed VRF	**Lower**
NERC VRF Discussion	This requirement is a Lower VRF because the tap setting data does not change frequently, and a violation is not expected adversely affect the BES.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, this requirement would not adversely impact the BES

	if violated. The tap information is provided during interconnection, and it is not expected to change frequently. Therefore, a Lower VRF is warranted.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The parts within Requirement R5 are consistent with Requirement R5 and is considered a Lower VRF.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: There are no other standards that address Tap settings.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a violation is similar to an administrative violation. Further, since tap settings are infrequently changed, a violation would not adversely impact the BES.
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation: This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level.

VSL Justification – VAR-002-3 Requirement R5	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering	There is no prior compliance obligation related to the subject of this standard.

the Current Level of Compliance	
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation,	The proposed VSL is not based on cumulative number of violations.

Not on A Cumulative Number of Violations	

VRF Justification – VAR-002-3 Requirement R6	
Proposed VRF	**Lower**
NERC VRF Discussion	This requirement is a Lower VRF because the tap setting data does not change frequently, and a violation is not expected adversely affect the BES.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, this requirement would not adversely impact the BES if violated. The tap information is provided during interconnection, and it is not expected to change frequently. If a violation were to occur, the system would still operate at the level prior to making any tap setting changes. Therefore, a Lower VRF is warranted.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The part within Requirement R6 is consistent with Requirement R6 and is considered a Lower VRF.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: There are no other standards that address Tap settings.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a violation is similar to an administrative violation. Further, since tap settings are infrequently changed, a violation would not adversely impact the BES.
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation:

	This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level.

VSL Justification – VAR-002-3 Requirement R6	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary because the requirement focuses on whether tap changes were made. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-002-3

Comment Period Open Now Open through April 14, 2014

Upcoming:
Additional Ballot and Non-Binding Poll: April 4-14, 2014

Now Available

A comment period for **Project 2013-04 – Voltage and Reactive Control (VAR-002-3 - Generator Operation for Maintaining Network Voltage Schedules)** is open through **8 p.m. Eastern on Monday, April 14, 2014.**.

Background information for this project can be found on the project page.

Instructions

Please use the electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

An additional ballot of **VAR-002-3** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **April 4, 2014 through 8 p.m. Eastern on Monday, April 14, 2014**.

For more information on the Standards Development Process, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-002-3

Comment Period Open Now Open through April 14, 2014

Upcoming:
Additional Ballot and Non-Binding Poll: April 4-14, 2014

Now Available

A comment period for **Project 2013-04 – Voltage and Reactive Control (VAR-002-3 - Generator Operation for Maintaining Network Voltage Schedules)** is open through **8 p.m. Eastern on Monday, April 14, 2014.**.

Background information for this project can be found on the project page.

Instructions

Please use the electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

An additional ballot of **VAR-002-3** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **April 4, 2014 through 8 p.m. Eastern on Monday, April 14, 2014**.

For more information on the Standards Development Process, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-002-3

Additional Ballot and Non-Binding Poll Results

Now Available

An additional ballot for **VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels concluded at **8 p.m. Eastern on Wednesday, April 16, 2014.**

This standard achieved a quorum and sufficient affirmative votes for approval. Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results for the ballot.

Approval	Non-Binding Poll Results
Quorum: 78.03%	Quorum: 76.52%
Approval: 82.40%	Supportive Opinions: 79.09%

Background information for this project can be found on the project page.

Next Steps

The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the standard. If the standard does not show the need for significant revisions, it will proceed to a final ballot

For information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller (via email), Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results

Ballot Name:	Project 2013-04 Voltage and Reactive Control VAR-002-3
Ballot Period:	4/4/2014 - 4/16/2014
Ballot Type:	Additional
Total # Votes:	309
Total Ballot Pool:	396
Quorum:	**78.03 % The Quorum has been reached**
Weighted Segment Vote:	82.40 %
Ballot Results:	**The Ballot has Closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	106	1	58	0.817	13	0.183	0	9	26
2 - Segment 2	9	0.5	5	0.5	0	0	0	1	3
3 - Segment 3	86	1	54	0.818	12	0.182	0	2	18
4 - Segment 4	30	1	16	0.667	8	0.333	0	2	4
5 - Segment 5	98	1	48	0.75	16	0.25	1	6	27
6 - Segment 6	52	1	37	0.804	9	0.196	0	2	4
7 - Segment 7	0	0	0	0	0	0	0	0	0
8 - Segment 8	4	0.3	3	0.3	0	0	0	0	1
9 - Segment	3	0.2	2	0.2	0	0	0	0	1

9									
10 - Segment 10	8	0.5	5	0.5	0	0	0	0	3
Totals	**396**	**6.5**	**228**	**5.356**	**58**	**1.144**	**1**	**22**	**87**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Abstain	
1	Arizona Public Service Co.	Robert Smith	Negative	COMMENT RECEIVED
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton		
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Negative	COMMENT RECEIVED
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES Power Marketing)
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	SUPPORTS THIRD PARTY COMMENTS - (Keith Morisette)
1	City of Tallahassee	Daniel S Langston	Abstain	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Richard Castrejana		
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
1	El Paso Electric Company	Pablo Onate	Abstain	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)

1	Hydro One Networks, Inc.	Ajay Garg		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane		
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon		
1	Kansas City Power & Light Co.	Jennifer Flandermeyer	Affirmative	
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))
1	Lincoln Electric System	Doug Bantam		
1	Long Island Power Authority	Robert Ganley		
1	Los Angeles Department of Water & Power	John Burnett	Abstain	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Cole C Brodine		
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke		
1	NorthWestern Energy	John Canavan		
1	Ohio Valley Electric Corp.	Robert Mattey		
1	Oklahoma Gas and Electric Co.	Terri Pyle	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Abstain	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Abstain	
1	Otter Tail Power Company	Daryl Hanson		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams		
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments will be submitted by Public Service Enterprise Group)
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen		
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	SaskPower	Wayne Guttormson		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	

1	South Carolina Public Service Authority	Shawn T Abrams	Abstain	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Texas Municipal Power Agency	Brent J Hebert		
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine		
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Abstain	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman		
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington		
3	Blue Ridge Electric	James L Layton		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Association)
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
3	City of Farmington	Linda R Jacobson		
3	City of Garland	Ronnie C Hoeinghaus		
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	John Bee	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon / Exelon)

3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	CPS Energy	Jose Escamilla		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	Entergy	Joel T Plessinger	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	Supports FirstEnergy's comments
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Georgia System Operations Corporation	Scott McGough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Oglethorpe Power Corporation)
3	Great River Energy	Brian Glover	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
3	Hydro One Networks, Inc.	David Kiguel		
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
3	Lakeland Electric	Mace D Hunter	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Nebraska Public Power District comments.)
3	New York Power Authority	David R Rivera	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Abstain	
3	Old Dominion Electric Coop.	Bill Watson		
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz		
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service

				Enterprise Group)
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen		
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Negative	COMMENT RECEIVED
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-County Electric Cooperative, Inc.	Mike Swearingen		
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	SUPPORTS THIRD PARTY COMMENTS - (Barb Kedrowski)
3	Wisconsin Public Service Corp.	Gregory J Le Grave		
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith		
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support comments of Indiana and Florida Municipal Power Agencies (IMPA & FMPA))
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen		
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon / Exelon)
4	Consumers Energy Company	Tracy Goble		
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Fort Pierce Utilities Authority	Cairo Vanegas	Abstain	
4	Georgia System Operations Corporation	Guy Andrews	Negative	SUPPORTS THIRD PARTY COMMENTS - (Oglethorpe Power Corporation)
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (Frank Gaffney, FMPA)
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	

4	Modesto Irrigation District	Spencer Tacke	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	COMMENT RECEIVED
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	SUPPORTS THIRD PARTY COMMENTS - (Kedrowski for We Energies)
5	AEP Service Corp.	Brock Ondayko		
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Negative	SUPPORTS THIRD PARTY COMMENTS - (prior comments by AZPS)
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	Avista Corp.	Steve Wenke	Affirmative	
5	BC Hydro and Power Authority	Clement Ma		
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly		
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	NO COMMENT RECEIVED - (Jerry Farringer)
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Alexander Eizans	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	El Paso Electric Company	Gustavo Estrada	Abstain	
5	Electric Power Supply Association	John R Cashin		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Essential Power, LLC	Patrick Brown		
5	Exelon Nuclear	Mark F Draper	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris

				Scanlon / Exelon)
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Lafayette Utilities System	Jamie B Webb	Abstain	
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Karin Schweitzer		
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	COMMENT RECEIVED
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	NiSource	Huston Ferguson		
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Oklahoma Gas and Electric Co.	Henry L Staples	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Abstain	
5	PacifiCorp	Bonnie Marino-Blair		
5	Pattern Gulf Wind LLC	Grit Schmieder-Copeland		
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway		
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Negative	SUPPORTS THIRD PARTY COMMENTS - (comments will be submitted by Public Service Enterprise Group)
5	Public Utility District No. 1 of Chelan County	John Yale		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County,	Michiko Sell	Affirmative	

	Washington			
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Raven Power	Scott A Etnoyer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Keith Morisette)
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State G & T Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Utility System Effeciencies, Inc. (USE)	Robert L Dintelman		
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Western Farmers Electric Coop.	Clem Cassmeyer		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	SUPPORTS THIRD PARTY COMMENTS - (Barb Kedrowski)
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Negative	COMMENT RECEIVED
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Chris Scanlon / Exelon)
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Municipal Power Pool	Thomas Washburn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	

6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley	Affirmative	
6	New York Power Authority	Saul Rojas	Affirmative	
6	Northern California Power Agency	Steve C Hill	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson		
6	Oklahoma Gas & Electric Services	Jerry Nottnagel	Abstain	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Kelly Cumiskey	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	SUPPORTS THIRD PARTY COMMENTS - (Public Service Enterprise Group)
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet		
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	Southern California Edison Company	Lujuanna Medina	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Negative	SUPPORTS THIRD PARTY COMMENTS - (Keith Morisette)
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney		
6	Wisconsin Public Service Corp.	David Hathaway		
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Edward C Stein		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito		
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2014 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Non-Binding Poll Results

Project 2013-04 Voltage and Reactive Control (VAR) VAR-002-3

Non-Binding Poll Results	
Non-Binding Poll Name:	Project 2013-04 Voltage and Reactive Control VAR-002-3
Poll Period:	4/4/2014 - 4/16/2014
Total # Opinions:	277
Total Ballot Pool:	362
Ballot Results:	76.52% of those who registered to participate provided an opinion or abstention; 79.09% of those who provided an opinion indicated support for the VRFs and VSLs that were proposed.

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	Comments
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz - AEP)
1	Arizona Public Service Co.	Robert Smith	Negative	COMMENT RECEIVED
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton		
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Abstain	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES Power Marketing)
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	

1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	SUPPORTS THIRD PARTY COMMENTS - (Keith Morisette)
1	City of Tallahassee	Daniel S Langston	Abstain	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Richard Castrejana		
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Abstain	
1	Duke Energy Carolina	Doug E Hils	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
1	El Paso Electric Company	Pablo Onate	Abstain	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Richard Bachmeier	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Hydro One Networks, Inc.	Ajay Garg		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane		
1	JDRJC Associates	Jim D Cyrulewski	Abstain	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon		
1	Kansas City Power & Light Co.	Jennifer Flandermeyer	Affirmative	
1	Lakeland Electric	Larry E Watt	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency (FMPA))

1	Lincoln Electric System	Doug Bantam		
1	Long Island Power Authority	Robert Ganley		
1	Los Angeles Department of Water & Power	John Burnett	Abstain	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Cole C Brodine		
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke		
1	NorthWestern Energy	John Canavan		
1	Ohio Valley Electric Corp.	Robert Mattey		
1	Oklahoma Gas and Electric Co.	Terri Pyle	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Abstain	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Abstain	
1	Otter Tail Power Company	Daryl Hanson		
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams		
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen		
1	Sacramento Municipal Utility District	Tim Kelley	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	SaskPower	Wayne Guttormson		
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Abstain	
1	Southern California Edison Company	Steven Mavis	Affirmative	

1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Texas Municipal Power Agency	Brent J Hebert		
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine		
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Abstain	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman		
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	SUPPORTS THIRD PARTY COMMENTS - (Thomas Foltz - American Electric Power)
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Services	Mark Peters	Abstain	
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (Florida Municipal Power Agency)
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS - (fmpa)
3	City of Farmington	Linda R Jacobson		
3	City of Garland	Ronnie C Hoeinghaus		
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	CPS Energy	Jose Escamilla		
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	COMMENT RECEIVED
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster		
3	Georgia System Operations Corporation	Scott McGough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Oglethorpe Power Corporation)
3	Great River Energy	Brian Glover	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
3	Hydro One Networks, Inc.	David Kiguel		
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Abstain	
3	Lakeland Electric	Mace D Hunter	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	

3	Nebraska Public Power District	Tony Eddleman	Negative	SUPPORTS THIRD PARTY COMMENTS - (Nebraska Public Power District comment.)
3	New York Power Authority	David R Rivera	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Abstain	
3	Old Dominion Electric Coop.	Bill Watson		
3	Omaha Public Power District	Blaine R. Dinwiddie		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz		
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Abstain	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seminole Electric Cooperative, Inc.	James R Frauen		
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Negative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-County Electric Cooperative, Inc.	Mike Swearingen		
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith		
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	SUPPORTS THIRD PARTY COMMENTS - (Support comments of Indiana & Florida Municipal Power Agencies

				(IMPA & FMPA))
4	Central Lincoln PUD	Shamus J Gamache	Abstain	
4	City of Clewiston	Kevin McCarthy	Negative	SUPPORTS THIRD PARTY COMMENTS - (fmpa)
4	City Utilities of Springfield, Missouri	John Allen		
4	Consumers Energy Company	Tracy Goble		
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	COMMENT RECEIVED
4	Georgia System Operations Corporation	Guy Andrews	Negative	SUPPORTS THIRD PARTY COMMENTS - (Oglethorpe Power Corporation)
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	SUPPORTS THIRD PARTY COMMENTS - (Frank Gaffney, FMPA)
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Abstain	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	COMMENT RECEIVED
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	SUPPORTS THIRD PARTY COMMENTS - (Kedrowski for we energies)
5	AEP Service Corp.	Brock Ondayko		
5	Amerenue	Sam Dwyer	Abstain	
5	Arizona Public Service Co.	Scott Takinen	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (Prior comments submitted by AZPS)
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	Avista Corp.	Steve Wenke	Affirmative	
5	BC Hydro and Power Authority	Clement Ma		
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly		
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	SUPPORTS THIRD PARTY COMMENTS - (Jerry Farringer)
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Alexander Eizans	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS - (Duke Energy)
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	El Paso Electric Company	Gustavo Estrada	Abstain	
5	Electric Power Supply Association	John R Cashin		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Essential Power, LLC	Patrick Brown		
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	

5	Florida Municipal Power Agency	David Schumann	Negative	COMMENT RECEIVED
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Karin Schweitzer		
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	NiSource	Huston Ferguson		
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Oklahoma Gas and Electric Co.	Henry L Staples	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas		
5	Pacific Gas and Electric Company	Alex Chua	Abstain	
5	PacifiCorp	Bonnie Marino-Blair		
5	Pattern Gulf Wind LLC	Grit Schmieder-Copeland		
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway		
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	

5	Public Utility District No. 1 of Chelan County	John Yale		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer		
5	Raven Power	Scott A Etnoyer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Abstain	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Abstain	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Keith Morisette)
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State G & T Association, Inc.	Mark Stein		
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Utility System Effeciencies, Inc. (USE)	Robert L Dintelman		
5	Western Farmers Electric Coop.	Clem Cassmeyer		
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	AEP Marketing	Edward P. Cox	Negative	SUPPORTS THIRD PARTY COMMENTS - (Tom Foltz - AEP)
6	Ameren Energy Marketing Co.	Jennifer Richardson	Abstain	
6	APS	Randy A. Young	Negative	COMMENT RECEIVED
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy	Greg Cecil	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (Duke Energy)
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	COMMENT RECEIVED
6	Florida Municipal Power Pool	Thomas Washburn	Negative	SUPPORTS THIRD PARTY COMMENTS - (FMPA)
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Negative	SUPPORTS THIRD PARTY COMMENTS - (Florida Municipal Power Agency)
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley	Affirmative	
6	New York Power Authority	Saul Rojas	Affirmative	
6	Northern California Power Agency	Steve C Hill	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson		
6	Oklahoma Gas & Electric Services	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Kelly Cumiskey	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Abstain	
6	Salt River Project	Steven J Hulet		
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	Southern California Edison Company	Lujuanna Medina	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (Keith Morisette)
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney		
8		Roger C Zaklukiewicz	Affirmative	
8		Edward C Stein		
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito		
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project 2013-04 Voltage & Reactive Control

The Voltage & Reactive Control Drafting Team thanks all commenters who submitted comments on the draft VAR-002-3. These standards were posted for a 45-day public comment period from February 27, 2014 through April 14, 2014. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 25 sets of comments, including comments from approximately 112 different people from approximately 68 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

Index to Questions, Comments, and Responses

1. Please provide your comments on the proposed VAR-002-3 below: 10

The Industry Segments are:

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

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

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	David Burke	Orange and Rockland Utilities Inc.	NPCC	3
3.	Greg Campoli	New York Independent System Operator	NPCC	2
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
5.	Ben Wu	Orange and Rockland Utilities Inc.	NPCC	1
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
7.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Michael Jones	National Grid	NPCC	1

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

10.	Mark Kenny	Northeast Utilities	NPCC	1
11.	Christina Koncz	PSEG Power LLC	NPCC	5
12.	Helen Lainis	Independent Electricity System Operator	NPCC	2
13.	Michael Lombardi	Northeast Power Coordinating Council	NPCC	10
14.	Alan MacNaughton	New Brunswick Power Corporation	NPCC	9
15.	Bruce Metruck	New York Power Authority	NPCC	6
16.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5
17.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
18.	Robert Pellegrini	The United Illuminating Company	NPCC	1
19.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
20.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
21.	Brian Robinson	Utility Services	NPCC	8
22.	Ayesha Sabouba	Hydro One Networks Inc.	NPCC	1
23.	Brian Shanahan	National Grid	NPCC	1
24.	Wayne Sipperly	New York Power Authority	NPCC	5

2.	Group	Erika Doot	US Bureau of Reclamation	X				X					

No Additional Responses

3.	Group	Janet Smith	Arizona Public Service Company	X		X		X	X				

No Additional Responses

4.	Group	Kathleen Black	DTE Electric			X	X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Kent Kujala	NERC Compliance	RFC	3
2.	Daniel Herring	NERC Training & Standards Development	RFC	4
3.	Mark Stefaniak	Regulated Marketing	RFC	5

5.	Group	Louis Slade	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Garton	NERC Compliance Policy	NA - Not Applicable	1, 3, 5, 6
2.	Randi Heise	NERC Compliance Policy	NA - Not Applicable	1, 3, 5, 6
3.	Connie Lowe	NERC Compliance Policy	NA - Not Applicable	1, 3, 5, 6
4.	Chip Humphrey	Power Generation Compliance	NA - Not Applicable	5
5.	Nancy Ashberry	Power Generation Compliance	RFC	5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Dan Goyne	Power Generation Compliance	NA - Not Applicable	5									
7.	Jarad L Morton	Power Generation Compliance	NPCC	5									
8.	Larry Whanger	Power Generation Compliance	SERC	5									
9.	Larry Nash	Transmission Compliance	SERC	1, 3									
10.	Angela Park	Electric Transmission Compliance	SERC	1, 3									
11.	Candace L Marshall	Transmission Compliance	SERC	1, 3									
12.	Larry W Bateman	Electric Transmission Compliance	SERC	1, 3									
13.	John Calder	Electric Transmission Compliance	SERC	1, 3									
14.	Jeffrey N Bailey	Nuclear Compliance	SERC	5									
15.	Tom Huber	Nuclear Compliance	NPCC	5									
6.	Group	Derrick Davis	Texas Reliability Entity, Inc.										X
No Additional Responses													
7.	Group	Marcus Pelt	Southern Company: Southern Company Services, Inc.; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Power Company; Southern Company generation; Southern Company Generationa and Energy Marketing	X		X		X	X				
No Additional Responses													
8.	Group	Shannon V. Mickens	SPP Standards Review Group		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Allen	City Utilities of Springfield	SPP	1, 4
2.	Louis Guidry	Cleco Power	SPP	1, 3, 5
3.	Michael Jacobs	Camstex	NA - Not Applicable	NA
4.	Mike Kidwell	Empire District Electric Company	SPP	1, 3, 5
5.	Nick McCarty	Kansas City Power and Light	SPP	1, 3, 5, 6
6.	James Nail	City of Independence Missouri	SPP	3
7.	Steve Ricard	Sunflower Electric Power Corporation	SPP	1
8.	Stephanie Johnson	Westar	SPP	1, 3, 5, 6
9.	Mahmood Safi	Nebraska Public Power District	SPP	1, 3, 5

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
10. J.Scott Williams	City Utilities of Springfield	SPP	1, 4									
11. Robert Rhodes	Southwest Power Pool	SPP	2									
9. Group	Matt Schebler	SERC OC Review Group	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	James Watson	Dynegy	SERC	5
2.	Ray Phillips	AMEA	SERC	4
3.	Tim Hattaway	PowerSouth	SERC	1, 5
4.	Richard Jackson	Alcoa Power Generating	SERC	5, 6, 7
5.	Scott Brame	NCEMC	SERC	1, 3, 4, 5

10. Group	Stephen J. Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brenda L. Truhe	PPL Electric Utilities	RFC	1
2.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3
3.	Annette M. Bannon	PPL Generation on behalf of its Supply NERC Registered Entities	RFC	5
4.			WECC	5
5.	Elizabeth A. Davis	PPL EnergyPlus, LLC	MRO	6
6.			NPCC	6
7.			SERC	6
8.			SPP	6
9.			RFC	6
10.			WECC	6

11. Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tim Beyrle	City of New Smyrna Beach	FRCC	4
2.	Jim Howard	Lakeland Electric	FRCC	3
3.	Greg Woessner	Kissimmee Utility Authority	FRCC	3
4.	Lynne Mila	City of Clewiston	FRCC	3
5.	Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4
6.	Randy Hahn	Ocala Utility Service	FRCC	3
7.	Stanley Rzad	Keys Energy Services	FRCC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
8. Don Cuevas	Beaches Energy Services	FRCC 1										
9. Mark Schultz	City of Green Cove Springs	FRCC 3										
12. Group	Ben Engelby	ACES Standards Collaborators						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Shaver	Arizona Electric Power Cooperative/Southwest Transmission Cooperative, Inc.	WECC	1, 4, 5
2.	Shari Heino	Brazos Electric Power Cooperative, Inc.	ERCOT	1, 5
3.	Paul Jackson	Buckeye Power, Inc.	RFC	3, 4
4.	Amber Skillern	East Kentucky Power Cooperative	SERC	1, 3, 5
5.	Michael Brytowski	Great River Energy	MRO	1, 3, 5, 6
6.	Scott Brame	North Carolina Electric Membership Corporation	SERC	1, 3, 4, 5
7.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
8.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
9.	Steve Ricard	Sunflower Electric Power Corporation	SPP	1
10.	Clem Cassmeyer	Western Farmers Electric Cooperative	SPP	1, 5

13.	Group	Mike O'Neil	Florida Power & Light	X									
No Additional Responses													
14.	Group	Richard Hoag	FirstEnergy Corp	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	William Smith	FirstEnergy Corp	RFC	1
2.	Larry Raczkowski	FirstEnergy Corp	RFC	3
3.	Doug Hohlbaugh	Ohio	RFC	4
4.	Ken Dresner	FirstEnergy Solutions	RFC	5
5.	Kevin Query	FirstEnergy Solutions	RFC	6
6.	Richard Hoag	FirstEnergy Corp		NA

15.	Individual	John Falsey	Invenergy LLC					X					
16.	Individual	Nazra Gladu	Manitoba Hydro	X		X		X	X				
17.	Individual	Chris Scanlon	Exelon	X		X	X	X	X				
18.	Individual	Thomas Foltz	American Electric Power	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
19.	Individual	John Seelke	Public Service Enterprise Group	X		X		X	X				
20.	Individual	Venona Greaff	Occidental Chemical Corporation							X			
21.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
22.	Individual	Barbara Kedrowski	Wisconsin Electric Power Co			X	X	X					
23.	Individual	Bill Fowler	City of Tallahassee			X							
24.	Individual	Bernard Johnson	Oglethorpe Power Corporation					X	X				
25.	Individual	Sergio Banuelos	Tri-State Generation and Transmission Association, Inc.	X		X		X					
26.	Individual	Karen Webb	City of Tallahassee					X					
27.	Individual	Keith Morisette	Tacoma Power	X		X	X	X	X				
28.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
29.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				

If you support the comments submitted by another entity and would like to indicate you agree with their comments, please select "agree" below and enter the entity's name in the comment section (please provide the name of the organization, trade association, group, or committee, rather than the name of the individual submitter).

Organization	Agree	Supporting Comments of "Entity Name"
Invenergy LLC	Agree	PSEG Public Service Enterprise Group
Occidental Chemical Corporation	Agree	Ingleside Cogeneration, LP
Oglethorpe Power Corporation	Agree	ACES
South Carolina Electric and Gas	Agree	SERC OC

1. Please provide your comments on the proposed VAR-002-3 below:

Organization	Question 1 Comment
Northeast Power Coordinating Council	Section M1. Add the word "in" to the following sentence: "The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or in a difference control mode ...."Footnote 3: suggest rewording the sentence to "The generator voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or a Reactive Power range communicated by the Transmission Operator to the Generator Operator."Footnote 4: suggest rewording the sentence to "A generating Facility's capability may be established by tests or other means, and may not be sufficient at times to return the system voltage within the schedule tolerance band...."Section M2, part 2.3: suggest rewording the sentence to "Generator Operators that do not monitor the voltage at the location specified on the voltage schedule shall document or be able to demonstrate the methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator."R3: While we agree with the 30 minute window to allow a GOP time to resolve an issue before having to notify the TOP of a status or capability change, the second part of the sentence seems to negate the first. The GOP has to notify the TOP of a status change within 30 minutes but if the status has been restored within 30 minutes then the GOP is not required to notify the TOP of the status change.Rationale for R4: typo in the version number of the standard VAR-002-2b.Section R4: remove the word "then" and "to" in the sentence. Suggest rewording the sentence to "Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within the first 30 minutes of such change, the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability".R1 Severe VSL: for consistency with the wording of the requirement, suggest rewording to "Unless exempted, the Generator Operator did not operate each generator connected to the interconnected transmission system in the automatic voltage

Organization	Question 1 Comment
	control mode ...."R2 Severe VSL: for consistency with the wording of the requirement, suggest adding the word "the" to the sentence: "The Generator Operator did not maintain the voltage or Reactive Power schedule ...." And "The Generator Operator did not modify the voltage when directed ....".R5 High VSL and Severe VSL: the requirement on page 9 applies to the Generator Owner yet the responsible entity for the VSL is the Generator Operator. The word " Generator Operator" needs to be changed to "Generator Owner".
Response: Thank you for your comments. Several of the clarifying changes were made to the wording in the standard based on your feedback. VSLs for R5 and rationales were also corrected. However, the intent behind R3 was to allow GOPs 30 minutes to address or correct an issue before having to notify the TOP of the status change. Currently, if the AVR goes in and out of service multiple times within a short timeframe, the GOP is obligated to make multiple notifications to the TOP, even if the AVR is corrected in less than a few minutes. The drafting team concluded the other suggested changes did not provide additional clarify.	
US Bureau of Reclamation	The US Bureau of Reclamation (Reclamation) reiterates that the VSLs for VARâ€002â€3 R3 and R4 should reflect a range of noncompliance like in VARâ€002â€2. A failure to notify the Transmission Operator of an AVR, power system stabilizer, or reactive capability change for 35 minutes should not be treated as severely as a failure to notify the Transmission Operator of a status change for 75 minutes or longer. Reclamation recommends that R4 be updated to specify a threshold of reactive capability change that requires notification (e.g., 20 MVAR). As written, R4 would require GOPs to notify TOPs of a change in reactive capability of as little as 1 MVAR. Reclamation also requests clarification on types of “changes in reactive capability” that could trigger the notification requirement in R4.Reclamation suggests that the time horizon for R6 should be changed from “Realâ€Time Operations” to “Operations Planning” to match VARâ€001â€4 R6 and reflect that tap setting changes are agreed upon in advance rather than in realâ€time. If the drafting team intends only to refer to tap settings that can be adjusted in real-time (e.g., On Load Tap Changers), the requirement should be more specific.Reclamation appreciates the drafting team’s efforts and recognizes that the proposed revisions include a number of improvements to VAR-001 and VAR-002. However, Reclamation disagrees with the drafting team’s approach to responding to all

Organization	Question 1 Comment
	November 2013 comments on VAR-002 with the statement, "Thank you for your comments. VAR-002 did not pass the last ballot, and the VAR SDT will consider this during the next successive ballot." By responding in this way to all VAR-002 comments, the drafting team provided no responses to the technical issues raised by commenters.
Response: Thank you for your response. The drafting team determined that the best way to ensure reliability was to allow the TOP to provide guidance on when to make notifications based on system needs. This is reflected in VAR-001-4 where the TOP may exempt GOPs from making certain notifications. Further, the drafting team determined that it was not possible to set a reactive capability change threshold that could apply continent-wide. Such a threshold will have to vary based on the entity's size and location of the entity. The drafting team did not change the time horizon for R6 because the currently enforceable standard that previously passed industry comment and ballot used "Real-time operations."	
Arizona Public Service Company	R3 & R4: Please provide the technical justification for the 30 minute time limit. Also, please provide an example of a specific action taken by the Transmission Operator in response to a notification of status change of AVR or PSS. In order to allow the GO time to fix minor problems before reporting, a minimum of 60 minutes should be allowed. This will eliminate unnecessary reporting and limit the impact of reporting on the Transmission Operator. We recommend that all time periods in these requirements be changed to 60 minutes.R5.1: copied below for discussion:For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage: The above language implies that if my GSU primary voltage is rated less than the generator primary voltage, this requirement will not apply. Hopefully, that is not the intent. There are examples of GSU transformers that have the primary voltage intentionally specified to be 5% less than the generator rated voltage to provide a voltage boost. R6: This requirement implies that an action is required whether there is a need for tap change or not. It should be clarified that it applies only when either a GO or a TO is planning a tap change.

Organization	Question 1 Comment
Response: Thank you for your comments. The 30 minutes was selected for two reasons: 1) an IROL T_v must be corrected within 30 minutes in accordance with the NERC Glossary, and 2) the industry consensus was that 30 minutes was appropriate for R3 and R4.	
DTE Electric	Positive improvements!Two minor grammar changes:Second sentence of R3 and R4 - remove "to" before "the Generator Operator"If the capability has been restored within 30 minutes of such change, then to the Generator Operator...
Response: Thank you for your comments. The word "to" was removed from the requirements R3 and R4.	
Dominion	Dominion has the following comments. o While we do not strongly oppose inclusion of the last sentence in requirements 3 and 4, we do not believe they are necessary. We are slightly concerned that such inclusion in this standard could infer that notification is required under similar circumstances in other standards o If the SDT choses to keep the last sentence in R3 and R4, Dominion suggests removing the first 'to' to read "....then the Generator Operator is not required to....".
Response: Thank you for your comments. The last sentences in R3 and R4 are necessary to avoid the situations where multiple entities are notifying TOPs of an issue being addressed/corrected thereby diverting the TOP from their primary objective of system reliability. The drafting team also removed the word "to" from both requirements R3 and R4.	
Texas Reliability Entity, Inc.	We would suggest rewording R2.2 to say "When instructed to modify voltage, the Generator Operator shall comply unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. If the Generator Operator cannot comply with the Transmission Operator's instructions, the Generator Operator shall provide an explanation why the instruction cannot be met."In R4, does the "reactive capability" include static capacitive or reactive devices that are behind the fence (for example, static capacitors and reactors installed on the low voltage feeders at wind plants). Would this requirement apply to such devices if they are not included in the Bulk Electric System per the new BES definition?The status and capability notifications in R3 and R4 may be directly or indirectly in conflict with IRO-005-3.1a, R1.1, TOP-005-2a,

Organization	Question 1 Comment
	Attachment 1, Item 1.2.4, and TOP-006-2, R2. These requirements require monitoring the status of generation and/or AVR status by the RC and BA, as well as the TOP. Will the TOP and RC be able to satisfy their obligations under these other standards in view of the proposed GOP reporting parameters?
Response: Thank you for your comments. The drafting team did not adopt the suggested changes in Part 2.2 because it is outside the scope of what was being addressed in this project. With regard to R4, the TOP may provide the GOP with an exemption for certain notifications under VAR-001-4, and the BES definition will apply with regard to the applicability of this standard.	
Southern Company: Southern Company Services, Inc.; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Power Company; Southern Company generation; Southern Company Generationa and Energy Marketing	Southern Company has the following general comments that are meant to provide non-substantial changes to parts of the standard:1. In the second sentence of the "Rational for R3" box, add "of this type of status change" between "notifications" and "provide". This provides emphasis that the scenario described in the first sentence is one type of status change that may occur. 2. In the third sentence of the "Rational for R3" box, delete "or capability". R3 deals with status changes and R4 deals with capability changes.3. In R4, delete the unneeded word "to" in the second sentence that appears between "then" and "the": ",,, change, then to the Generator Operator is not required ...."4. It is noted that TOP-003-2, R5 and MOD-032-1, R2 (both currently filed with FERC for approval) contain requirements for the GO to provide data to the TOP and the TP similar to that found in VAR-002-3 R5. Duplication of identical requirements for the GO may occur if all three standards are ratified.
Response: Thank you for your comments. The drafting team adopted most of the changes based on your feedback. However, the drafting team retained R5 because the TOP standards are currently being revised. Additionally, MOD-032-1, which is currently pending before FERC, addresses a different time horizon.	
SPP Standards Review Group	Standard:In Requirement R3 second sentence, we would suggest the removal of 'to' from the phrase ' then to the Generator' and have it to read as followed: 'then the Generator Operator'. In Requirement R 4 we would like to suggest the second sentence to be revised and to read as followed; "If the capability has been restored within 30 minutes of

Organization	Question 1 Comment
	becoming aware of such change, then the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability. In Requirement R4 second sentence, we would suggest the removal of 'to' from the phrase ' then to the Generator' and have it to read as followed: 'then the Generator Operator'. In the last line of the 2nd bullet of R1, insert space between 'Operator' and 'for'.Capitalize Part whenever it is referencing a Requirement. For example, in the Rationale Box for R2, the last sentence in the 1st paragraph would read 'Additionally, a new Part 2.3 has been...' Do this throughout the standard.In the Rationale Box for R4, correct the reference to VAR-002-2b.In the Rationale Box for R5, the 3rd sentence should read 'The prior version of VAR-002-2b, Part 4.1.4 (the +/- voltage range...'In the High VSL for R2, insert an 'a' between 'have' and 'conversion'.Replace 'cannot' with 'could not' in the Severe VSL for R6.RSAWIn the RSAW R5 (page 11) under Evidence Requested11, we would like to suggest changing 'M4' to 'M5'....then it would read 'Evidence as outlined in M5'.Similar to the standard, Part should be capitalized when referenced in conjunction with a requirement.In the 3rd row of the table under the Compliance Assessment Approach Specific to VAR-002-3, R2 heading, delete the 'in' in the last line in the cell. In the 5th line in the 1st paragraph in the Note to Auditor section, insert a comma between 'sound' and 'only' such that it reads '...documentation review, are sound, only limited audit...'. In the last line of the same paragraph, insert a 'the' between 'that' and 'entity'.In the 3rd row of the table under the Compliance Assessment Approach Specific to VAR-002-3, R3 heading, insert a 'the' between 'if' and 'entity'. In the 5th line in the 1st paragraph in the Note to Auditor section, insert a comma between 'sound' and 'only' such that it reads '...documentation review, are sound, only limited audit...'. In the last line of the same paragraph, insert a 'the' between 'that' and 'entity'.In the Evidence Requested table for R4, insert a 'the' in front of 'entity' or 'entity's' in the 2nd and 3rd line of the 2nd row and the 1st line of the 3rd row. In the 1st line of the 3rd row of the table under the Compliance Assessment Approach Specific to VAR-002-3, R4 heading, insert a 'the' between 'if' and 'entity'.In the Evidence Requested table for R5, change the reference to M5 in the 2nd row to M4.In the 1st line of the 2nd row of the table under the Compliance Assessment Approach Specific to VAR-002-3, R5 heading, insert a 'the' between 'if' and 'entity'.In the 1st line of the 2nd

Organization	Question 1 Comment
	row of the table under the Compliance Assessment Approach Specific to VAR-002-3, R6 heading, insert a 'the' between 'if' and 'entity'.
Response: Thank you for your comments. The drafting team was able make most of the recommended changes to the standard. The drafting team will forward your recommendations for the RSAW to NERC Compliance staff for their consideration.	
SERC OC Review Group	Requirement R1:The OC Review Group believes that R1 would be strengthened with further report timing clarification is required in the case where the AVR changes state unexpectedly. The OC Review Group respectfully recommends adding a bullet to R1 which reads "In cases where the AVR changes state unexpectedly the Generator Operator will notify the Transmission Operator within 30 minutes."Current R1: The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode, as instructed by the Transmission Operator unless: 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following: [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] o That the generator is being operated in start-up,1 shutdown,2 or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or o That the generator is not being operated in the control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing. Proposed R1: The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode, as instructed by the Transmission Operator unless: 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following: [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] o That the generator is being operated in start-up,1 shutdown,2 or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or o That the generator is not

Organization	Question 1 Comment
	being operated in the control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing. o In cases where the AVR changes state unexpectedly the Generator Operator will notify the Transmission Operator within 30 minutes only if reactive capability is not restored.Measure 1:The OC Review Group recommends that Measure 1 be modified to specifically include that SCADA alarming may be used for real-time notification.Current Measure 1: The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If a generator is exempted, the Generator Operator shall also have evidence that the generator is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage). Proposed Measure 1: The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. SCADA alarming may be used for real-time notification. If a generator is exempted, the Generator Operator shall also have evidence that the generator is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage). Requirement 2:The OC Review

Organization	Question 1 Comment
	Group believes and recommends that the phrase “or other control capabilities” to provide further clarification to the Requirement.Current R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedulecapabilities4) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] Proposed R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage, Reactive Power schedule, or other control capabilities provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] Measure 2:The OC Review Group believes and recommends that the phrase “or other control capabilities” to provide further clarification to the Measure.Current M2, paragraph 1: M2. In order to identify when a generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator’s instructions for addressing deviations from the voltage or Reactive Power schedule. Proposed M2, paragraph 1: M2. In order to identify when a generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage, Reactive Power schedule or other control capabilities, provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA

Organization	Question 1 Comment
	data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage or Reactive Power schedule.Requirement 3:The OC Review Group believes that R3 would be strengthened with further report timing The OC Review Group respectfully recommends adding a bullet to R3 which reads "The Generator Operator is not required to notify the Transmission Operator of the status change if the change is expected as part of a startup, shutdown, or testing procedure previously provided to the Transmission Operator per Requirement 1."Current R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within 30 minutes of such change, then to the Generator Operator is not required to notify the Transmission Operator of the status change [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]Proposed R3: Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within 30 minutes of such change, then to the Generator Operator is not required to notify the Transmission Operator of the status change [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] o The Generator Operator is not required to notify the Transmission Operator of the status change if the change is expected as part of a startup, shutdown, or testing procedure previously provided to the Transmission Operator per Requirement 1.Measure 3:The OC Review Group recommends that Measure 3 be modified to specifically include that SCADA alarming may be used for real-time notification.Current Measure 3: The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any status change identified in Requirement R3. If the status has been restored within the first 30 minutes, no notification is necessary. Proposed Measure 3: The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any status change identified in Requirement R3. SCADA alarming may be used for real-time notification. If the status has been restored within the first 30 minutes, no notification is

Organization	Question 1 Comment
	necessary. Requirement 4:Current R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within 30 minutes of such change, then to the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability. [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations] The SERC OC Review Group respectfully requests further clarification for the phrase "becoming aware of a change in reactive capability". Without clarifying the size "of a change in reactive capability" it is possible that the TOP will receive numerous calls reporting extremely small changes in reactive capability.Violation Severity Levels:Requirement 1: The SERC OC Review Group proposed change does not require VSL modifications.Requirement 2: The SERC OC Review Group proposes the following change to the VSL to reflect the modification to Requirement 2. Current R2 Severe VSL: The Generator Operator did not maintain voltage or Reactive Power schedule as directed by the Transmission Operator and did not make the necessary notifications required by the Transmission Operator. OR The Generator Operator did not have an operating AVR, and the responsible entity did not use an alternative method for controlling voltage. OR The Generator Operator did not modify voltage when directed, and the responsible entity did not provide any explanation. Proposed R2 Severe VSL: The Generator Operator did not maintain voltage, Reactive Power schedule, or other control capabilities as directed by the Transmission Operator and did not make the necessary notifications required by the Transmission Operator. OR The Generator Operator did not have an operating AVR, and the responsible entity did not use an alternative method for controlling voltage. OR The Generator Operator did not modify voltage when directed, and the responsible entity did not provide any explanation. The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Review Group only and should not be construed as the position of the SERC Reliability Corporation, or its board or its officers.
Response: Thank you for your comments. The drafting team did not make the suggested change to R1 because it would create a conflict with R3. The measure for R3 does not prevent SCADA alarms/data from serving as evidence of compliance, and the	

Organization	Question 1 Comment
standard does not explicitly list all the forms of compliance. With regard to R4, the TOP can provide notification exemptions under VAR-001-4. This will allow the TOP to tailor notifications based on size of reactive capability if necessary. For the R2 VSL, the language was not modified because the GOP must maintain the voltage or Reactive Power schedules, regardless of the method of control.	
PPL Corporation NERC Registered Affiliates	1. The PPL NERC Registered Affiliates agree with R2 stating that GOPs shall maintain the voltage/MVAR schedule or meet the TOP's deviation notification criteria; however, there is no explicit requirement for TOPs to issue any such notification criteria. We request that the standard be revised to require TOPs to issue reasonable notification criteria for deviations from the TOP-provided voltage or reactive power schedule. Such criteria can enhance reliability by reducing the number of repetitive, unnecessary telephone calls to TOP system operators that could distract from other reliability tasks. 2.We recommend that the first sentence of VAR-002-3 R6 be changed from, "After consultation with the Transmission Operator regarding necessary step-up transformer tap changes," to, "After consultation with the Transmission Operator regarding necessary step-up transformer tap changes and the implementation schedule," to mirror the language in R6 of VAR-001-3.3. We wish to point-out also that the low side-to-high side ratio of a transformer is fixed only for an ideal (no losses) device, and for actual equipment it changes with load (termed "regulation"), and this effect is not trivial in magnitude. The "Rationale for R2" section of VAR-002-3 explicitly permits "straight ratio conversion," however; so, if the standard passes in its present form, GOPs using this method can be officially compliant yet factually operating well outside the voltage schedule bandwidth. The term, "straight ratio conversion," should be replaced with "nominal ratio conversion compensated for transformer regulation."3. We recommend that Measures M1 and M3 include language that would allow for SCADA alarms to count as evidence of notification to the TOP from the GOP. We suggest adding the language, "SCADA alarming, or some other electronic automatic system, may be used for real-time notification."
Response: Thank you for your comments. VAR-001-4 does address TOP notification requirements, and VAR-001-4 allows the TOP to tailor the notifications based on their system needs. For R6, the consultation with the TOP can encompass the implementation schedule. R2 rationale was not modified because the standard allows each entity to select the conversion	

Organization	Question 1 Comment
methodology that best suits their needs. For M1 and M3, SCADA alarms are not precluded as evidence of compliance, but the drafting team did not want to provide an exhaustive list of all forms of compliance.	
Florida Municipal Power Agency	There are grammar issues with R1 including a ambiguous references. There are at least two ways to read R1: (i) does R1 mean that the AVR is put into automatic voltage control mode as a default with the ability to operate in a different control modes only at the instruction of a TOP - in other words, there is no instruction from a TOP if the AVR is operating in automatic voltage control mode; or (ii) a TOP instruction is required to determine in which control mode to operate, including automatic voltage control mode? Also, does the "... unless ..." and the ensuing two bullets apply only to alternative control modes or also to automatic voltage control mode?Another ambiguity is the use of the word "notified" in R1. "Notify" as used in R3 allows the GOP a 30 minute (after the fact) window. Does R1 allow the same after the fact notification period? R1, R2, R3 and R4 all include notifaction provisions that in some ways overlap and cause confusion. If the Generator Operator needs to take immediate or emergency actions and transfer the automatic voltage controller from "auto" to "manual", it is not clear in the requirements (especially requirement R1) that the Generator Operator is allowed to perform this action without obtaining prior instruction from the Transmisison Operator or giving prior notification to the Transmission Operator. FMPA believes it would be clearer to re-write R1, R2, R3 and R4 into two requirements: R1 for desired performance and R2 for notifications of when that performance cannot be maintained.FMPA offers the following re-write of R1, R2, R3 and R4 into two proposed requirements that we believe reflects the intent of the SDT while clarifying:"R1 The Generator Operator shall operate each generator connected to the interconnected transmission system with its automatic voltage regulator (AVR): (i) in service; (ii) in the control mode instructed by the Transmission Operator; and (iii) maintaining the generator voltage or Reactive Power schedule (within each generating Facility's capabilities) provided by the Transmission Operator, unless: (a) the generator is exempted by the Transmission Operator; (b) the generator does not have an AVR; or (c) the Generator Operator has notified the Transmission Operator in accordance with R2 of an inability to meet these performance requirements:1.1 When a generator's AVR is out of service or the generator does not have

Organization	Question 1 Comment
	an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.1.2 Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.R2 Each Generator Operator shall notify its associated Transmission Operator prior to or within 30 minutes of becoming aware of any of the following, unless the performance requirements of R1 are restored within 30 minutes: o That the generator is not being operated in the control mode that was instructed by the Transmission Operator; or o A status change of the AVR, power system stabilizer, or alternative voltage controlling device o A change in reactive capability of a generator due to factors other than those described aboveA procedure previously provided by the Generator Operator to the Transmission Operator that includes a description of AVR, power system stabilizer or alterantive voltage controlling device status changes or control mode changes during start-up, shutdown or testing acts as standing notification such that the Real-time communication of start-up, shutdown, or testing also fulfilles the required notification."FMPA is aware that this offered language removes the SDTs proposed R2 bullet 2.2 that requires the GOP to modify voltage when instructred to do so by the TOP; however, this bullet is duplicative of the parent requirement (e.g., if a TOP instructs the GOP to modify voltage, is that not a new voltage schedule, albeit maybe a temporary schedule?) and TOP-001-1, R3 that requires GOPs to comply with directives from a TOP. FMPA believes that this offered alterantive language simplifies and clarifies the SDT's intent.
Response: Thank you for your comments. R1 has been modified to provide clarity with regard to AVR settings. R1 clearly states that the AVR must be run in either controlling voltage mode or the mode instructed by the TOP. The only time that the GOP can run in a different mode or in manual is if the GOP has been exempted or the GOP has notified the TOP of one of the bulleted items. Both bullets for R1 still apply to the entire body of R1. Further, the timing for the second bullet of R1 must work in tandem with the new R3.	

Organization	Question 1 Comment
ACES Standards Collaborators	(1) VAR-002-3 R1 is confusing. Please clarify the second bullet in R1 so it ties into the previous part of the sentence. Read literally, R1 states, "The GOP shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode, as instructed by the TOP unless... 2) the GOP has notified the TOP of one of the following: [second bullet] That the generator is not being operated in the control mode that was instructed by the TOP for a reason other than start-up, shutdown, or testing." This exception is circular and needs to be revised.(2) The RSAW for R1 does not provide any additional details for compliance beyond the language in the requirement and corresponding measure. We would like to see additional compliance statements in the RSAWs, especially considering that the compliance input document contained several relevant issues with VAR-002-3.(3) VAR-002-3 R2 and Part 2.1 need to be modified so that the GOP is only required to follow the voltage schedule if provided by the TOP. It is not desirable for the TOP to provide all generators voltage schedules. As an example, the TOP may determine it does not need to provide a voltage schedule to a small generator. To consider this situation, the clause "if a voltage schedule is provided by the TOP" could be added to both Part 2.1 and the main requirement. (4) VAR-002-3 R2 will be problematic for some GOPs because it does not reflect the characteristics of the voltage schedule provided by some TOPs. For example, some TOPs provide an hourly average voltage schedule to avoid the need for notification for every time the GOP drifts out of schedule. How would R2 be applicable in this situation? Would it only apply for the first 15 minutes of each hour looking back at the last hour? Please modify the requirement accordingly to address this issue.(5) The RSAW for R2 contains ambiguous language, stating that the auditor should "select a sample of timeframes" to verify compliance. The evidence retention section (section C.1.2.) of VAR-002-3 states that the Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers and maintain all other evidence for the current and previous calendar year. The RSAW should be revised to "review instances when a generator deviates from its schedule" for time periods applicable to the evidence retention section of the standard. (6) VAR-002-3 R3 is improved by expanding the time from 15 to 30 minutes before a GOP must notify the

Organization	Question 1 Comment
	TOP of a status or capability change. We thank the drafting team for providing additional flexibility.(7) The RSAW for R3 states that the auditor may select certain instances where an entity had a status change on AVR. Is the intent of the drafting team to require an entity to maintain a list of all status changes? This does not appear to align with the requirement, especially considering that the rationale for R3 clarifies that the requirement was modified to limit notifications for quick status changes, as these provide little to no benefit to reliability. Having to maintain a list of status changes for an auditor verify also provides little to no benefit to reliability. We recommend revising the RSAW to state that the auditor may select "evidence of GOP status change notifications to its TOP."(8) Requirement R4 in the RSAW is inconsistent with the requirement in the proposed standards. It still contains 15 minutes which has been updated to 30 minutes in the latest proposed standard.(9) VAR-002-3 R4 could be clarified further in the second sentence to account for awareness. We recommend modifying the language to state, "If the capability has been restored within 30 minutes of [becoming aware] of such change..." This revision will align both sentences in R4.(10) We are concerned about the statement in the "Note to Auditor" section that the auditor will look for instances "where it is likely that an entity was made aware of the change in reactive capability" such as when a unit trips or an AVR fails. The statement is problematic for two reasons. First, the requirement is clear that the GOP must be aware of the change before they are required to communicate it. The auditor should not be looking for evidence such as when an AVR fails but rather for log book entries and similar information that the GOP was aware of the change. They should not be looking for when the AVR went offline. Second, a unit trip is a bad example because the TOP will have telemetry necessary to observe when a unit is forced off-line. Is it really necessary to have a compliance requirement for the GOP to notify the TOP when the TOP will already know of the unit's off-line status? We agree that communication between the GOP and the TOP should take place following such an event, but we do not think it rises to a compliance level for this specific example.(11) VAR-002-3 R5 meets multiple P81 criteria and should be removed. It meets Criterion A because it does little, if anything, to benefit or protect the reliable operation of the BES. It also meets Criterion B2 - Data Collection/Data Retention and Criterion B4 - Reporting because

Organization	Question 1 Comment
	it requires the GOP to gather their tap setting information and report it to a third party (i.e. its TOP), which is unnecessary to implement, as a reliability requirement. A GOP is not going to refuse to provide data to its TOP on its generator step-up transformer in a compliance-driven world. In fact, making this data subject to compliance slows down the free exchange of the information because of all the extra checking that goes into managing (i.e. verifying, checking, storing) compliance documentation. This requirement also meets B7 - Redundant because the TOP can specify this data in its data specification per TOP-003-2 R1, distribute it to the GO per TOP-003-2 R3, and then have the GO respond per TOP-003-2 R5. We do not support the VSLs for R5 because it meets P81 criteria and should be removed. (12) The RSAW for R5 should specify the evidence auditors will verify, including tap settings, available fixed tap ranges, and impedance data. The current RSAW refers to "evidence as outlined in M4." This is an incorrect reference to the wrong measure and needs to be updated.(13) VAR-002-3 Part 6.1 meets a P81 criterion and should be removed. It meets Criterion A because it does little, if anything, to benefit or protect the reliable operation of the BES. It also meets Criterion B4 - Reporting because it requires the GO to report a technical justification for not implementing tap changes. This technical justification simply does not support reliability. The TOP can make adjustments to other voltage schedules to account for the GO's inability to implement the tap changes. What is the purpose of the GO providing the TOP a technical justification? Is it to provide the TOP some assurance there is a technical reason for failing to implement the tap changes? In a compliance-driven world, the TOP can reasonably expect the GOP to implement the tap changes unless the changes would violate safety, equipment limits, or regulatory and statutory requirements since these are the only deviations allowed by the main requirement. The threat of sanctions assures this. Furthermore, the GOP may legitimately not have a "technical" justification because a regulatory requirement is a legal justification, not a technical justification. (14) The RSAW for R6 needs to be developed. It is currently incomplete and does not list any evidence or any additional guidance beyond what is listed in the measure.(15) Thank you for the opportunity to comment.
Response: Thank you for your comments. R1 has been modified to provide clarity with regard to AVR settings. R1 clearly states that the AVR must be run in either controlling voltage mode or the mode instructed by the TOP. The only time that the	

Organization	Question 1 Comment
GOP can run in a different mode or in manual is if the GOP has been exempted or the GOP has notified the TOP of one of the bulleted items. Both bullets for R1 still apply to the entire body of R1. The RSAW was concurrently developed with the standard so the intent of the drafting team is reflected in how compliance is assessed, but the RSAW is a NERC Compliance document that the drafting team does edits. However, these comments will be forwarded to the appropriate individuals for review. The drafting team could not remove the requirements to make tap setting changes and provide tap data under P81 because the TOP standards are being currently revised, and FERC has not approved the most recent MOD filing. Further, the data requirements are important for TOP studies which impact tap setting/max VAR output. With regard to the technical justification for a tap setting, the TOP will need to understand why the GOP cannot make a tap setting modification. Changing a tap will impact reactive support from a generating unit, and this will impact reliability. Finally, the requirement to provide a technical justification is an existing requirement in the currently enforceable VAR-002-2b.	
Florida Power & Light	For R4, the loss of an individual wind turbine should not be considered a reactive capability change, since the real power capability would change incrementally along with the reactive capability change and in most cases other turbines would compensate for the reactive capability loss. In general, these requirements should all be applied on the aggregate level for dispersed generating resource facilities. Clarification on R5 is needed to better understand applicability of tap settings changes and request on dispersed generating resources as these typically are designed with a smaller padmount transformer or similar for each individual generating resource, along with a larger aggregating GSU to collect the aggregate generation. Intent would be to include the GSU, but exclude the smaller individual padmount transformers.
Response: Thank you for your comments. With regard to R4, the TOP may provide the GOP with an exemption for certain notifications under VAR-001-4, and the BES definition will apply with regard to the applicability of this standard.	
FirstEnergy Corp	FirstEnergy would like to offer the following comments:1. With regards to clarifying that the Generation Operator will follow the condition of notification of the Transmission Operator. We offered the following two options, where option 1 modifies the current red line version of the Requirement 2 and option 2 adds a sub Requirement to explicitly specify the situational required action of the Generator Operator for the Transmission Operator.OPTION 1:R2. Unless exempted by the Transmission Operator, each Generator

Organization	Question 1 Comment
	Operator shall maintain the generator voltage or Reactive Power schedule (within each generating Facility's capabilities) provided by the Transmission Operator, or otherwise shall meet the conditions of notification provided by the Transmission Operator for deviations from the voltage or Reactive Power schedule. [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]OPTION 2:R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule3 (within each generating Facility's capabilities4) provided by the Transmission Operator. [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]2.1 The Generator Operator shall meet the conditions of notification provided by the Transmission Operator for deviations from the voltage or Reactive Power schedule. Then renumber remaining sub Requirement as needed.Pertaining to Measure 2:Remove the first sentence ("In order to identify when a unit generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility") from measure 2. This sentence does not apply to requirement 2 since it only requires the Generator Operator to maintain the generator voltage or Reactive Power schedule that is provided by the Transmission Operator. The inclusion of this sentence could be interpreted that the Generator Operator will need to provide evidence of "monitoring" activities which is not a performance based requirement.
Response: Thank you for your comments. The requirement and measure language was selected very carefully. The first and second sentences of M2 provide GOPs with the ability to monitor and maintain voltage based on existing equipment, and it does not require GOPs to install new metering.	
Manitoba Hydro	(1) R1 - R1 appears to be such a lax requirement that it is arguably unnecessary. Under the second bullet, the only step that a GO has to take in order to avoid compliance is to notify the TO that it is not complying and provide any reason whatsoever. This leads one to question how important the requirement is to reliability. (2) R3 - It appears that the two sentences in R3 conflict with each other. Based on the second sentence, the GOP is not required to notify the TOP if the status has been restored within 30 minutes. However, the first sentence requires the GOP to notify the TOP within 30 minutes of the change. If at the 30th minute, the GOP realizes that the status is not restored, there will not be enough

Organization	Question 1 Comment
	time for the GOP to notify the TOP. If the 30 minute notification time could be extended to 45 or 60 minutes, there will be enough time for the GOP to notify the TOP. (3) M3 - For consistency with that in R3, "the first" in the second sentence should be deleted. (4) R4 - Similar to that in R3, if the 30 minute notification time could be extended to 45 or 60 minutes, there will be enough time for the GOP to notify the TOP. (5) M4 - For consistency with that in R4, "the first" in the second sentence should be deleted. (6) Based on the Standards Process manual, "Time Horizon: The time period an entity has to mitigate an instance of violating the associated requirement." the Time Horizon for R5 and R6 should be changed from "Real-time Operations" to "Operations Planning" because in R5 the GO is required to provide the information within 30 days and in R6 the tap changes should be scheduled during an outage after consultation with the TOP.
Response: Thank you for your comments. R1 is important because it requires a notification to the TOP when the generator is not in AVR or the instructed control mode. It also provides flexibility for the GOP in case the AVR switches modes. The coordination is necessary in order to provide the TOP with the opportunity to plan for other reactive resources. The 30 minutes is similar to the requirement to correct T_V issues within 30 minutes. The 30 minutes did not exist in VAR-002-2b, and now the 30 minutes provide GOPs with the time to address issues before having to notify the TOPs. The time horizons for R5 and R6 exist in the currently enforceable standard, and were not modified by this drafting team.	
Exelon	1.VARâ€002â€3 Effective DatesThe Implementation Plan for VAR-001-4 and VARâ€002â€3 requires the new Standard revisions to be implemented the first day of the first calendar quarter after applicable regulatory approval, allowing for a situation in which the standard could receive regulatory approval towards the end of the calendar quarter, resulting in an effective date with little or no implementation time, e.g., if regulatory approval is received on March 30, the standard would need to be implemented on April 1. IN addition, although the Implementation Plan justification states that the VARâ€002 standard "cannot go into effect without the new TOP schedules and notification requirements" it does not address the implementation associated with changes to VARâ€002 with respect to status notifications. There is not sufficient time to allow generating units to implement training of operators and procedural changes necessary to implement the proposed changes to notification requirements associated

Organization	Question 1 Comment
	with the AVR, PSS or alternative voltage controlling device. In the VAR-002 Directives Project Implementation Plan, the NERC SDT acknowledges that the TOPs will "need some time" to adjust to providing data and therefore the TOPs are provided a quarter to prepare documentation. The GO/GOPs should be afforded at least that amount of time for implementation. We suggest a 6 month implementation period following regulatory approval.2.Dispersed GenerationThis version does not account for dispersed generation (such as wind or solar as found in the new BES definition). These generators may not have a traditional AVR, may only provide limited reactive resources and the individual elements may not have AVR or be capable of operating in voltage control mode. We understand Project 2014-04 is addressing standards changes for dispersed resources and recognize there are parallel efforts that may be difficult to reconcile. Given that, we request the Drafting Team consider how best to acknowledge that VAR-002-4 may have limited applicability to dispersed generation resources and that it is likely to be revised based on the work of Project 2014-04. 3.VAR-002-3 R2.3Exelon believes it is reasonable to allow the GOP to monitor the voltage specified in their TOP issued voltage schedule by allowing the GOP to monitor at a different location by applying a methodology for converting the voltage monitored; however, the conversion method should be specifically communicated to the TOP. There is not a one for one conversion between grid voltage and terminal voltage and therefore the conversion method and monitoring point should be clearly communicated to the TOP to avoid any future compliance audit or implementation issues.4.VSLsExelon understands that R3 and R4 are binary requirements as outlined in Guideline 2 of the "Violation Risk Factor and Violation Severity Level Justifications" associated with VAR-002-3, (e.g., did or did not notify in 30 minutes), it is however unreasonable that a complete failure to notify would have the same VSL as a notification that is one minute late versus one that is days or weeks late. We urge NERC to address this issue from reliability, not a strict compliance perspective; in instances such as this, there should be levels of severity not simply binary requirements.
Response: Thank you for your comments. The implementation schedule is shorter than other projects, but that date was selected originally because industry provided feedback that VAR-002-2b changes should be implemented quickly to avoid unnecessary notifications to the TOP. FERC has not historically approved standards within one quarter of filing. Further, the	

Organization	Question 1 Comment
Dispersed Generation project has released its whitepaper, and no changes are being recommended for VAR-002-2b. The standard does not require the GOPs to provide TOPs with the methodology for conversion because the TOPs provided feedback that their primary concern was that the voltage schedule was maintained. The VSLs were simplified to remove the gradation in the currently enforceable requirement. If a large unit reports later than a small unit, then the severity will vary between the two. Therefore, the timing elements were removed since the requirements are binary in nature.	
American Electric Power	AEP would like to thank the drafting team for their efforts on this project. Their willingness to incorporate industry's input into the draft standard is very much appreciated.VSL Table: The High and Severe VSL entries for R5 should indicate Generator Owner rather than Generator Operator.
Response: Thank you for your comments. The VSL table has been updated.	
Public Service Enterprise Group	PSEG appreciates the SDT's hard work on this standard and we have only one comment.In R2, subpart 2.3 uses the words "monitor" and "monitored." These words have unintended implications in two respects:1. There was never an obligation in the prior version of VAR-002 that the GOP "monitor" its voltage. The objective in this standard, as in its predecessor, is to require the GOP to maintain a voltage or Reactive Power schedule specified by the TOP. (Under VAR-001-4, R5.3, a TOP's schedule must have tolerance bands, which is an improvement over the R4 in the current VAR-001-3.) While "monitoring" the TOP-specified schedule in an activity that may be related to maintaining such a schedule, is not the results-based purpose of the standard. 2. What would constitute acceptable monitoring? As written, this is an open question that an auditor must answer. It's possible that a GOP could be in violation of subpart 2.3 if its "monitoring" was deemed unacceptable by an auditor even though the GOP maintained the TOP's schedule within the tolerance bands 100% of the time!We therefore recommend that the SDT replace prescribed activities of "monitor" and "monitored," respectively in subpart 2.3, with the performance requirement of "maintain" and "maintained." This would preserve the requirement that the GOP have a conversion methodology if it does not maintain the voltage schedule at the location specified by in TOP's schedule, without also prescribing that GOPs monitor voltage to do so. To

Organization	Question 1 Comment
	implement this change, subpart 2.3 would read:"Generator Operators that do not maintain the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being maintained by the Generator Operator."
Response: Thank you for your comments. The intent behind Part 2.3 is to require a methodology for a conversion, and the drafting team chose the word "monitor" and "monitored" to specifically alleviate concerns that an auditor will take issue with monitoring equipment and where it is located. The drafting team used the word monitor to convey where the GOP has visibility of the voltage. The words "maintain" and "maintained" may introduce ambiguity in Part 2.3 because the industry was concerned that an auditor would question how voltage is maintained if the GOP and TOP are not metering the same point. The drafting team selected "monitor" and "monitoring" based on input from many GOPs that they did not want their monitoring systems questioned, nor did they want to be required to install new monitoring systems for this standard.	
Ingleside Cogeneration LP	Ingleside Cogeneration LP (ICLP) believes that VAR-002-3 Draft 3 adds much needed flexibility in the manner that GOP supports voltage at the transmission interconnection. Combined with the updates to VAR-001-4, we agree that close coordination with the TOP is inherent in the process - which is a key reliability need. A primary example is the allowance for the TOP to determine how the GOP may communicate changes in AVR and PSS status. Those of less intrinsic importance to BES reliability may be required to notify a status change through telemetry; high-impact generation facilities may need to call the TOP as well. The result is that distracting calls are eliminated - which can otherwise pose a threat to the BES in as of themselves.In fact, our only concerns are related to the draft RSAW that was posted concurrently with the standard. First, a further description in the RSAW under R1 and R2 which directs how the CEAs must react to a TOP voltage control strategy that goes against today's model. For example, if exemptions are given, it must be clear that it is not up to the auditor to question their technical veracity. Their only focus must be how well the Generator Operator adhered to the TOP's voltage/Reactive schedule. In addition, the auditor instructions for R2 needs to include a line item addressing footnote 4 which allows capability exceptions for adherence to the TOP's voltage/Reactive schedule. This may take two forms - first, if the external system attempts to force the generator past its Facility Rating limits. Such a condition may persist

Organization	Question 1 Comment
	indefinitely, and can damage the unit if compliance is forced. Second, a rapid change in loading will create Reactive-power spikes that can easily exceed the TOP's specified range. These typically last for under a minute and must also be accepted as compliant by the CEA. In both cases, a notification to the TOP is unnecessary as it will serve only as a nuisance call.
Response: Thank you for your comments. The RSAW was concurrently developed with the standard so the intent of the drafting team is reflected in how compliance is assessed, but the RSAW is a NERC Compliance document that the drafting team does not edit. However, these comments will be forwarded to the appropriate individuals for review.	
Wisconsin Electric Power Co	R1 As written, the requirement is difficult to interpret (four different actions or qualifictions for one requirement). The draft language allows the Transmission Operator to instruct the Generator Operator to operate a generator in any number of undefined control modes without prior agreements in place between the TO and GO. Prior versions of the draft standard allowed for unusual circumstances to be addressed via the, "unless the Generator Operator is exempted by the Transmission Operator" language. The rational for keeping the Requirement 1 language as is in the July 18th draft is to avoid allowing Transmission Operators from determining the mode in which AVR is to be operated without the need for the process of exempting the generator from operating in AVR in the voltage control mode prior to making the request to the Generator Operator. The new Rationale for R1 does not address the change, but merely includes the proposed changes within the rationale. This is unacceptable and the Standard Drafting Team is asked to expanded the rational for inserting, "or in a different mode, as instructed by the Transmission Operator" into the VAR-002-3 Draft Standard should the request to use the July 18th 2014 draft version of VAR-002-3 not be returned.R2 The requirement references "conditions of notification for deviations from the voltage or Reactive Power schedule." Where are the conditions defined relative to voltage or Reactive Power?R3: The redline version includes an extra "to" in the following sentence, "If the status has been restored within 30 minutes of such change, then to the Generator Operator is not required to notify the Transmission Operator of the status change. Additionally, as currently written the requirement incents a delay in reporting changes in status. Entities should be

Organization	Question 1 Comment
	required to report status changes as soon as possible. Allowing entities to not report status changes that reverse within 30 minutes creates a mixed message. Entities may be incented to report status changes at 29 minues and 59 seconds in a hope that the status has been restored.
Response: Thank you for your comments. R1 has been modified to provide clarity with regard to AVR settings. R1 clearly states that the AVR must be run in either controlling voltage mode or the mode instructed by the TOP. The only time that the GOP can run in a different mode or in manual is if the GOP has been exempted or the GOP has notified the TOP of one of the bulleted items. Both bullets for R1 still apply to the entire body of R1. The notification conditions will come from the TOP under VAR-001-4. Also the extra words were removed from R3 and R4. The timing in R3 was added to improve reliability by allowing the GOP to address issues and correct them within the 30 minutes. This would alleviate the TOP from receiving numerous unnecessary notifications.	
City of Tallahassee	1. R3 & R4 - Need to delete the inserted "to" in front of the inserted "the Generator Operator is required to". (see redline to last posted)2. Table of Compliance Elements (pg 12 of 16, redline to last posted) for R2 under severe VSL, the last paragraph " The Generator Operator did not modify voltage when directed, and the responsible entity did not provide an explanation" should be modified to be "The Generator Operator did not modify voltage as instructed, and the responsible entity did not provide an explanation" to match the requirement language.
Response: Thank you for your comments. The extra words were removed from R3 and R4. The VS for R2 has also been modified.	
Tri-State Generation and Transmission Association, Inc.	The VRF chart in the standard contradicts the language in the requirements. Requirement R5 has the GO as the applicable entity but in the VRF chart it refers to the GOP as the applicable entity. Tri-State believes the GOP should be the applicable entity for requirement R5. Tri-State also believes R5 and R6 should match up and be applicable to the same entities. Thus Tri-State believes the GOP should be the applicable entity for R6.There are also minor edits needed to the requirements below: In R3... If the status has been restored within 30 minutes of such change, then the GOP is not required to notify

Organization	Question 1 Comment
	the TOP of the status change.In R4... If the capability has been restored within 30 minutes of such change, then the GOP is not required to notify the TOP of the change in reactive capability.
Response: Thank you for your comments. The VSL for R5 has been corrected, and the extra words have been removed from R3 and R4. For R5 and R6, the GO was selected because the owner of the asset is the entity that should have the ultimate responsibility for making those tap changes. The GO will work with the GOP to ensure those change are made.	
Tacoma Power	Tacoma Power submits the following comments: Requirement R4. There is no requirement for GOPs to calculate the baseline reactive capability, so it makes no sense to have R4 require GOPs to notify TOPs when the reactive capability deviates from the baseline reactive capability. Furthermore, the reactive capability of plants can vary in Real-time based on real power output, system voltage, or weather conditions. Per MOD-11 and 12, GOs/GOPs must provide modeling data to the that the TOP can use to evaluate reactive capability. Any notifications under R4 should be limited changes resulting equipment malfunctions. Revise R4 to state "Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to equipment malfunctions other than those malfunctions requiring notification under Requirement R3. If the capability has been restored within 30 minutes of such change, then to the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability."Requirement R5 is redundant to MOD-011 R1.4 and should therefore be removed from VAR-002-3. Requirement R5.1 does need to include auxiliary transformers because typically system powerflow models do not include unit auxiliary transformers or excitation transformers. If R5.1 is retained, please clarify that auxiliary transformer does not include PTs or CTs.
Response: Thank you for your comments. The standard does not require a baseline calculation, and the currently enforceable VAR-002-2b requires a notification to the TOP as soon as a reactive capability change occurs. Also, the MOD standards are in different time horizons from the VAR standards. R5.1 states "auxiliary transformers with primary voltages equal to or greater	

Organization	Question 1 Comment
than the generator terminal voltage." The drafting team does not believe this encompasses PTs or CTs or excitation transformers.	
Nebraska Public Power District	In Requirement R3 and R4 second sentence, we would suggest the removal of 'to' from the phrase ' then to the Generator' and have it to read as followed: 'then the Generator Operator'. In the last line of the 2nd bullet of R1, insert space between 'Operator' and 'for'.Second bullet of R1 reads: "That the generator is not being operated in the control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing." The language lends itself to the Generator Operator to not operate in control mode for any reason. We would suggest that the language be tightened up and we suggest the following: "that the generator is not capable of operating in control mode as instructed by the Transmission Operator other than start-up, shutdown, or testing". R4 second sentence: add the words "becoming aware of" between the words "of" and "such".M6: after "Requirment 6" add "and shall have evidence of technical justification as provided in Part 6.1".VSL's R3: add at the end "....of the status change".
Response: Thank you for your comments. The standard has been revised for R2-R4, and the second bullet for R1 has been modified for clarity. R4 has been modified to add the phrase "becoming aware of." The VSLs have also been updated to incorporate your feedback.	

Additional comments received from Doug Hils – Duke Energy:

Duke Energy suggests the following revision to R1 for added clarity on the instants when a GOP can have its AVR in another mode other than controlling voltage:

" The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage unless: 1) the generator is exempted by the Transmission Operator 2) the GOP is instructed by the Transmission Operator to operate in a different control mode or 3) the Generator Operator has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- **That the generator is being operated in start-up,1 shutdown,[2] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or**
- **That the generator is not being operated in the control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing. "**

We believe that without this rewording, ambiguity exists of the instances when a GOPs AVR can be different than in service and controlling voltage.

Response: Thank you for your comments. R1 has been modified to provide clarity with regard to AVR settings. R1 clearly states that the AVR must be run in either controlling voltage mode or the mode instructed by the TOP. The only time that the GOP can run in a different mode or in manual is if the GOP has been exempted or the GOP has notified the TOP of one of the bulleted items. Both bullets for R1 still apply to the entire body of R1.

END OF REPORT

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR and supporting package posted for comment on July 19, 2013.
2. Draft standard posted for initial comments and ballot from July 19, 2013 to September 3, 2013.
3. Draft standard posted for additional comments and ballot from October 11, 2013 to November 26, 2013.
4. Draft standard posted for additional comments and ballot from February 27, 2014 to April 14, 2014.

Description of Current Draft

This is the fourth posting of the proposed draft standard. This proposed draft standard will be posted for final ballot.

Anticipated Actions	Anticipated Date
Final Ballot	April 2014
NERC Board of Trustees Adoption	May 2014
Filing to Applicable Regulatory Authorities	May 2014

Version History

Version	Date	Action	Change Tracking
1	5/1/2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and 2.4.3.	July 5, 2006
1a	12/19/2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	1/16/2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	Errata
1.1a	10/29/2008	BOT adopted errata changes; updated version number to "1.1a"	Errata
1.1b	3/3/2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	Revised
2b	4/16/2013	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4. FERC Order issued approving VAR-002-2b.	Revised

Definitions of Terms Used in the Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the NERC Glossary of Terms used in Reliability Standards (Glossary) are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None.

A. Introduction

1. Title: **Generator Operation for Maintaining Network Voltage Schedules**

2. Number: VAR-002-3

3. Purpose: To ensure generators provide reactive support and voltage control, within generating Facility capabilities, in order to protect equipment and maintain reliable operation of the Interconnection.

4. Applicability:

4.1. Generator Operator

4.2. Generator Owner

5. Effective Dates

The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

Rationale for R1: This requirement has been maintained due to the importance of running a unit with its automatic voltage regulator (AVR) in service and in either voltage controlling mode or the mode instructed by the TOP. However, the requirement has been modified to allow for testing, and the measure has been updated to include some of the evidence that can be used for compliance purposes.

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode as instructed by the Transmission Operator unless: 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- That the generator is being operated in start-up,[1] shutdown,[2] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in automatic voltage control mode or in the control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or in a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If a generator is exempted, the Generator Operator shall also have evidence that the generator is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.
[2] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

Rationale for R2:

Requirement R2 details how a Generator Operator (GOP) operates its generator(s) to provide voltage support and when the GOP is expected to notify the Transmission Operator (TOP). In an effort to remove prescriptive notification requirements for the entire continent, the VAR-002-3 standard drafting team (SDT) opted to allow each TOP to determine the notification requirements for each of its respective GOPs based on system requirements. Additionally, a new Part 2.3 has been added to detail that each GOP may monitor voltage by using its existing facility equipment.

Conversion Methodology: There are many ways to convert the voltage schedule from one voltage level to another. Some entities may choose to develop voltage regulation curves for their transformers; others may choose to do a straight ratio conversion; others may choose an entirely different methodology. All of these methods have technical challenges, but the studies performed by the TOP, which consider N-1 and credible N-2 contingencies, should compensate for the error introduced by these methodologies, and the TOP possesses the authority to direct the GOP to modify its output if its performance is not satisfactory. During a significant system event, such as a voltage collapse, even a generation unit in automatic voltage control that controls based on the low-side of the generator step-up transformer should see the event on the low-side of the generator step-up transformer and respond accordingly.

Voltage Schedule Tolerances: The bandwidth that accompanies the voltage target in a voltage schedule should reflect the anticipated fluctuation in voltage at the GOP's Facility during normal operations and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a GOP's AVR control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within each generating Facility's capabilities[4]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive

[3] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.

[4] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a generator is operating in manual control, reactive power capability may change based on stability considerations.

output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

2.2. When instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage or Reactive Power schedule.

For Part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

For Part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's instructions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the instruction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For Part 2.3, for Generator Operators that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall demonstrate the methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

Rationale for R3:

This requirement has been modified to limit the notifications required when an AVR goes out of service and quickly comes back in service. Notifications of this type of status change provide little to no benefit to reliability. Thirty (30) minutes have been built into the requirement to allow a GOP time to resolve an issue before having to notify the TOP of a status change. The requirement has also been amended to remove the sub-requirement to provide an estimate for the expected duration of the status change.

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within 30 minutes of such change, then the Generator Operator is not required to notify the Transmission Operator of the status change *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any status change identified in Requirement R3. If the status has been restored within the first 30 minutes, no notification is necessary.

Rationale for R4:

This requirement has been bifurcated from the prior version VAR-002-2b Requirement R3. This requirement allows GOPs to report reactive capability changes after they are made aware of the change. The current standard requires notification as soon as the change occurs, but many GOPs are not aware of a reactive capability change until it has taken place.

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within 30 minutes of the Generator Operator becoming aware of such change, then the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability in accordance with Requirement R4. If the capability has been restored within the first 30 minutes, no notification is necessary.

Rationale for R5:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected. The prior version of VAR-002-2b, Requirement R4.1.4 (the +/- voltage range with step-change in % for load-tap changing transformers) has been removed. The percentage information was not needed because the tap settings, ranges and impedance are required. Those inputs can be used to calculate the step-change percentage if needed.

R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

5.1. For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

5.1.1. Tap settings.

5.1.2. Available fixed tap ranges.

5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirement R5, Part 5.1.1 through Part 5.1.3 within 30 calendar days.

Rationale for R6:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected.

R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

6.1. If the Generator Owner cannot comply with the Transmission Operator's specifications, the Generator Owner shall notify the Transmission Operator and shall provide the technical justification.

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation in accordance with Requirement R6. The Generator Owner shall have evidence that it notified its associated Transmission Operator when it could not comply with the Transmission Operator's step-up transformer tap specifications in accordance with Requirement R6, Part 6.1.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. The Generator Operator shall maintain all other evidence for the current and previous calendar year.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Real-time Operations**	**Medium**	N/A	N/A	N/A	Unless exempted, the Generator Operator did not operate each generator connected to the interconnected transmission system in the automatic voltage control mode or in a different control mode as instructed by the Transmission Operator, and failed to provide the required notifications to Transmission Operator as identified in Requirement R1.
R2	**Real-time Operations**	**Medium**	N/A	N/A	The Generator Operator did not have a conversion methodology when it monitors voltage at a location different from the schedule provided by the Transmission Operator.	The Generator Operator did not maintain the voltage or Reactive Power schedule as instructed by the Transmission Operator and did not make the necessary notifications required by the Transmission Operator. OR The Generator Operator did not have an operating AVR, and the responsible entity did not use an alternative method for controlling voltage. OR The Generator Operator did not modify voltage when directed, and the responsible entity did not provide any

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						explanation.
R3	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of the status change.
R4	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of becoming aware of the capability change.
R5	**Real-time Operations**	**Lower**	N/A	N/A	The Generator Owner failed to provide its associated Transmission Operator and Transmission Planner one of the types of data specified in Requirement R5 Parts 5.1.1, 5.1.2, and 5.1.3.	The Generator Owner failed to provide to its associated Transmission Operator and Transmission Planner two or more of the types of data specified in Requirement R5 Parts 5.1.1, 5.1.2, and 5.1.3.
R6	**Real-time Operations**	**Lower**	N/A	N/A	N/A	The Generator Owner did not ensure the tap changes were made according the Transmission Operator's specifications. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Generator Owner failed to perform the tap changes, and the Generator Owner did not provide technical justification for why it could not comply with the Transmission Operator specifications.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR and supporting package posted for comment on July 19, 2013.
2. Draft standard posted for initial comments and ballot from July 19, 2013 to September 3, 2013.
3. Draft standard posted for additional comments and ballot from October 11, 2013 to November 26, 2013.
4. Draft standard posted for additional comments and ballot from February 27, 2014 to April 14, 2014.

Description of Current Draft

This is the third fourth posting of the proposed draft standard. This proposed draft standard will be posted for a 45-day formalfinal comment period and parallel ballot.

Anticipated Actions	Anticipated Date
Additional 45-Day SAR Comment Period with Ballot	February/March
Final Ballot	April 2014
NERC Board of Trustees Adoption	May 2014
Filing to Applicable Regulatory Authorities	May 2014

Version History

Version	Date	Action	Change Tracking
1	5/1/2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and 2.4.3.	July 5, 2006
1a	12/19/2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	1/16/2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	Errata
1.1a	10/29/2008	BOT adopted errata changes; updated version number to "1.1a"	Errata
1.1b	3/3/2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	Revised
2b	4/16/2013	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4. FERC Order issued approving VAR-002-2b.	Revised

Definitions of Terms Used in the Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the NERC Glossary of Terms used in Reliability Standards (Glossary)~~Reliability Standards Glossary of Terms~~ are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None.

A. Introduction

1. Title: **Generator Operation for Maintaining Network Voltage Schedules**

2. Number: VAR-002-3

3. Purpose: To ensure generators provide reactive support and voltage control, within generating Facility capabilities, in order to protect equipment and maintain reliable operation of the Interconnection.

4. Applicability:

4.1. Generator Operator

4.2. Generator Owner

5. Effective Dates

The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

B. Requirements and Measures

Rationale for R1: This requirement has been maintained due to the importance of running a unit with its automatic voltage regulator (AVR) in service and in either voltage controlling mode or the mode instructed by the TOP. However, the requirement has been modified to allow for testing, and the measure has been updated to include some of the evidence that can be used for compliance purposes.

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode~~,~~ as instructed by the Transmission Operator unless: 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- That the generator is being operated in start-up,[1] shutdown,[2] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in automatic voltage control mode or in the control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or in a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If a generator is exempted, the Generator Operator shall also have evidence that the generator is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.
[2] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

Rationale for R2:

Requirement R2 details how a Generator Operator (GOP) operates its generator(s) to provide voltage support and when the GOP is expected to notify the Transmission Operator (TOP). In an effort to remove prescriptive notification requirements for the entire continent, the VAR-002-3 standard drafting team (SDT) opted to allow each TOP to determine the notification requirements for each of its respective GOPs based on system requirements. Additionally, a new ~~p~~Part 2.3 has been added to detail that each GOP may monitor voltage by using its existing facility equipment.

Conversion Methodology: There are many ways to convert the voltage schedule from one voltage level to another. Some entities may choose to develop voltage regulation curves for their transformers; others may choose to do a straight ratio conversion; others may choose an entirely different methodology. All of these methods have technical challenges, but the studies performed by the TOP, which consider N-1 and credible N-2 contingencies, should compensate for the error introduced by these methodologies, and the TOP possesses the authority to direct the GOP to modify its output if its performance is not satisfactory. During a significant system event, such as a voltage collapse, even a generation unit in automatic voltage control that controls based on the low-side of the generator step-up transformer should see the event on the low-side of the generator step-up transformer and respond accordingly.

Voltage Schedule Tolerances: The bandwidth that accompanies the voltage target in a voltage schedule should reflect the anticipated fluctuation in voltage at the GOP's Facility during normal operations and be based on the TOP's assessment of N-1 and credible N-2 system contingencies. The voltage schedule's bandwidth should not be confused with the control dead-band that is programmed into a GOP's AVR control system, which should be adjusting the AVR prior to reaching either end of the voltage schedule's bandwidth.

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within each generating Facility's capabilities[4]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive

[3] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.

[4] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a generator is operating in manual control, reactive power capability may change based on stability considerations.

output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

2.2. When instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage or Reactive Power schedule.

For ~~p~~Part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

For ~~p~~Part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's instructions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the instruction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For ~~p~~Part 2.3, for Generator Operators that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall demonstrate the methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator~~document or be able to demonstrate the method of conversion from the voltage level monitored to the voltage level specified on the voltage schedule~~.

Rationale for R3:

This requirement has been modified to limit the notifications required when an AVR goes out of service and quickly comes back in service. ~~Such n~~Notifications of this type of status change provide little to no benefit to reliability. Thirty (30) minutes have been built into the requirement to allow a GOP time to resolve an issue before having to notify the TOP of a status ~~or capability~~ change. The requirement has also been amended to remove the sub-requirement to provide an estimate for the expected duration of the status change. ~~The 30-minute window should resolve most issues.~~

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within 30 minutes of such change, then ~~to~~ the Generator Operator is not required to notify the Transmission Operator of the status change *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any status change identified in Requirement R3. If the status has been restored within the first 30 minutes, no notification is necessary.

Rationale for R4:

This requirement has been bifurcated from the prior version VAR-002~~0~~-2b Requirement R3. This requirement allows GOPs to report reactive capability changes after they are made aware of the change. The current standard requires notification as soon as the change occurs, but many GOPs are not aware of a reactive capability change until it has taken place.

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within ~~-~~30 minutes of the Generator Operator becoming aware of such change, then ~~to~~ the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes ~~-~~of becoming aware of a change in reactive capability in accordance with Requirement R4. If the capability has been restored within the first 30 minutes, no notification is necessary.

Rationale for R5:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected. The prior version of VAR-002-2b, Requirement ~~subpart~~ Part R4.1.4 (the +/- voltage range with step-change in % for load-tap changing transformers) has been removed. The percentage information was not needed because the tap settings, ranges and impedance are required. Those inputs can be used to calculate the step-change percentage if needed.

R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

5.1. For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

5.1.1. Tap settings.

5.1.2. Available fixed tap ranges.

5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirement R5, P~~p~~art 5.1.1 through ~~p~~Part 5.1.3 within 30 calendar days.

Rationale for R6:

This requirement and corresponding measure have been maintained due to the importance of having accurate tap settings. If the tap setting is not properly set, then the VARs available from that unit can be affected.

R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

6.1. If the Generator Owner cannot comply with the Transmission Operator's specifications, the Generator Owner shall notify the Transmission Operator and shall provide the technical justification.

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation in accordance with Requirement R6. The Generator Owner shall have evidence that it notified its associated Transmission Operator when it could not

comply with the Transmission Operator's step-up transformer tap specifications in accordance with Requirement R6, Ppart 6.1.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. The Generator Operator shall maintain all other evidence for the current and previous calendar year.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Real-time Operations**	**Medium**	N/A	N/A	N/A	Unless exempted, the Generator Operator did not operate each generator connected to the interconnected transmission system in the automatic voltage control mode or in a different control mode~~,~~ as instructed by the Transmission Operator, and failed to provide the required notifications to Transmission Operator as identified in Requirement R1.
R2	**Real-time Operations**	**Medium**	N/A	N/A	The Generator Operator did not have a conversion methodology when it monitors voltage at a location different from the schedule provided by the Transmission Operator.	The Generator Operator did not maintain the voltage or Reactive Power schedule as ~~directed~~ instructed by the Transmission Operator and did not make the necessary notifications required by the Transmission Operator. OR The Generator Operator did not have an operating AVR, and the responsible entity did not use an alternative method for controlling voltage. OR The Generator Operator did not modify voltage when directed, and the responsible entity did not provide any

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						explanation.
R3	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of the status change.
R4	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of becoming aware of the capability change.
R5	**Real-time Operations**	**Lower**	N/A	N/A	The Generator ~~Operator~~ Owner failed to provide its associated Transmission Operator and Transmission Planner one of the types of data specified in Requirement R5 ~~p~~Parts 5.1.1, 5.1.2, and 5.1.3.	The Generator ~~Operator~~ Owner failed to provide to its associated Transmission Operator and Transmission Planner two or more of the types of data specified in Requirement R5 ~~p~~Parts 5.1.1, 5.1.2, and 5.1.3.
R6	**Real-time Operations**	**Lower**	N/A	N/A	N/A	The Generator Owner did not ensure the tap changes were made according the Transmission Operator's specifications. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Generator Owner failed to perform the tap changes, and the Generator Owner did not provide technical justification for why it ~~cannot~~ could not comply with the Transmission Operator specifications.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

VAR Directives Project

Implementation Plan for VAR-001-4 and VAR-002-3

Approvals Required

VAR-001-4 – Voltage and Reactive Control
VAR-002-3 — Generator Operation for Maintaining Network Voltage Schedules

Prerequisite Approvals

There are no other standards that must receive approval prior to the approval of this standard.

Revisions to Glossary Terms

None

Applicable Entities

Generator Operators (VAR-002-3)

Generator Owners (VAR-002-3)

Transmission Operators (VAR-001-4)

Applicable Facilities

N/A

Conforming Changes to Other Standards

None

Effective Dates

VAR-001-4 and VAR-002-3 – All requirements shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-001-4 and VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Justification

The currently effective VAR-002 standard is one of the most violated standards; however, the industry argues these violations do not address any reliability gaps. Instead, Generator Operators and Transmission Operators are required to handle many nuisance phone calls for slight deviations from a voltage schedule. The nuisance phone calls can be a distraction during a scheduled maintenance or a system event; thus, the industry would support making the changes as soon as possible. However, since VAR-001 now requires determining voltage and reactive power schedules with associated tolerance bands in addition to any notification requirements, the Transmission Operators need a quarter to prepare documentation. The VAR-002 standards cannot go into effect without the new TOP schedules and notification requirements. Also for Transmission Operators that do not already provide tolerance bands with voltage schedules, those Transmission Operators will need some time to adjust to providing new data (more specifically, the criteria for schedules) to Generator Operators.

Retirements

VAR-001-3 and VAR-002-2b will be retired at midnight of the day immediately prior to the Effective Date of VAR-001-4 and VAR-002-3 in the particular jurisdiction in which the new standards are becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

VAR Directives Project

Implementation Plan for VAR-001 and VAR-002

Approvals Required

VAR-001-4 – Voltage and Reactive Control
VAR-002-3 — Generator Operation for Maintaining Network Voltage Schedules

Prerequisite Approvals

There are no other standards that must receive approval prior to the approval of this standard.

Revisions to Glossary Terms

None

Applicable Entities

Generator Operators (VAR-002-3)

Generator Owners (VAR-002-3)

Transmission Operators (VAR-001-4)

~~Reliability Coordinators~~

Applicable Facilities

N/A

Conforming Changes to Other Standards

None

Effective Dates

VAR-001-4 and VAR-002-3 – All requirements ~~- In those jurisdictions where regulatory approval is required, this standard~~ shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority ~~regulatory approval~~ or as otherwise provided for in a jurisdiction where approval by an~~made effective pursuant to the laws~~ applicable ~~to such ERO~~ governmental authority~~authorities. In those jurisdictions where no regulatory approval~~ is required for a~~, this~~ standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-001-4 and VAR-002-3 shall become effective on the first

day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction~~approval~~.

Justification

The currently effective VAR-002 standard is one of the most violated standards; however, the industry argues these violations do not address any reliability gaps. Instead, Generator Operators and Transmission Operators are required to handle many nuisance phone calls for slight deviations from a voltage schedule. The nuisance phone calls can be a distraction during a scheduled maintenance or a system event; thus, the industry would support making the changes as soon as possible. However, since VAR-001 now requires determining voltage and reactive power schedules with associated tolerance bands in addition to any notification requirements~~a documented policy or procedure for assessments~~,~~;~~ the Transmission Operators need a quarter to prepare documentation. The VAR-002 standards cannot go into effect without the new TOP schedules and notification requirements. Also for Transmission Operators that do not already provide tolerance bands with voltage schedules, those Transmission Operators will need some time to adjust to providing new data (more specifically, the criteria for schedules) to Generator Operators.

Retirements

VAR-001-3 and VAR-002-2b will be retired at midnight of the day immediately prior to the Effective Date of VAR-001-4 and VAR-002-3 in the particular j~~J~~urisdiction in which the new standards are becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Operations

Draft Reliability Standard Compliance Guidance for VAR-001-4 and VAR-002-3
October 21, 2013

Introduction

The NERC Compliance department (Compliance) worked with the VAR standard drafting team (SDT) to review the proposed standards VAR-001-4 and VAR-002-3. The purpose of the review was to discuss the requirements of the proposed standard to obtain an understanding of its intended purpose and the evidence necessary to support compliance. The purpose of this document is to address specific questions posed by the VAR SDT in order to aid in the drafting of the requirements and provide a level of understanding regarding evidentiary support necessary to demonstrate compliance.

While all compliance evaluations require levels of auditor judgment, participating in these reviews allows Compliance to develop training and approaches to support a high level of consistency in audits conducted by the Regional Entities. The following questions and answers are intended to assist the SDT in further refining the standard and to serve as a resource in the development of training for auditors.

VAR-001 and VAR-002 Questions

Question 1

How will compliance determine if sufficient reactive resources were scheduled as part of VAR-001-4 Requirement R2?

Compliance Response to Question 1

For VAR-001-4 Requirement R2, an auditor would review the studies that a TOP used to schedule resources to see that the studies show whether new resources should be brought online, or if the resources online are sufficient to regulate voltage levels. An auditor may observe a TOP reviewing the study and scheduling live and may pull samples from various time periods to determine whether a TOP scheduled resources as required in the study.

Question 2

Is it clear that VAR-001-4 Requirement R4 allows for exemptions, for any duration, from: 1) voltage schedules, 2) being in automatic voltage control mode, or 3) any notification requirements?

Compliance Response to Question

It is clear that VAR-001 Requirement R4 allows for any combination of exemptions for generator operators from 1) voltage schedules, 2) being in automatic voltage control mode, or 3) any notification requirements, as long as the

exemption meets the criteria specified by the TOP. An auditor will not look for any pre-authorization from the TOP; rather an auditor will verify that the generator operator has met the criteria set forth by the TOP.

Question 3

Tolerance bands apply to a set voltage or Reactive Power number with a +/- percentage as the tolerance band. The voltage range or Reactive Power range is a high and low number that a Generator Operator is expected to operate within for reliability purposes. With regard to VAR-001-4 Requirement R5, is it clear that when a voltage range or Reactive Power range is provided as a schedule, a tolerance band is not expected to also be provided?

Compliance Response to Question 3

Yes, it is clear based on VAR-001-4 Requirement R5 that a voltage or Reactive power schedule can be either: 1) a target number with a tolerance band, OR 2) a voltage or Reactive Power range to operate within. An auditor would not expect to see a tolerance band provided with an operating range for voltage or Reactive Power.

Question 4

With regard to VAR-002-3, will generators receive a violation for instances where a system event is affecting system voltage, but the generators made the appropriate conversions and set the AVRs to meet the original schedule provided by the TOP?

Compliance Response to Question 4

No, the generator operators can only be responsible for maintaining the schedule provided by the TOP based on existing facility equipment. In the event that a generator operator does not have the equipment to have visibility of high-side system voltage, the GOP will not have the ability to adjust VARs to maintain system voltage. An auditor is not to determine that, where the GOP does not have the high side monitoring equipment and where the AVR is set appropriately based on existing facility equipment, the generator operator is non-compliant. However, if the TOP provides a new directive or schedule, the GOP is required to follow the new directive. This directive can include modifying an AVR setting or providing more voltage support, and the generator operator is expected to comply pursuant to VAR-002-3.

Question 5

Related to VAR-002-3, generators can monitor voltage on either the low side and high side of the GSU (depending on equipment limitation) and the “number” being monitored by the Generator will not always equate to the number provided by the TOP. Is it clear that VAR-002 Requirement R2, part 2.3 only wants a conversion of the schedule provided to the number monitored? Is it clear that there should not be a violation if the schedule does not match the number being monitored on the low side as long as there is a documented conversion?

Compliance Response to Question 5

The Generator should be able to provide documentation that identifies the "number" being monitored and the calculation demonstrating how the "number" equates to the schedule provided by the TOP. The measure for VAR-002-3 Requirement R2, part 2.3 is clear on what evidence should be able to demonstrate this during an audit.

Question 6

VAR-002-3, Requirement R4 was added because generators cannot report a capability change until they are aware of the change. The currently enforceable standard requires a notification as soon as the capability change occurs; however, many times the change occurred well before the generators were aware of the problem. Is it clear that VAR-002-3 Requirement R4 is only violated after the generator is made aware of the change?

Compliance Response to Question 6

It is clear that VAR-002-3, Requirement R4 will only be a violation if the change is not reported after 30 minutes of becoming aware of the reactive capability change. An auditor will ask an entity for evidence to demonstrate when it became aware of the change in reactive capability. This will not be purely subjective; there are technical instances where it will be clear that an entity would have been made aware of the change in reactive capability. For example, one instance is where a unit is ramping to an expected VAR output, and it cannot reach it; a reactive capability change has occurred.

Conclusion

Following final approval of the Reliability Standard, Compliance will develop the final Reliability Standards Auditor Worksheet (RSAW) and associated training.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VAR-002 Mapping Document

Transition of VAR-002-2b

Standard: VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b, R1	Requirement R1	The requirement has been modified to allow for testing and exemptions for other AVR modes when necessary. This requirement was also modified to allow GOPs to operate in a different control mode as instructed by the TOP.
VAR-002-2b, R2	Requirement R2	The new requirement has been updated to allow for the TOP to define notification requirements. The requirement also adds parts to allow for the conversion of a high side schedule to a low side number for monitoring purposes. Reactive Power schedules have been added for generators that use those schedules, and for consistency purposes "unit" has been changed to "generator".

Standard: VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b, R3	Requirement R3 and R4.	The old requirement has been broken into two requirements: 1) one for AVR/PSS status, and 2) one for reactive capability. Both allow 30 minutes to correct an issue before having to notify the TOP.
VAR-002-2b, R3	Requirement R5	The requirement has been modified to remove the sub-part that requires the GOP to provide "[t]he +/- voltage range with step-change in % for load-tap changing transformers." The measure was also modified to add that a GOP must provide the data "within 30 calendar days"
VAR-002-2b, R4	Requirement R6	The requirement has been updated to apply to the same functional entity for the Requirement and sub-part.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

VAR-002 Mapping Document

Transition of VAR-002-2b

Standard: VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b, R1	Requirement R1	The requirement has been modified to allow for testing and exemptions for other AVR modes when necessary. This requirement was also modified to allow GOPs to operate in a different control mode as instructed by the TOP.
VAR-002-2b, R2	Requirement R2	The new requirement has been updated to allow for the TOP to define notification requirements. The requirement also adds parts to allow for the conversion of a high side schedule to a low side number for monitoring purposes. Reactive Power schedules have been added for generators that use those schedules, and for consistency purposes "unit" has been changed to "generator".

Standard: VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules		
Requirement in Approved Standard	**Transitions to the below Requirement in New Standard or Other Action**	**Description and Change Justification**
VAR-002-2b, R3	Requirement R3 and R4.	The old requirement has been broken into two requirements: 1) one for AVR/PSS status, and 2) one for reactive capability. Both allow ~~15~~ 30 minutes to correct an issue before having to notify the TOP.
VAR-002-2b, R3	Requirement R5	The requirement has ~~not been modified~~been modified to remove the sub-part that requires the GOP to provide "[t]he +/- voltage range with step-change in % for load-tap changing transformers." The measure was also modified to add that a GOP must provide the data "within 30 calendar days"~~.~~
VAR-002-2b, R4	Requirement R6	The requirement has ~~not been modified.~~been updated to apply to the same functional entity for the Requirement and sub-part.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Reliability Standard Audit Worksheet[1]

VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	Audit
Names of Auditors:	Supplied by CEA

Applicability of Requirements *[RSAW developer to insert correct applicability]*

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1				X											
R2				X											
R3				X											
R4				X											
R5			X												
R6			X												

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Subject Matter Experts

Identify Subject Matter Expert(s) responsible for this Reliability Standard. (Insert additional rows if necessary)

Registered Entity Response (Required):

SME Name	Title	Organization	Requirement(s)

DRAFT

R1 Supporting Evidence and Documentation

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode, as instructed by the Transmission Operator unless ~~the Generator Operator~~ 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following:

- That the generator is being operated in start-up,[3] shutdown,[4] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in the ~~automatic voltage~~ control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence ~~must~~ may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If a generator is exempted, the Generator Operator shall also have evidence that the generator ~~it~~ is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

Registered Entity Response to Question (Required):

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[5]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this

[3] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.
[4] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.
[5] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M1.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R1
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	For instances where entity did not operate a generator in automatic voltage control mode or in a different control mode, as instructed by the Transmission Operator, ensure notification was given to the Transmission Operator in accordance with Requirement R1.

Note to Auditor: Auditors can identify instances where entities did not operate~~d~~ generators ~~outside of~~in automatic voltage control mode, or in a different control mode, as instructed by the Transmission Operator, through their general knowledge of the interconnected transmission system in the entity's area. Auditor knowledge is obtained through activities such as conversations with the entity under audit or the Transmission Operator, and an awareness of events occurring on the interconnected transmission system. In situations where the entity's compliance with this requirement poses little risk to the BES, conversations with other entities, such as Transmission Operators, is most likely not necessary.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[6] (within each generating Facility's capabilities[7]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator.

2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive output to meet the voltage or Reactive Power schedule ~~directed~~ provided by the Transmission Operator.

2.2. When ~~directed~~ instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a ~~unit~~ generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage or Reactive Power schedule.

For part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule ~~directed~~ provided by the Transmission Operator.

For part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's ~~directions~~ instructions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the

[6] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.

[7] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a ~~Generator~~ generator is operating in manual control, reactive power capability may change based on stability considerations.

~~direction~~instruction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For part 2.3, for ~~units~~ Generator Operators that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall document or be able to demonstrate the method of conversion from the voltage level monitored to the voltage level specified on the voltage schedule.

Question: As a Generation Operator, have you operated the generator with the AVR out of service?

Registered Entity Response to Question (Required):

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[8]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M2.
Any written policies, procedures or protocols describing how the entity maintains the generator voltage or Reactive Power schedule provided by Transmission Operator, if the entity has such documents.
Generator voltage or Reactive Power schedule provided to entity by Transmission Operator, or entity's record thereof, for timeframes selected by the auditor.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

[8] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

Compliance Assessment Approach Specific to VAR-002-3, R2

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Interview entity staff and/or review documentation provided by the entity to understand how they maintain the generator voltage or Reactive Power schedule or authorized exemption per Requirement R2.
	Read entity's response to compliance Question above and understand how entity complies with Requirement R2, when they operate a generator with AVR in not in service.
	Select a sample of timeframes during the audit period and have entity walkthrough how they complied with Requirement R2 for those timeframes.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough timeframes, per above, to gain reasonable assurance that entity is complying with Requirement R2.

For part 2.3, the entity should be able to provide documentation that identifies the voltage number being monitored and the calculation demonstrating how it equates to the schedule provided by the Transmission Operator. The measure for VAR-002-3 Requirement R2, part 2.3 is clear on what evidence should be able to demonstrate this during an audit. The entity can only be responsible for maintaining the schedule provided by the Transmission Operator based on existing facility equipment. In the event that an entity does not have the equipment to have visibility of high-side system voltage, the entity will not have the ability to adjust VARs to maintain system voltage. An auditor is not to determine that, where the entity does not have the high side monitoring equipment and where the AVR is set appropriately based on existing facility equipment, the entity is non-compliant. However, if the Transmission Operator provides a new directive or schedule, the entity is required to follow the new directive. This directive can include modifying an AVR setting or providing more voltage support, and the entity is expected to comply pursuant to VAR-002-3.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within ~~the first 15~~30 minutes of such change, then the Generator Operator is not required to ~~there is no need to~~ notify the Transmission Operator of the status change.

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of ~~the~~ any status change identified in Requirement R3. If the status has been restored within the first ~~15~~ 30 minutes, no notification is necessary~~; therefore, if a status change lasts more than 15 minutes, the GOP must notify its associated Transmission Operator within 30 minutes of when the change first occurred~~.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[9]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
Any written policies, procedures or protocols describing how the entity responds to a status change on AVR, if the entity has such documents. An example of entity's response to a status change on AVR provided by entity, if applicable.
Auditor may select certain instances where entity had a status change on AVR. In such instances, provide associated evidence of awareness and resolution/notification.
Evidence as outlined in M3.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

[9] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

Compliance Assessment Approach Specific to VAR-002-3, R3
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Interview entity staff and/or review documentation provided by the entity to understand how they respond to status changes on AVR.
	Review evidence provided to determine if entity responded to status change on AVR in accordance with Requirement R3.

Note to Auditor: Based on the risk of the entity's compliance with this requirement on the Bulk Electric System (BES) and the auditor's assessment of the entity's management practices (or internal controls) over compliance with this Requirement, auditors will determine the extent of the above audit procedures to apply. In cases where risk to the BES is low and the entity's management practices, gleaned by the auditor through walkthroughs or documentation review, are sound only limited audit testing is necessary. In cases where risk is higher and controls are less effective, an auditor should sample enough timeframes, per above, to gain reasonable assurance that entity is complying with Requirement R3.

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes after becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within the first 15 minutes of such change, then there is no need to notify the Transmission Operator.

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of the recognition of a reactive capability change identified in Requirement R4. If the capability has been restored within the first 15 minutes, no notification is necessary; therefore, if a capability change lasts more than 15 minutes, the Generator Operator must notify its associated Transmission Operator within 30 minutes of when the change first occurred.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[10]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
Any written policies, procedures or protocols describing how the entity responds to a change in reactive capability, if the entity has such documents. An example of entity's response to a change in reactive capability provided by entity, if applicable.
Auditor may select certain instances where entity ~~should~~ may have been aware of a status change in reactive capability. In such instances, provide associated evidence of awareness and resolution/notification. See Note to Auditor for additional details.
Evidence as outlined in M4.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R4
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Interview entity staff and/or review documentation provided by the entity to understand how they respond to change in reactive capability.
	Review evidence provided to determine if entity responded to change in reactive capability in accordance with Requirement R4.
Note to Auditor: It is clear that VAR-002-3, Requirement R4 will only be a violation if the change is not reported after 30 minutes of becoming aware of the status change in reactive capability. An auditor will ask an entity for evidence to demonstrate when it became aware of the change. This will not be purely	

[10] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

subjective; there are technical instances (e.g. unit trips, ramping, equipment/AVR failures) where it ~~will be~~is ~~clear~~ likely that an entity ~~would have been~~was made aware of the change in reactive capability. ~~For example, one instance is where a unit is ramping to an expected VAR output, and it cannot reach it; a reactive capability change has occurred.~~

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request.

5.1. For generator step-up transformers and auxiliary transformers with primary voltages equal to or greater than the generator terminal voltage:

5.1.1. Tap settings.

5.1.2. Available fixed tap ranges.

5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirements R5 part 5.1.1 through part 5.1.3.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[11]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
Evidence as outlined in M4. Evidence of transmittal of the data could include, but is not limited to, items such as an electronic message or a transmittal letter with the information included or attached.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted:

[11] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R5
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Review evidence (documented date of request and reply) to determine if entity responded to information request(s) as required in Requirement R5 within 30 days of receiving a request from associated Transmission Operator.
Note to Auditor: Based on the auditors professional judgment, he or she may confirm with Transmission Operators to determine if requests for data were made or simply confirm the existence of such requests with the entity under audit.	

Auditor Notes:

R6 Supporting Evidence and Documentation

R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement.

6.1. If the Generator Operator cannot comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation as identified in Requirement R6. The Generator Operator shall have evidence that it notified its associated Transmission Operator when it could not comply with the Transmission Operator's step-up transformer tap specifications as identified in Requirement R6 part 6.1.

Registered Entity Response to General Compliance with this Requirement (Required):
Describe, in narrative form, how you meet compliance with this Requirement. Provide a brief explanation, in your own words, of how you meet compliance with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[12]:

Provide the following evidence, or other evidence to demonstrate compliance. If the provisioning of this evidence is burdensome or otherwise unreasonable, contact your CEA to arrange for sampling or other means of reduction of the quantity of evidence submitted.
See M6.

Registered Entity Evidence (Required):

The following information is recommended for all evidence submitted: File Name, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to VAR-002-3, R6
This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	Review evidence (documented date of request and response) to determine if entity responded to change(s) as required in Requirement R6.
Note to Auditor: Based on the auditors professional judgment, he or she may confirm with Transmission Operators to determine if requests for changes to transformer tap positions were made or simply confirm the existence of such requests with the entity under audit.	

[12] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

Auditor Notes:

Revision History

Version	Date	Reviewers	Revision Description
1	11/XX/2013	NERC Ceompliance, Standards	New Document
2	3/14/2014	NERC Compliance, Standards	Revisions based on changes to underlying Reliability Standard.

DRAFT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules

This document provides the Standard Drafting Team's (SDT) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project. A copy of the standard with the associated VRFs and VSLs is available here.

NERC Criteria - Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Violation Risk Factor Guidelines

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

The Commission seeks to ensure that Violation Risk Factors assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities

• Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

Guideline (3) – Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) –Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria - Violation Severity Levels

Violation Severity Levels (VSLs) define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

Violation severity levels should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

FERC's VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline 1 – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline 2 – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3 – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline 4 – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the

Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justification – VAR-002-3 Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium is necessary because this requirement could affect the stability of the BES, but the requirement itself addresses instances where a GOP will not necessarily operate in with the AVR in different control modes or when the TOP will instruct a GOP to operate in other modes.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although the Blackout Report list Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, the GOP control modes are not as critical because the TOP is monitoring the system. The companion requirement to VAR-002-3 (in VAR-001-4) are properly designated with a HIGH VRF to ensure voltage schedules are provided as part of the TOPs plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The VRF applies to the entire requirement.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: Because maintaining a voltage schedule is critical to preventing a violation of a System Operating Limit, this VRF was drafted to be the same VRFs for VAR-001-4 Requirement R5. VAR-001-4 Requirement R5 requires the TOP to specify a schedule and notification requirements that the GOP must follow.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a GOP not operating in the proper control mode can affect the BES, but a single violation is unlikely to lead to instability, separation, or cascading failure. This is especially the case since a TOP will also be monitoring for voltage deviations.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More Than One Obligation:

	This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level.

VSL Justification – VAR-002-3 Requirement R1	
NERC VSL Guidelines	Consistent with NERC's VSL Guideline, this VSL acknowledges the criticality of this requirement and whether or not a system voltage schedule was created.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The current level of compliance is not lowered with the proposed VSL because this requirement only has a "severe" VSL.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary, and therefore, a single severe VSL is necessary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is consistent with the corresponding requirements.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on a cumulative number of violations.

VRF Justification – VAR-002-3 Requirement R2	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium is consistent with the NERC VRF definition. Requirement R2 focuses on GOPs maintaining a schedule, but there could be system events that will pull a GOP out of schedule. Also, late at night and early in the morning, the system may experience instances of low or high voltage. This could impact the BES, but a single instance is unlikely to lead to instability, separation, or cascading failure. The sub-requirements also require the GOP to modify the voltage schedule when directed by the TOP.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although the Blackout Report lists Reactive Power and voltage control as critical areas where a violation could severely affect the reliability of the Bulk-Power System, there are general times when a GOP will be unable to maintain a voltage schedule due to system condition. These instances occur frequently during the early morning and late at night. The companion requirement to VAR-002-3 (in VAR-001-4) are properly designated

	with a HIGH VRF to ensure voltage schedules are provided as part of the TOP's plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The VRF applies to the entire requirement, including all sub-parts.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: Because maintaining a voltage schedule is critical to preventing a violation of a System Operating Limit, this VRF was drafted to be the same VRFs for VAR-001-4 Requirement R5. VAR-001-4 Requirement R5 requires the TOP to specify a schedule and notification requirements that the GOP must follow.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a GOP not maintaining a schedule can affect the BES, but a single violation is unlikely to lead to instability, separation, or cascading failures. This is especially the case since a TOP will also be monitoring for voltage deviations
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation: This VRF does not co-mingle multiple objectives, nor does it water down the requirement to reflect a lower risk level.

VSL Justification – VAR-002-3 Requirement R2	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines, the VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering	There is no prior compliance obligation related to the subject of this standard.

the Current Level of Compliance	
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation,	The proposed VSL is not based on cumulative number of violations.

Not on A Cumulative Number of Violations	

VRF Justification – VAR-002-3 Requirement R3	
Proposed VRF	**Medium**
NERC VRF Discussion	This requirement warrants a Medium VRF and is consistent with the NERC definition because this requirement is whether the GOP made the required notifications to the TOP within the appropriate timeframes.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although the Blackout Report list Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, the GOP notifications are unlikely to lead to system instability, separation, or cascading failures. This is particularly the case because the TOP is still operating the system to stay within System Operating Limits and Interconnection Reliability Operating Limits.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: There is no sub-part to Requirement 3; therefore, the requirement is consistent.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: This VRF is drafted to be consistent with other standards (e.g., BAL) that address making appropriate notifications.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because not making the appropriate notifications can impact the grid, but the TOPs are still effectively monitoring the system; thus, instability, separation, or cascading failures are unlikely due to a single violation.
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level

VSL Justification – VAR-002-3 Requirement R3	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The current level of compliance is not lowered with the proposed VSL.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary because the standard is violated only when a notification is not made to the TOP; therefore, a severe VSL is warranted. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be	The proposed VSL is worded consistently with the corresponding requirement.

Consistent with the Corresponding Requirement	
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

VRF Justification – VAR-002-3 Requirement R4	
Proposed VRF	**Medium**
NERC VRF Discussion	This requirement warrants a Medium VRF and is consistent with the NERC definition because this requirement is whether the GOP made the required notifications to the TOP within the appropriate timeframes.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although the Blackout Report list Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, the GOP notifications are unlikely to lead to system instability, separation, or cascading failures. This is particularly the case because the TOP is still operating the system to stay within System Operating Limits and Interconnection Reliability Operating Limits.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: There is no sub-part to Requirement 3; therefore, the requirement is consistent.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: This VRF is drafted to be consistent with other standards (e.g., BAL) that address making appropriate notifications.

FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because not making the appropriate notifications can impact the grid, but the TOPs are still effectively monitoring the system; thus, instability, separation, or cascading failures are unlikely due to a single violation.
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level

VSL Justification – VAR-002-3 Requirement R4	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The current level of compliance is not lowered with the proposed VSL.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary because the standard is violated only when a notification is not made to the TOP; therefore, a severe VSL is warranted.

"Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

VRF Justification – VAR-002-3 Requirement R5	
Proposed VRF	**Lower**
NERC VRF Discussion	This requirement is a Lower VRF because the tap setting data does not change frequently, and a violation is not expected adversely affect the BES.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, this requirement would not adversely impact the BES

	if violated. The tap information is provided during interconnection, and it is not expected to change frequently. Therefore, a Lower VRF is warranted.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The parts within Requirement R5 are consistent with Requirement R5 and is considered a Lower VRF.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: There are no other standards that address Tap settings.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a violation is similar to an administrative violation. Further, since tap settings are infrequently changed, a violation would not adversely impact the BES.
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation: This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level.

VSL Justification – VAR-002-3 Requirement R5	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering	There is no prior compliance obligation related to the subject of this standard.

the Current Level of Compliance	
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation,	The proposed VSL is not based on cumulative number of violations.

Not on A Cumulative Number of Violations	

VRF Justification – VAR-002-3 Requirement R6	
Proposed VRF	**Lower**
NERC VRF Discussion	This requirement is a Lower VRF because the tap setting data does not change frequently, and a violation is not expected adversely affect the BES.
FERC VRF G1 Discussion	Guideline 1 – Consistency with Blackout Report: Although Reactive Power and voltage control are part of the list of critical areas where a violation could severely affect the reliability of the Bulk-Power System, this requirement would not adversely impact the BES if violated. The tap information is provided during interconnection, and it is not expected to change frequently. If a violation were to occur, the system would still operate at the level prior to making any tap setting changes. Therefore, a Lower VRF is warranted.
FERC VRF G2 Discussion	Guideline 2 – Consistency within a Reliability Standard: The part within Requirement R6 is consistent with Requirement R6 and is considered a Lower VRF.
FERC VRF G3 Discussion	Guideline 3 – Consistency among Reliability Standards: There are no other standards that address Tap settings.
FERC VRF G4 Discussion	Guideline 4 – Consistency with NERC Definitions of VRFs: This VRF is consistent with the NERC Definition because a violation is similar to an administrative violation. Further, since tap settings are infrequently changed, a violation would not adversely impact the BES.
FERC VRF G5 Discussion	Guideline 5 - Treatment of Requirements that Co-mingle More Than One Obligation:

	This VRF does not co-mingle multiple objectives, nor does it water down the Requirement to reflect a lower risk level.

VSL Justification – VAR-002-3 Requirement R6	
NERC VSL Guidelines	Consistent with NERC's VSL Guidelines. The VSL describes degrees of noncompliant performance in an incremental manner.
FERC VSL G1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The single VSL assignment category for "Binary" Requirements is not consistent Guideline 2b: VSL Assignments that contain ambiguous language	The proposed VSL is written to ensure uniformity and consistency in the determination of penalties. Guideline 2a: The proposed VSL is binary because the requirement focuses on whether tap changes were made. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

FERC VSL G3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL is worded consistently with the corresponding requirement.
FERC VSL G4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The proposed VSL is not based on cumulative number of violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-002-3

Final Ballot Now Open through May 5, 2014

Now Available

A final ballot for **VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules** is open through **8 p.m. Eastern on Monday, May 5, 2014.**

Background information for this project can be found on the project page.

Instructions for Balloting

In the final ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their previously cast votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the final ballot window. If a ballot pool member does not participate in the final ballot, that member's vote cast in the previous ballot will be carried over as that member's vote in the final ballot.

Members of the ballot pool associated with this project may log in and submit their vote for the standard by clicking here.

Next Steps

Voting results for the standard will be posted and announced after the ballot window closes. If approved, it will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2013-04 Voltage and Reactive Control
VAR-002-3

Final Ballot Results

Now Available

A final ballot for **VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules** concluded at **8 p.m. Eastern on Monday, May 5, 2014.**

The standard achieved a quorum and sufficient affirmative votes for approval. Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results for the ballot.

Standard	Quorum / Approval
VAR-002-3	83.84% / 88.26%

Background information for this project can be found on the project page.

Next Steps

The standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

For information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller (via email), Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results

Ballot Name:	Project 2013-04 Voltage and Reactive Control VAR-002-3
Ballot Period:	4/23/2014 - 5/5/2014
Ballot Type:	Final
Total # Votes:	332
Total Ballot Pool:	396
Quorum:	**83.84 % The Quorum has been reached**
Weighted Segment Vote:	88.26 %
Ballot Results:	**A quorum was reached and there were sufficient affirmative votes for approval.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	106	1	65	0.867	10	0.133	0	9	22
2 - Segment 2	9	0.6	6	0.6	0	0	0	3	0
3 - Segment 3	86	1	62	0.873	9	0.127	0	4	11
4 - Segment 4	30	1	22	0.786	6	0.214	0	1	1
5 - Segment 5	98	1	55	0.809	13	0.191	0	7	23
6 - Segment 6	52	1	39	0.867	6	0.133	0	3	4
7 - Segment 7	0	0	0	0	0	0	0	0	0
8 - Segment 8	4	0.3	3	0.3	0	0	0	0	1
9 -									

Segment 9	3	0.2	2	0.2	0	0	0	0	1
10 - Segment 10	8	0.7	7	0.7	0	0	0	0	1
Totals	**396**	**6.8**	**261**	**6.002**	**44**	**0.798**	**0**	**27**	**64**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Abstain	
1	Arizona Public Service Co.	Robert Smith	Negative	COMMENT RECEIVED
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton		
1	Austin Energy	James Armke	Affirmative	
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Negative	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Richard Castrejana		
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Negative	SUPPORTS THIRD PARTY COMMENTS
1	El Paso Electric Company	Pablo Onate	Abstain	
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Richard Bachmeier	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Affirmative	
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon		
1	Kansas City Power & Light Co.	Jennifer Flandermeyer	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lincoln Electric System	Doug Bantam		
1	Long Island Power Authority	Robert Ganley		
1	Los Angeles Department of Water & Power	John Burnett	Abstain	

1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	Nebraska Public Power District	Cole C Brodine		
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Bruce Metruck	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke		
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey		
1	Oklahoma Gas and Electric Co.	Terri Pyle	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Jen Fiegel	Abstain	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Abstain	
1	Otter Tail Power Company	Daryl Hanson		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams		
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen		
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	SaskPower	Wayne Guttormson		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo		
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Abstain	
1	Southern California Edison Company	Steven Mavis	Abstain	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Affirmative	
1	Texas Municipal Power Agency	Brent J Hebert		
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Abstain	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Abstain	

2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blue Ridge Electric	James L Layton		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila	Negative	SUPPORTS THIRD PARTY COMMENTS
3	City of Farmington	Linda R Jacobson		
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	John Bee	Negative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	Entergy	Joel T Plessinger	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	Supports FirstEnergy's comments
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel		
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Lakeland Electric	Mace D Hunter	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	David R Rivera	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	

3	Oklahoma Gas and Electric Co.	Donald Hargrove	Abstain	
3	Old Dominion Electric Coop.	Bill Watson		
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz		
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Negative	COMMENT RECEIVED
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-County Electric Cooperative, Inc.	Mike Swearingen		
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	COMMENT RECEIVED
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	SUPPORTS THIRD PARTY COMMENTS
3	Wisconsin Public Service Corp.	Gregory J Le Grave		
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	SUPPORTS THIRD PARTY COMMENTS
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	SUPPORTS THIRD PARTY COMMENTS
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell	Negative	
4	Consumers Energy Company	Tracy Goble		
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Negative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney	Affirmative	

4	Tacoma Public Utilities	Keith Morisette	Negative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	SUPPORTS THIRD PARTY COMMENTS
5	AEP Service Corp.	Brock Ondayko		
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Associated Electric Cooperative, Inc.	Matthew Pacobit	Affirmative	
5	Avista Corp.	Steve Wenke	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Calpine Corporation	Hamid Zakery	Affirmative	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy Power Management, LLC	Mike D Hirst		
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Alexander Eizans	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	El Paso Electric Company	Gustavo Estrada	Abstain	
5	Electric Power Supply Association	John R Cashin		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Essential Power, LLC	Patrick Brown		
5	Exelon Nuclear	Mark F Draper	Negative	
5	First Wind	John Robertson		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Hydro-Québec Production	Roger Dufresne	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Lafayette Utilities System	Jamie B Webb	Abstain	
5	Lakeland Electric	James M Howard	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Karin Schweitzer	Affirmative	
5	Luminant Generation Company LLC	Rick Terrill	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	COMMENT RECEIVED

5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	NiSource	Huston Ferguson		
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Abstain	
5	PacifiCorp	Bonnie Marino-Blair		
5	Pattern Gulf Wind LLC	Grit Schmieder-Copeland		
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway		
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Public Utility District No. 1 of Chelan County	John Yale		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Raven Power	Scott A Etnoyer		
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tacoma Power	Chris Mattson	Negative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State G & T Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	USDI Bureau of Reclamation	Erika Doot	Negative	
5	Utility System Effeciencies, Inc. (USE)	Robert L Dintelman		
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Western Farmers Electric Coop.	Clem Cassmeyer		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Negative	COMMENT RECEIVED
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Negative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Negative	SUPPORTS THIRD PARTY COMMENTS
6	FirstEnergy Solutions	Kevin Querry	Affirmative	

6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley	Affirmative	
6	New York Power Authority	Saul Rojas	Affirmative	
6	Northern California Power Agency	Steve C Hill	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson		
6	Oklahoma Gas & Electric Services	Jerry Nottnagel	Abstain	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Kelly Cumiskey	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	SUPPORTS THIRD PARTY COMMENTS
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet		
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	Southern California Edison Company	Lujuanna Medina	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney		
6	Wisconsin Public Service Corp.	David Hathaway		
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Edward C Stein		
8		Roger C Zaklukiewicz	Affirmative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2014 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Exhibit G

Standard Drafting Team Roster

Drafting Team Members and Observers for VAR

Name and Title	Company	Contact Info	Bio
Bill Harm, Chair	PJM Interconnection	(610) 666-8868 harm@pjm.com	Bill Harm is a Senior Consultant at PJM in the NERC and regional coordination department. Bill has over 39 years of experience in various aspects of the planning and operation of the PJM network. Before joining the NERC and regional coordination department Bill worked in operations, operations planning, system planning and operations support. Bill's background also includes technical support of operations and markets during the integration of new members into the PJM market as well as developing various joint operating agreements. Bill Harm has also participated in the follow NERC activities: • NERC Systems Analysis and Modeling Subcommittee • NERC Modifications to FAC-012 and FAC-013 for Order 729 • NERC ATC SAR Drafting team • ERAG Management Committee • MEN/VEM study Committees • Joint Inter regional Review Committee • NERC 2003 Blackout Investigation Team
Martin Kaufman, Vice Chair	ExxonMobil Research and Engineering	(281) 834-7549 martin.kaufman@exxonmobil.com	Martin Kaufman is experienced in industrial electric system design, operation, and configuration; including cogeneration facility operation and design, and an in-depth understanding of the supply needs of large end-users and how the operation and planning of the bulk power system impacts these needs. Martin Kaufman currently performs a global power system design and operation subject matter expert role for ExxonMobil, and provides compliance assurance support for NERC activities.

Name and Title	Company	Contact Info	Bio
Scott Berry	Indiana Municipal Power Agency	317-428-6710 sberry@impa.com	Scott Berry has 21 years of Generator experience which include, 6 years in the Navy Nuclear Power Program as a Reactor Operator and 15 years with Gas Combustion turbines as an Operator. Scott has also served as a Technician and Plant Superintendent, and he has been working with NERC and regional standards for approximately 6 years. Scott is currently active in the following areas: Transmission Access Study Group (TAPS); Small Entity Working Group (RFC and SERC Entities); North American Generator Forum; and Combustion Turbine Operation Task Force (CTOTF).
Brian Buckley	TECO Energy	bsbuckley@tecoenergy.com	Brian Buckley is the Manager of Compliance and Performance responsible for leading all Energy Supply regulatory activities including our Compliance Program for FERC, NERC and FRCC standards. Brian received a Bachelor of Science degree in Mechanical Engineering in 1997 from the Georgia Institute of Technology and a Master of Business Administration from the University of South Florida in 2003. Brian's past positions at Tampa Electric include: Operations Engineer at Gannon/Bayside Station (a natural gas combined cycle plant), Instrumentation and Controls Engineer at Big Bend Station (a coal-fired plant), and Senior Engineer in Operations Planning (maintaining reliability of all company plants).

Name and Title	Company	Contact Info	Bio
Steve Hitchens	Bonneville Power Administration	509-465-0339 sbhitchens@bpa.gov	Steve Hitchens is an Electrical Engineer with Bonneville Power Administration since 1991. Steve served for six years with substation Design, outdoor design for high voltage substations. From 1997 to present , Steve has worked as the Technical Operations Engineer responsible for: • Seasonal and outage planning studies for determining SOL's on the major BPA interchanges and flowgates; • BPA Dispatch support for main grid and sub grid operation; • NERC VAR-001 SME for Requirements R2, R3, R4, R6 and R11; and • Reactive and Voltage SME (since 2004) responsible for, in part, the BPA Voltage Schedule updates, modifications and circulation
Sharma Kolluri	SERC	(504) 576-4045 vkollur@entergy.com	Sharma Kolluri has over 30 years of experience in the Planning and Operation areas. He is currently the Manager of Transmission Planning at Entergy where is responsible for stability studies, reactive power planning studies, reactive power management and generator interconnection studies. Sharma is responsible for reactive power planning and management studies at Entergy. He has also published several papers at IEEE in the area of reactive power planning and voltage stability, especially dealing with static and dynamic reactive power compensation. He served as a past chairman of the Dynamics Review Sub Committee (DRS) at SERC, and he is a member of the IEEE Dynamic Performance Committee, Stability Controls sub-committee and Voltage stability task force.

Name and Title	Company	Contact Info	Bio
Joshua Pierce	Southern Company Services-Transmission Planning	205-257-6196 jspierce@southernco.com	Joshua Pierce has worked for Southern Company for more than ten years with extensive experience within the transmission organization of a vertically integrated utility. He began his career with Southern Company in 2002 as a student engineer in Transmission Line Design and Maintenance Support for Alabama Power Company (APC). He began full time employment in 2004 in APC Substation Protective Equipment and Controls Design and joined APC Substation Protection and Control Field Services in 2008. In 2011, he joined Transmission Planning for Southern Company Services where he presently works performing tariff generator interconnection and transmission service studies as well as regional planning.

Name and Title	Company	Contact Info	Bio
Joe Seabrook	Puget Sound Energy	(425) 462-3577 Joe.Seabrook@pse.com	Joe Seabrook has worked in transmission expansion planning and operating at Puget Sound Energy since 1980. Puget's transmission and transmission rights extend from Washington State to Canada, through Montana, and south to the Oregon-California border. Joe is currently chairing a WECC working group to add SPS, relays, contingency descriptions, sequence components and breaker-node topology to WECC planning and operating base cases. Joe also helped develop the reactive margin requirements and voltage stability assessment methodology used by WECC, and he co-authored WECC reports, studies, guidelines, methodology, and criteria on voltage stability, reactive margin, and under voltage load tripping beginning in 1994. Joe has served on the WECC Technical Studies Subcommittee since 1993, serving as the chair, vice-chair, and secretary, and leading and serving many work groups and task forces on reliability criteria, transmission path rating, off-nominal frequency, under voltage generator and load issues, and synchronous and wind generator dynamic modeling. Joe also helped develop the reactive margin requirements and voltage stability assessment methodology used by WECC. This began with the original report in 1997 that was used to develop the WECC reactive margin criteria requirements in 2002, and the WECC Safety Net policy.

Name and Title	Company	Contact Info	Bio
Hari Singh	Xcel Energy	(303) 571-7095 hari.singh@xcelenergy.com	Hari Singh has been a member of the NERC Transmission Issues Subcommittee (TIS) since 2009. Hari is also a member of the WECC Modeling & Validation Working Group (MVWG) and well versed with the composite load model being developed and tested by WECC MVWG for promoting improved dynamic load modeling to study FIDVR events and/or evaluate voltage stability in load centers to identify the need for implementing UVLS. Currently, Hari serves as the Transmission Planning Engineer responsible for conducting the periodic studies required by PRC-010 to assess the need for UVLS or the effectiveness of existing UVLS. Hari is also a member of the NERC System Analysis & Modeling Subcommittee and the WECC Reliability Subcommittee. He has also served as the WECC Modeling & Validation WG Technical Consultant to Rocky Mountain Voltage Coordination Guidelines Working Group.
Mike Swearingen	Tri-country Electric Cooperative, Inc.	580-652-3804 mikeswearingen@tri-countyelectric.coop	Mike Swearingen has over 19 years of experience as a power system engineer for transmission and distribution systems. Mike designed and oversaw the design and construction of substations and mobile substations. He also has field experience in power system operation and control systems. Mike has also participated in the IEEE Power Quality Subcommittee and associated working groups by helping in the development of standards. Further, Mike developed the NERC program and Internal Compliance Program for Tri-County Electric Cooperative

Name and Title	Company	Contact Info	Bio
Hamid Zakery	Calpine Corporation	(832) 325-5007 hamid.zakery@calpine.com	For the past 28 years, Hamid Zakery have served the utility industry in various technical and operation responsibilities. Hamid started his career with Illinois Power Company as a relay engineer where he designed protection schemes for Transmission, Distribution and Generation assets. Later he became responsible for operation and maintenance activities for utility substations ranging from 480 volts to 345 Kv systems. As a plant engineering manager, Hamid held responsibilities for fossil plants engineering functions including performance and predictive maintenance. Over the past 10 years, he has been involved with development and implementation of engineering, operation and maintenance programs to prepare IPP generation assets in all 8 NERC Regions for compliance with NERC standards and regional guidelines.

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

SUNSHINE ACT MEETING NOTICE

June 12, 2014

The following notice of meeting is published pursuant to section 3(a) of the government in the Sunshine Act (Pub. L. No. 94-409), 5 U.S.C. 552b:

AGENCY HOLDING MEETING:	FEDERAL ENERGY REGULATORY COMMISSION
DATE AND TIME:	June 19, 2014 10:00 A.M.
PLACE:	Room 2C 888 First Street, N.E. Washington, D.C. 20426
STATUS:	OPEN
MATTERS TO BE CONSIDERED:	Agenda * NOTE - Items listed on the agenda may be deleted without further notice.
CONTACT PERSON FOR MORE INFORMATION:	Kimberly D. Bose Secretary Telephone (202) 502-8400 For a recorded message listing items struck from or added to the meeting, call (202) 502-8627.

This is a list of matters to be considered by the Commission. It does not include a listing of all documents relevant to the items on the agenda. All public documents, however, may be viewed on line at the Commission's website at http://www.ferc.gov using the eLibrary link, or may be examined in the Commission's Public Reference Room.

1006TH - MEETING

REGULAR MEETING

June 19, 2014

10:00 AM

Item No	Docket No.	Company
		ADMINISTRATIVE
A-1	AD02-1-000	Agency Business Matters
A-2	AD02-7-000	Customer Matters, Reliability, Security and Market Operations
A-3	AD14-14-000	Price Formation in Energy and Ancillary Services Markets Operated by Regional Transmission Organizations and Independent System Operators
		ELECTRIC
E-1	OMITTED	
E-2	OMITTED	
E-3	ER13-83-003 ER13-83-004 ER13-83-005 ER13-897-001 ER13-897-002 ER13-908-001 ER13-908-002 ER13-913-001 ER13-913-002	Duke Energy Carolinas, LLC and Duke Energy Progress, Inc. Louisville Gas and Electric Company and Kentucky Utilities Company Alabama Power Company Ohio Valley Electric Corporation
E-4	ER14-1386-000	California Independent System Operator Corporation
E-5	ER14-1578-000	PacifiCorp
E-6	RM14-14-000	Refinements to Policies and Procedures for Market-Based Rates for Wholesale Sales of Electric Energy, Capacity and Ancillary Services by Public Utilities
E-7	EL11-66-001	Martha Coakley, Massachusetts Attorney General; Conneticut Public Utilities Regulatory Authority; Massachusetts Department of Public Utilities; New Hampshire Public Utilities Commission; Connecticut Office of Consumer Counsel; Maine Office of the Public Advocate; George Jepsen, Connecticut Attorney General; New Hampshire Office of Consumer Advocate; Rhode Island Division of Public Utilities and Carriers; Vermont Department

		of Public Service; Massachusetts Municipal Wholesale Electric Company; Associated Industries of Massachusetts; The Energy Consortium; Power Options, Inc.; and the Industrial Energy Consumer Group v. Bangor Hydro-Electric Company; Central Maine Power Company; New England Power Company d/b/a National Grid; New Hampshire Transmission LLC d/b/a NextEra; NSTAR Electric and Gas Corporation; Northeast Utilities Service Company; The United Illuminating Company; Unitil Energy Systems, Inc. and Fitchburg Gas and Electric Light Company; Vermont Transco, LLC
E-8	EL13-33-000	ENE (Environment Northeast), The Greater Boston Real Estate Board, National Consumer Law Center, and NEPOOL Industrial Customer Coalition v. Bangor Hydro-Electric Company, Central Maine Power Company, New England Power Company, New Hampshire Transmission LLC, NSTAR Electric Company, Northeast Utilities Service Company, The United Illuminating Company, Unitil Energy Systems, Inc., Fitchburg Gas and Electric Light Company, and Vermont Transco, LLC.
E-9	EL12-39-000	Seminole Electric Cooperative, Inc. and Florida Municipal Power Agency v. Florida Power Corporation
E-10	EL13-63-000	Seminole Electric Cooperative, Inc. and Florida Municipal Power Agency v. Duke Energy Florida, Inc.
	EL12-39-000	Seminole Electric Cooperative, Inc. and Florida Municipal Power Agency v. Florida Power Corporation
E-11	EL12-59-000	Golden Spread Electric Cooperative, Inc. v. Southwestern Public Service Company
E-12	EL13-78-000 EL12-59-000	Golden Spread Electric Cooperative, Inc. v. Southwestern Public Service Company
E-13	OMITTED	
E-14	OMITTED	
E-15	OMITTED	
E-16	EL13-86-000	Grand Valley Rural Power Lines, Holy Cross Electric Association, Inc., Intermountain Rural Electric Association, Inc. and Yampa Valley Electric Association, Inc. v. Public Service Company of Colorado
E-17	RM14-7-000	Modeling, Data, and Analysis Reliability Standards

E-18	RM14-1-000	Reliability Standard for Geomagnetic Disturbance Operations
E-19	RD14-7-000	North American Electric Reliability Corporation
E-20	ER14-1626-000 ER14-1627-000 ER14-1625-000	Constellation NewEnergy, Inc. Constellation Energy Commodities Group Maine, LLC Exelon Generation Company, LLC
E-21	ER13-1748-000 ER13-1748-001	Southwest Power Pool, Inc.
E-22	ER12-1179-018 ER13-1173-000	Southwest Power Pool, Inc.
E-23	ER13-2452-001	California Independent System Operator Corporation
E-24	ER08-375-006	Southern California Edison Company
E-25	AC11-46-000	Ameren Corporation
E-26	AC11-46-002 AC11-46-003	Ameren Corporation
	MISCELLANEOUS	
M-1	RM13-17-001	Communication of Operational Information Between Natural Gas Pipelines and Transmission Operators
	GAS	
G-1	RP14-380-000	National Fuel Gas Supply Corporation and Empire Pipeline, Inc.
G-2	RP14-453-000	Enable Gas Transmission, LLC and Enable Mississippi River Transmission, LLC
	HYDRO	
H-1	P-12690-008 P-12690-007 EL14-47-000	Public Utility District No. 1 of Snohomish County, Washington
H-2	P-2082-058	PacifiCorp
H-3	P-14589-000	Green Energy Storage Corp
H-4	P-12756-004	BOST3 Hydroelectric LLC
H-5	P-12714-004	H20 Holdings, LLC
H-6	P-13579-003 P-14491-001	FFP Qualified Hydro 14, LLC Western Minnesota Municipal Power Agency
H-7	P-13123-002	Eagle Crest Energy Company

CERTIFICATES

C-1	CP13-25-000 CP13-27-000	Cameron LNG, LLC Cameron Interstate Pipeline, LLC
C-2	CP13-545-001	Dominion Transmission, Inc. and Tennessee Gas Pipeline Company, L.L.C.
C-3	CP13-516-000	EcoEléctrica, L.P.

Kimberly D. Bose,
Secretary.

A free webcast of this event is available through www.ferc.gov. Anyone with Internet access who desires to view this event can do so by navigating to www.ferc.gov's Calendar of Events and locating this event in the Calendar. The event will contain a link to its webcast. The Capitol Connection provides technical support for the free webcasts. It also offers access to this event via television in the DC area and via phone bridge for a fee. If you have any questions, visit www.CapitolConnection.org or contact Danelle Springer or David Reininger at 703-993-3100.

Immediately following the conclusion of the Commission Meeting, a press briefing will be held in the Commission Meeting Room. Members of the public may view this briefing in the designated overflow room. This statement is intended to notify the public that the press briefings that follow Commission meetings may now be viewed remotely at Commission headquarters, but will not be telecast through the Capitol Connection service.

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

SUNSHINE ACT MEETING NOTICE

June 12, 2014

The following notice of meeting is published pursuant to section 3(a) of the government in the Sunshine Act (Pub. L. No. 94-409), 5 U.S.C. 552b:

AGENCY HOLDING MEETING:	FEDERAL ENERGY REGULATORY COMMISSION
DATE AND TIME:	June 19, 2014 10:00 A.M.
PLACE:	Room 2C 888 First Street, N.E. Washington, D.C. 20426
STATUS:	OPEN
MATTERS TO BE CONSIDERED:	Agenda * NOTE - Items listed on the agenda may be deleted without further notice.
CONTACT PERSON FOR MORE INFORMATION:	Kimberly D. Bose Secretary Telephone (202) 502-8400 For a recorded message listing items struck from or added to the meeting, call (202) 502-8627.

This is a list of matters to be considered by the Commission. It does not include a listing of all documents relevant to the items on the agenda. All public documents, however, may be viewed on line at the Commission's website at http://www.ferc.gov using the eLibrary link, or may be examined in the Commission's Public Reference Room.

1006TH - MEETING

REGULAR MEETING

June 19, 2014

10:00 AM

Item No	Docket No.	Company
		ADMINISTRATIVE
A-1	AD02-1-000	Agency Business Matters
A-2	AD02-7-000	Customer Matters, Reliability, Security and Market Operations
A-3	AD14-14-000	Price Formation in Energy and Ancillary Services Markets Operated by Regional Transmission Organizations and Independent System Operators
		ELECTRIC
E-1	OMITTED	
E-2	OMITTED	
E-3	ER13-83-003 ER13-83-004 ER13-83-005 ER13-897-001 ER13-897-002 ER13-908-001 ER13-908-002 ER13-913-001 ER13-913-002	Duke Energy Carolinas, LLC and Duke Energy Progress, Inc. Louisville Gas and Electric Company and Kentucky Utilities Company Alabama Power Company Ohio Valley Electric Corporation
E-4	ER14-1386-000	California Independent System Operator Corporation
E-5	ER14-1578-000	PacifiCorp
E-6	RM14-14-000	Refinements to Policies and Procedures for Market-Based Rates for Wholesale Sales of Electric Energy, Capacity and Ancillary Services by Public Utilities
E-7	EL11-66-001	Martha Coakley, Massachusetts Attorney General; Conneticut Public Utilities Regulatory Authority; Massachusetts Department of Public Utilities; New Hampshire Public Utilities Commission; Connecticut Office of Consumer Counsel; Maine Office of the Public Advocate; George Jepsen, Connecticut Attorney General; New Hampshire Office of Consumer Advocate; Rhode Island Division of Public Utilities and Carriers; Vermont Department

		of Public Service; Massachusetts Municipal Wholesale Electric Company; Associated Industries of Massachusetts; The Energy Consortium; Power Options, Inc.; and the Industrial Energy Consumer Group v. Bangor Hydro-Electric Company; Central Maine Power Company; New England Power Company d/b/a National Grid; New Hampshire Transmission LLC d/b/a NextEra; NSTAR Electric and Gas Corporation; Northeast Utilities Service Company; The United Illuminating Company; Unitil Energy Systems, Inc. and Fitchburg Gas and Electric Light Company; Vermont Transco, LLC
E-8	EL13-33-000	ENE (Environment Northeast), The Greater Boston Real Estate Board, National Consumer Law Center, and NEPOOL Industrial Customer Coalition v. Bangor Hydro-Electric Company, Central Maine Power Company, New England Power Company, New Hampshire Transmission LLC, NSTAR Electric Company, Northeast Utilities Service Company, The United Illuminating Company, Unitil Energy Systems, Inc., Fitchburg Gas and Electric Light Company, and Vermont Transco, LLC.
E-9	EL12-39-000	Seminole Electric Cooperative, Inc. and Florida Municipal Power Agency v. Florida Power Corporation
E-10	EL13-63-000	Seminole Electric Cooperative, Inc. and Florida Municipal Power Agency v. Duke Energy Florida, Inc.
	EL12-39-000	Seminole Electric Cooperative, Inc. and Florida Municipal Power Agency v. Florida Power Corporation
E-11	EL12-59-000	Golden Spread Electric Cooperative, Inc. v. Southwestern Public Service Company
E-12	EL13-78-000 EL12-59-000	Golden Spread Electric Cooperative, Inc. v. Southwestern Public Service Company
E-13	OMITTED	
E-14	OMITTED	
E-15	OMITTED	
E-16	EL13-86-000	Grand Valley Rural Power Lines, Holy Cross Electric Association, Inc., Intermountain Rural Electric Association, Inc. and Yampa Valley Electric Association, Inc. v. Public Service Company of Colorado
E-17	RM14-7-000	Modeling, Data, and Analysis Reliability Standards

E-18	RM14-1-000	Reliability Standard for Geomagnetic Disturbance Operations
E-19	RD14-7-000	North American Electric Reliability Corporation
E-20	ER14-1626-000 ER14-1627-000 ER14-1625-000	Constellation NewEnergy, Inc. Constellation Energy Commodities Group Maine, LLC Exelon Generation Company, LLC
E-21	ER13-1748-000 ER13-1748-001	Southwest Power Pool, Inc.
E-22	ER12-1179-018 ER13-1173-000	Southwest Power Pool, Inc.
E-23	ER13-2452-001	California Independent System Operator Corporation
E-24	ER08-375-006	Southern California Edison Company
E-25	AC11-46-000	Ameren Corporation
E-26	AC11-46-002 AC11-46-003	Ameren Corporation
	MISCELLANEOUS	
M-1	RM13-17-001	Communication of Operational Information Between Natural Gas Pipelines and Transmission Operators
	GAS	
G-1	RP14-380-000	National Fuel Gas Supply Corporation and Empire Pipeline, Inc.
G-2	RP14-453-000	Enable Gas Transmission, LLC and Enable Mississippi River Transmission, LLC
	HYDRO	
H-1	P-12690-008 P-12690-007 EL14-47-000	Public Utility District No. 1 of Snohomish County, Washington
H-2	P-2082-058	PacifiCorp
H-3	P-14589-000	Green Energy Storage Corp
H-4	P-12756-004	BOST3 Hydroelectric LLC
H-5	P-12714-004	H20 Holdings, LLC
H-6	P-13579-003 P-14491-001	FFP Qualified Hydro 14, LLC Western Minnesota Municipal Power Agency
H-7	P-13123-002	Eagle Crest Energy Company

CERTIFICATES

C-1	CP13-25-000 CP13-27-000	Cameron LNG, LLC Cameron Interstate Pipeline, LLC
C-2	CP13-545-001	Dominion Transmission, Inc. and Tennessee Gas Pipeline Company, L.L.C.
C-3	CP13-516-000	EcoEléctrica, L.P.

Kimberly D. Bose,
Secretary.

A free webcast of this event is available through www.ferc.gov. Anyone with Internet access who desires to view this event can do so by navigating to www.ferc.gov's Calendar of Events and locating this event in the Calendar. The event will contain a link to its webcast. The Capitol Connection provides technical support for the free webcasts. It also offers access to this event via television in the DC area and via phone bridge for a fee. If you have any questions, visit www.CapitolConnection.org or contact Danelle Springer or David Reininger at 703-993-3100.

Immediately following the conclusion of the Commission Meeting, a press briefing will be held in the Commission Meeting Room. Members of the public may view this briefing in the designated overflow room. This statement is intended to notify the public that the press briefings that follow Commission meetings may now be viewed remotely at Commission headquarters, but will not be telecast through the Capitol Connection service.

RSC Meeting #14-2, Agenda Item 11.0: Standards Activity Post NERC BOT Approval

Latest Changes (Since Last RSC Meeting):

Project	11.1: NERC Filings to FERC	11.2: FERC Orders / Rules	11.3: Federal Register	Stage
Project: 2007-09 — Generator Verification		**Docket #:** RM13-16-000 / **Date:** 3/20/2014 **Title:** Order No. 796 Approving Generator Verification Reliability Standards **Summary:** FERC issues a final rule approving five Generator Verification Reliability Standards MOD-025-2 (Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability), MOD-026-1 (Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions), MOD-027-1 (Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions), PRC-019-1 (Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection), and PRC-024-1 (Generator Frequency and Voltage Protective Relay Settings).	**Vol. 79, No. 59 – Date: Thursday, March 27, 2014** **RULES** Generator Verification Reliability Standards **Key Dates:** Rule effective May 27, 2014	Subject to Future Enforcement

RSC Meeting #14-2, Agenda Item 11.0: Standards Activity Post NERC BOT Approval

Project	11.1: NERC Filings to FERC	11.2: FERC Orders / Rules	11.3: Federal Register	Stage
Project: 2008-06, Cyber Security Order 706 Version 5 CIP Standards	**Docket #:** RM13-5-000/ **Date:** 3/18/2014 **Title:** **Request of NERC for Extension of Time to File Revisions to the Violation Risk Factors Assigned to Reliability Standards CIP-006-5, Requirement R3 and CIP-004-5, Requirement R4** **Summary:** NERC submits a request for a 10-day extension of time to file revisions to the Violation Risk Factors ("VRFs") assigned to Reliability Standards CIP-006-5, Requirement R3 and CIP-004-5, Requirement R4.	**Docket #:** RM13-5-000 / **Date:** 2/28/2014 **Title:** **Notice of Reliability Technical Conference on Version 5 Critical Infrastructure Protection Reliability Standards** **Summary:** FERC issues a notice of a technical conference focused on Critical Infrastructure Protection Issues Identified in Order No. 791. This staff-led conference will take place on April 29, 2014 beginning at 9:00 AM and ending at approximately 5:00 PM EST at FERC. **Docket #:** RM13-5-000 / **Date:** 3/19/2014 **Title:** **Notice of Extension of Time** **Summary:** FERC issues a notice granting a 10-day extension of time, until May 15, 2014, to file revisions to the Violation Risk Factors (VRF) assigned to Reliability Standards CIP-006-5, Requirement R3 and CIP-004-5, Requirement R4 (motion). **Docket #:** RM13-5-001 / **Date:** 3/20/2014 **Title:** **Order on Clarification and Rehearing** **Summary:** FERC issues an order granting clarification in part and denying rehearing of Order No. 791, filed jointly by Edison Electric Institute (EEI) and Electric Power Supply Association (EPSA) as well as the American Public Power Association (APPA), National Rural Electric Cooperative Association (NRECA), and Utility Services, Inc. (Utility Services).		Subject to Future Enforcement

RSC Meeting #14-2, Agenda Item 11.0: Standards Activity Post NERC BOT Approval

Project	11.1: NERC Filings to FERC	11.2: FERC Orders / Rules	11.3: Federal Register	Stage
Project: 2008-12, Coordinate Interchange Standards	**Docket #:** RD14-4-000 / **Date:** 2/27/2014 **Title:** **Petition of NERC for Approval of Proposed Reliability Standards for Interchange Scheduling and Coordination** **Summary:** NERC submits a petition for approval of five proposed Reliability Standards INT-004-3 (Dynamic Transfers), INT-006-4 (Evaluation of Interchange Transactions), INT-009-2 (Implementation of Interchange), INT-010-2 (Interchange Initiation and Modification for Reliability), and INT-011-1 (Intra-Balancing Authority Transaction Identification).			Filed and Pending Regulatory Approval
Project: 2010-01, Support Personnel Training	**Docket #:** RM14-9-000 / **Date:** 3/7/2014 **Title:** **Petition of NERC for Approval of Proposed Reliability Standard PER-005-2 and Retirement of Reliability Standard PER-005-1** **Summary:** NERC submits a petition for approval of proposed Reliability Standard PER-005-2-Operations Personnel Training and the retirement of the currently effective Reliability Standard PER-005-1.			Filed and Pending Regulatory Approval
Project: 2010-03, Modeling Data (MOD B)	**Docket #:** RD14-5-000 / **Date:** 2/25/2014 **Title:** **Petition of NERC for Approval of Proposed Reliability Standards MOD-032-1 and MOD-033-1** **Summary:** NERC submits a petition for approval of proposed Reliability Standards MOD-032-1 (Data for Power System Modeling and Analysis) and MOD-033-1 (Steady-State and Dynamic System Model Validation).			Filed and Pending Regulatory Approval
Project: 2010-13.2 Relay Loadability		**Docket #:** RM13-19-000 and RM14-3-000 / **Date:** 3/20/2014 **Title:** **Notice of Proposed Rulemaking to Approve Reliability Standards PRC-025-1 and PRC-023-3** **Summary:** FERC issues a Notice of Proposed of Proposed Rulemaking (NOPR) proposing to approve Reliability Standards PRC-025-1 (Generator Relay Loadability) and PRC-023-3 (Transmission Relay Loadability).	**Vol. 79, No. 59 – Date: Thursday, March 27, 2014** **PROPOSED RULES** **Generator Relay Loadability and Revised Transmission Relay Loadability Reliability Standards** **Key Dates:** Comments due April 28, 2014	Filed and Pending Regulatory Approval

RSC Meeting #14-2, Agenda Item 11.0: Standards Activity Post NERC BOT Approval

Project	11.1: NERC Filings to FERC	11.2: FERC Orders / Rules	11.3: Federal Register	Stage
Project: 2010-14.1 Phase 1 of Balancing Authority Reliability-based Controls: Reserves	**Docket #:** _____ / **Date:** 4/2/2014 **Title:** **Petition of NERC for Approval of Reliability Standard BAL-001-2-Real Power Balancing Control Performance** **Summary:** NERC submits a petition for approval of proposed Reliability Standard BAL-001-2-Real Power Balancing Control Performance.			
Project: 2010-17, BES Definition and BES Exception Procedure	**Docket #:** RD14-2-000 / **Date:** 4/1/2014 **Title:** **Revised Bulk Electric Definition in the NERC Rules of Procedure** **Summary:** NERC submits this filing to update the revised Phase 2 definition of Bulk Electric System, approved in FERC's March 20, 2014 order, in the NERC Rules of Procedure, Appendix 2 Definitions Used in the Rules of Procedure and Appendix 5B Statement of Compliance Registry Criteria.	**Docket** #: RD14-2-000 / **Date:** 3/20/2014 **Title:** **Order Approving Revised Definition** **Summary:** FERC issued an order approving revisions to the definition of "bulk electric system" in the NERC Glossary of Terms Used in Reliability Standards (NERC Glossary).		Subject to Future Enforcement
Project: 2013-03, Geomagnetic Disturbance Mitigation	**Docket #:** RM14-1-000 / **Date:** 3/24/2014 **Title:** **Comments of NERC in Response to Notice of Proposed Rulemaking EOP-010-1 (Geomagnetic Disturbance Operations)** **Summary:** NERC submits comments in response to the Notice of Proposed Rulemaking (NOPR) proposing to approve Reliability Standard EOP-010-1 (Geomagnetic Disturbance Operations).			Filed and Pending Regulatory Approval

RSC Meeting #14-2, Agenda Item 11.0: Standards Activity Post NERC BOT Approval

Project	11.1: NERC Filings to FERC	11.2: FERC Orders / Rules	11.3: Federal Register	Stage
Project: 2014-04, Physical Security	**Docket #:** RD14-6-000/ **Date:** 3/10/2014 **Title:** Doc-Less Motion to Intervene in Docket No. RD14-6-000 **Summary:** NERC submits a doc-less motion to intervene in the proceeding regarding direction to develop reliability standards requiring owners and operations of the Bulk-Power System to address risks due to physical security threats and vulnerabilities.	**Docket #:** RD14-6-000 / **Date:** 3/7/2014 **Title:** Notice of Designation of Commission Staff **Summary:** FERC issues a letter order identifying the staff from the Office of Electric Reliability designated as non-decisional, who are prohibited from communicating with advisory staff concerning any deliberations for Physical Security Measures Reliability Standards. **Docket #:** RD14-6-000 / **Date:** 3/7/2014 **Title:** Order Directing Filing of Standards **Summary:** FERC issues an order requiring NERC to develop reliability standards requiring owners and operators of the Bulk-Power System to address risks due to physical security threats and vulnerabilities.	**Vol. 79, No. 50 – Date: Friday, March 14, 2014** **NOTICES** **Reliability Standards for Physical Security Measures: Designation of Commission Staff as Non-Decisional** **Key Dates:** N/A	Under Development

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Standards Committee Meeting

June 10, 2014 | 1:00 – 5:00 p.m. Mountain
June 11, 2014 | 8:00 – Noon Mountain

Xcel Energy
1800 Larimer Street
Denver, CO 80212

Dial-in: 1-866-740-1260 | Access Code: 8314765 | Security Code: 061014

Click here for ReadyTalk web access: June 10, 2014
Click here for ReadyTalk web access: June 11, 2014

NERC Antitrust Compliance Guidelines and Public Announcement*

Introductions and Chair's Remarks

Agenda Items for June 10, 2014

1. **Review of Agenda — (Approve)** (5 minutes)
2. **Consent Agenda — (Approve)** (5 minutes)
   a. May 14, 2014 Meeting Minutes*- **(Approve)**
   b. May 16, 2014 Meeting Minutes*- **(Approve)**
3. **Three-Month Outlook on Upcoming Standard Projects or Issues*— (Update)** (V. Agnew, S. Miller) (10 minutes)
4. **Projects Under Development — (Review)**
   a. Project Tracking Spreadsheet (R. Parsons, V. Agnew, L. Hussey, S. Noess) (15 minutes)
   b. Projected Posting Schedule (B. Nutter) (5 minutes)
5. **Project 2008-02 Undervoltage Load Shedding*— (Authorize)** (V. Agnew) (15 minutes)
6. **Project 2010-05.2 Special Protection Systems*— (Authorize)** (V. Agnew) (15 minutes)
7. **Project 2010-14.2 Periodic Review of BAL Standards*— (Accept, Appoint)** (L. Hussey) (15 minutes)
8. **Project 2014-01 Dispersed Generation Resources*— (Authorize)** (L. Hussey) (15 minutes)
9. **Subcommittee Reports**
   a. **PMOS Update*** - **(Update)** (J. Sterling) (10 Minutes)

b. **Process Subcommittee*— (Update)** (L. Lee) (15 minutes)
   i. **Ballot Pool Management*** - **(Informational)** (L. Lee) (15 minutes)
   ii. **Consensus Building and SAR Development*** - **(Endorse)** (B. Li) (15 minutes)
   iii. **Review of Standards Processes and Procedures*** - **(Endorse)** (L. Lee) (15 minutes)

10. **Communication Updates and Activities* — (Update)** (S. Miller, M. Huggins) (10 minutes)
11. **Upcoming Standards Filings* — (Review)** (S. Tyrewala) (10 minutes)

Agenda Items for June 11, 2014

12. **Project 2013-03 Geomagnetic Disturbance Mitigation* — (Authorize)** (L. Hussey) (15 minutes)
13. **Informational Items — (Enclosed)**
    a. SC Expectations*
    b. 2014 Meeting Dates and Locations*
    c. 2014 Standards Committee Roster*
    d. Highlights of Parliamentary Procedure*
14. **Adjourn**

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Public Announcements

REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

Conference call version:
Participants are reminded that this conference call is public. The access number was posted on the NERC website and widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Minutes
Standards Committee Meeting

May 14, 2014 | 1:00 - 4:00 p.m. Eastern

NERC Antitrust Compliance Guidelines and Public Announcement

Introductions and Chair's Remarks

S. J. Kim started the meeting and took attendance of Standards Committee (SC or Committee) members and determined a quorum. She reviewed the NERC Antitrust Compliance Guidelines and reminded participants that the meeting is public and that notice of the meeting had been widely distributed.

B. Murphy provided introductory remarks. He noted that at the recent NERC Board meeting, it was mentioned several times that several members were pleased with the direction of the Committee, the Committee's relationship with NERC staff, its relationship with stakeholders, and the flexibility it showed on the physical security standard. He also noted that PRC-005, PRC-026 was authorized for posting by the SC Executive Committee in between the SC calls, and that the SC would discuss the revised TOP/IRO authorization on a May 16, 2014 call. He also stated that FERC announced a June 10, 2014 technical conference, the same date as the June SC meeting. Informal polling of the SC members indicated that the SC would still like to meet on June 10 and 11 with the understanding that some members may want to watch the technical conference on June 10. In light of the possible desire to watch the FERC conference, the SC Committee may conduct its business on the June 11, if only a half day is anticipated to cover the entire agenda. He also announced that V. Agnew has been promoted to Director of Standards.

V. Agnew made introductory remarks, and explained further that M. Lauby has been promoted to Chief Reliability Officer. She also announced that the Board adopted the physical security standard yesterday. She also added that the SBS software launch has been delayed due to technical issues. NERC will address and fix those outstanding issues, and then it will continue the registration effort.

Agenda Items

1. **Review of Agenda — (Approve)**
   F. Plett moved to approve the agenda, striking item 10.b.i. and move that item to a May 16, 2014 call. F. Gaffney seconded the motion.

   -The Committee approved the motion with no objections or abstentions.

2. **Consent Agenda — (Approve)**

   a. April 9, 2014 Meeting Minutes **– (Approve)**

      A. Gallo moved to approve the Minutes.

E. Skiba seconded the motion.

-The Committee approved the motion by unanimous consent.

3. **Three-Month Outlook on Upcoming Standard Projects or Issues — (Update)**
   V. Agnew provided the three-month outlook. She indicated that the EOP project may be ready earlier than anticipated, and she said the project might be ready to present to the SC by the 30th.

4. **Projects Under Development — (Review)**

   a. Project Tracking Spreadsheet
      B. Murphy indicated that the PMOS representatives have been working well with NERC staff and FERC staff on the TOP/IRO project and invited PMOS representatives to discuss their projects.

      J. Seelke asked that the QR checklist be updated due to a concern he saw with the wording in the Stable Power Swings project. V. Agnew indicated that an updated checklist may not be necessary, but that she would investigate and report back to the Committee.

   b. Projected Posting Schedule
      B. Nutter reported that the BAL-002 team is coordinating with the EOP team, and NERC does not want to post until coordination is complete. Further, the PRC-027 team is resolving an issue with FERC before posting.

5. **Draft 2015-2017 Reliability Standards Development Plan and Enhanced Periodic Review — (Authorize)**

   B. Murphy asked for a motion to adopt the action item as written with the understanding that SC leadership will work to incorporate suggested edits by members of the SC.

   F. Plett moved to adopt the action item as written. G. Zito seconded the motion.

   -The Committee approved the motion with no objections or abstentions.

6. **SC Meeting Schedule for 2015* — (Approve)**
   B. Murphy thanked B. Hampton for volunteering to lead this effort. He asked for a motion to adopt the action item as written and solicited volunteers to work with B. Hampton.

   J. Sterling moved to adopt the action item as written. B. Li seconded the motion.

   B. Hampton noted that it is useful to work with NERC staff on where the Committee intends to meet in 2015, and emphasized she would like support from SC members. V. Agnew volunteered NERC staff to assist. F. Plett expressed a preference of two meetings in the west, two in the east. J. Sterling asked the planners to consider costs when scheduling meetings. B. Murphy also noted that times should not conflict with FERC open meetings and should be scheduled at a time that FERC staff is available to attend.

   -The Committee approved the motion with no objections or abstentions.

7. **Detail of Minutes re: Appointment of Drafting Teams — (Approve)**
   B. Murphy provided background on this agenda item. He explained that D. Kiguel expressed concern about whether to provide more detail in the SC minutes with regard to drafting team appointments. G. Zito expressed support for more detail in the meeting minutes as the official record for the meetings, but S. Miller stated most minutes are not providing this level of detail. The agenda item was tabled for further discussion on the options proposed regarding the enhanced minutes.

8. **Reliability Issues Steering Committee Triage Diagram — (Informational item)**
   B. Murphy explained that he presented the RISC diagram to the SCPS and PMOS. F. Gaffney asked who decides whether a triage moves forward. B. Murphy responded that the SC would make that determination. B. Murphy asked for comments within the next two weeks on the diagram.

9. **Update on Reaching Quorum for Standards Ballots — (Informational item)**
   B. Murphy noted that there have been issues in reaching quorum on two standards within the last month. B. Murphy and S. Miller sent emails asking people to vote in order to close the ballot. The emails were helpful, and both are willing to do this as an interim resolution.

   L. Lee indicated that on a more permanent basis she would be working with B. Nutter on this issue, hopefully through the new balloting software. She further explained that NERC will develop a report to present to the SC to make it aware of the new features of the new balloting software that will help with the problem. NERC also is looking at patterns of people failing to vote and is targeting the June 2014 Committee meeting for a more detailed write-up.

   B. Murphy asked legal to explore whether NERC can publish who has and has not voted in a ballot. Others have an issue with making public such a list.

10. **Subcommittee Reports**

    a. **PMOS – (Update)**
       J. Sterling noted that since the SC met on April 17, 2014, she has added a column to tracking spreadsheet indicating consistency with the IERP effort. She stated there has been good discussion with PMOS liaisons on the status of projects. PMOS is considering possible changes to the PMOS charter, but that was tabled in anticipation of further conversations. Additionally, she added that the PMOS meetings are set for the rest of the year.

    b. **Process Subcommittee**

       i. **Process Subcommittee Membership – CONFIDENTIAL (Approve)**

    -This agenda item was moved to the May 16th SC call.

11. **Communication Updates and Activities — (Update)**
    S. Miller provided an update, and M. Huggins noted that next year NERC is looking at one long week for ERO auditor and Standards and Compliance workshops during the same week. The expectations is

to get more NERC staff involved. B. Murphy asked for an update as these ideas are a little further developed.

12. **Upcoming Standards Filings — (Review)**
    H. Hawkins provided an overview of upcoming standards filings as detailed in the agenda packet**.**
13. **Informational Items — (Enclosed)**
    a. SC Expectations
    b. 2014 Meeting Dates and Locations
    c. 2014 Standards Committee Roster
    d. Highlights of Parliamentary Procedure
14. **Adjourn**

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Minutes
Standards Committee Meeting

May 16, 2014 | 3:00 p.m. Eastern

NERC Antitrust Compliance Guidelines and Public Announcement*

S.J. Kim determined a quorum and reviewed the NERC Antitrust Compliance Guidelines and reminded participants that notice of the meeting had been widely distributed.

Introductions and Chair's Remarks

B. Murphy provided no opening remarks, but, rather, immediately transitioned to the agenda.

Agenda Items

1. **Review of Agenda — (Approve)**
   G. Zito moved to approve the agenda. F. McElvain seconded the motion.

   -The Committee approved the motion with no objections or abstentions.

2. **Project 2014-03: Revisions to Transmission Operations/Interconnection Reliability Operations and Coordination Reliability Standards *— (Authorize)**
   G. Zito moved to approve the agenda item as written with an addendum for VRF revisions. B. Li seconded the motion.

   L. Hussey provided background on the project, and explained that an addendum was necessary for full transparency to show the VRFs were updated for consistency. Further, the rationale boxes within the standards were revised. She went on to explain no substantive changes were made to the proposed standard requirements. L. Hussey added that PRC-001 now will need to be updated based on the TOP/IRO project, but those changes are not currently in the scope of the current project. L. Hussey also noted that there will be some duplicate language in TOP/IRO and the PRC-001 project, but the team will work with Compliance and Enforcement to ensure no double jeopardy occurs. V. Agnew added that PRC-027 will not be adding PRC-001 revisions to its project scope either.

   G. Zito provided additional context for the proposed standards by stating he attended the last drafting team meeting and the workshop. He expressed that the drafting team addressed outstanding issues and were responsive to many concerns. F. Gaffney asked is the drafting team supported the VRF changes in the recent addendum, and E. Dobrowolski, A Pankratz (vice chair of the standards drafting team) and L. Hussey replied that the team did support the changes. F. Gaffney further inquired about the necessary changes for PRC-001, and E. Dobrowolski answered that the language was added back to the proposed drafts because there were two concerns: 1) coordination and 2) notification. He explained the notifications were covered by the proposed standards, but the relaying of information was not sufficient. F. Gaffney then asked if PRC-027 could handle revisions to PRC-001. E.

Dobrowolski stated the necessary changes for coordination will mean more than passing data between entities, and V. Agnew explained that coordination will take another drafting team effort.

-The Committee approved the motion with no objections or abstentions.

3. **Project 2008-02- Undervoltage Load shedding revised SAR to include UFLS* — (Review)**
   F. Plett moved to approve the agenda item as written. R. Crissman seconded the motion.

   V. Agnew provided background by explaining the revised SAR was necessary to address an outstanding PRC-006 directive. UVLS includes language on corrective actions, and the UFLS standard now needs to mirror that language. F. Gaffney asked for a sentence on steady-state in the SAR to be revised. V. Agnew agreed to revisions clarifying what steady-state meant. F. McElvain and R. Blohm supported removing references to steady-state from the SAR. B. Murphy suggested that they propose a friendly amendment clarifying steady-state meant results-based standards that follow P81 and independent expert recommendations. He further explained that striking the phrase on steady-state in entirety could alter the SAR to allow any modifications in the standard. F. Gaffney supported a friendly amendment to just clarify the language with regard to steady-state. G. Zito then interjected by asking if QR was done on the documents. V. Agnew explained the documents were reviewed internally, and the SAR changes were minimal.

   -The Committee approved the motion with no objections or abstentions.

4. **Process Subcommittee Membership* – CONFIDENTIAL (Approve)**
   G. Zito moved to approve the agenda item as written. B. Li seconded the motion.

   L. Lee explained that solicitations for new members were sent broadly throughout the industry. The recommended new members include some SC members, active observers, and a new person to the committee.

   -The Committee approved the motion with no objections or abstentions.

5. **Adjourn**

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Anticipated Standards Committee Actions

Brian Murphy, Standards Committee Chair
Valerie Agnew, Director of Standards
Standards Committee

RELIABILITY | ACCOUNTABILITY

Drafting Team Appointments

- June 2014
  - Project 2010-14.2 Implementation of BAL Periodic Review Recommendations

Authorize Posting

- June 2014:
  - Project 2013-03: GMD Stage 2 (45-day comment and initial ballot of 1 standard) (High)
  - Project 2009-03: Emergency Operations (45-day comment and initial ballot of 1 standard) (High)
  - Project 2008-02: Undervoltage Load shedding (45-day comment and initial ballot for PRC-010-1) (High)
  - Project 2010-05.2: Protection Systems (Special Protection Systems) (45-day comment and initial ballot of one revised definition) (Medium)
  - Project 2014-01: Standards Applicability for Dispersed Power Producing Resources (45-day comment and ballot of high-priority standards) (High)
  - Project 2010-14.2: Implementation of BAL Periodic Review Recommendations (SAR for 30-day comment period) (Medium)

Authorize Posting

- July 2014:
  - Project 2008-02: Undervoltage Load shedding for UFLS (45-day comment and initial ballot for PRC-010-1) (High)

Authorize Posting

- August 2014:
  - Project 2012-09: Implementation of Interconnection Reliability Operations and Coordination Five-year Review (Medium)

Questions and Answers

Project 2008-02 Undervoltage Load Shedding (PRC-010-1)

Action

Authorize the posting of the Project 2008-02 Undervoltage Load Shedding proposed Reliability Standard PRC-010-1, Implementation Plan, Violation Risk Factors (VRFs), and Violation Severity Levels (VSLs) for an initial 45-day formal comment period with ballot pool formation during the first 30 days and initial ballot and non-binding poll during the last 10 days of the comment period.

Background

Project History

In January 2010, NERC posted the Project 2008-02 Undervoltage Load Shedding Standard Authorization Request (SAR) for public comment. The SAR cited NERC technical reports and assessments of UVLS programs and standards, along with the FERC Order No. 693 directive (Paragraph 1509) that approved PRC-010-0 but requested that it be modified to require that an integrated and coordinated approach be included in all protection systems on the Bulk Power System, including generators and transmission lines, generators' low voltage ride-through capabilities, and underfrequency load shedding (UFLS) and undervoltage load shedding (UVLS) programs.

Concurrently with the SAR posting, nominations were accepted for a drafting team. Work was deferred due to prioritization for the 2011–2013 Reliability Standards Development Plan (RSDP) and the effort was restarted as part of the 2013–2015 RSDP. A formal drafting team was appointed by the Standards Committee on May 21, 2013. The drafting team reevaluated the SAR to address NERC's existing UVLS standards such that they are results-based, address the Order No. 693 directive for PRC-010-0 and current reliability issues associated with UVLS, and consider all relative inputs, including appropriate NERC technical committee reports, Paragraph 81 criteria, Independent Expert Review Panel (IERP) recommendations, and existing standards and active development projects that may require coordinating changes.

A revised SAR was posted for a 30-day informal comment period in September 2013 along with draft standard requirements for a proposed PRC-010-1. Industry comments were considered and additional outreach was performed to develop a complete PRC-010-1, VRFs and VSLs, an Implementation Plan, and supporting documentation. The first formal posting was then postponed to coordinate with Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems) to accommodate the Project 2008-02 drafting team's proposed transition of certain types of UVLS systems to be covered by Special Protection System (SPS) or Remedial Action Scheme (RAS)-related standards due to commensurate design and characteristics. In the interim, PRC-010-1 and all supporting documents were posted for a 30-day informal comment period in March 2014 to solicit further feedback from the industry.

Proposal, Retirements, and Coordinating Efforts

Proposed PRC-010-1 consolidates, revises, and subsequently retires four existing UVLS standards: PRC-010-0 – Assessment of the Design and Effectiveness of UVLS Program; PRC-020-1 – Under-Voltage Load Shedding Program Database; PRC-021-1 – Under-Voltage Load Shedding Program Data; and PRC-022-1 – Under-Voltage Load Shedding Program Performance. Redlines to these standards are not provided because the revision resulted in changes to content and structure that do not lend themselves to a direct, one-to-one comparison.

PRC-010-1 also introduces a new NERC Glossary term "Undervoltage Load Shedding Program (UVLS Program)" to identify the systems to which the standard is applicable with respect to reliability requirement-related needs. As such, the term excludes a specific type of undervoltage-based load shedding that is more appropriately categorized as a SPS or RAS. This transition is being facilitated with concurrent Project 2010-05.2 – Special Protection Systems by way of a conforming revision to the definition of the term "Special Protection System" and is addressed in the implementation plans for both PRC-010-1 and the revised definition of "Remedial Action Scheme" proposed by Project 2010-05.2.

In addition, concurrent Project 2009-03 – Emergency Operations (EOP-011-1) proposes to retire certain requirements from EOP-003-2 that map to PRC-010-1. This transition is reflected in both the PRC-010-1 and EOP-011-1 implementation plans as well.

As a result of the coordinating efforts above, the effective dates of PRC-010-1 and its proposed new NERC Glossary term, EOP-011-1, the revised NERC Glossary definition of "Remedial Action Scheme," and each of the associated retirements are intended to align to accommodate the needed transitions of standard coverage. In addition, the formal comment periods and ballots for each of these projects are being timed to run concurrently or overlap.

Building Consensus and Quality

Over the course of Project 2008-02, NERC technical, legal, and compliance staff, and the Project Management and Oversight Committee (PMOS) liaison were intricately involved to facilitate a comprehensive approach to standard development. In addition, the Project 2008-02 drafting team regularly sought feedback on both quality and content of the standard from a variety of stakeholders, including representatives from trade associations, Regional standard review and system protection committees, appropriate NERC technical committees, and governmental authority staff. This included observer participation during drafting team meetings, informal discussions and reviews with colleagues, two informal comment periods, two industry webinars, and more than 20 outreach presentations with individual forums.

A final quality review of the Standard, VRFs and VSLs, and Implementation Plan was conducted May 21–28. All documents were reviewed by an industry technical expert, the PMOS liaison, and NERC staff from the Legal, Standards, and Reliability Assessments and Performance Analysis (RAPA) departments. Minor issues regarding clarity and consistency of language and general document formatting were identified and addressed by the lead Standards Developer and the drafting team Chair and Vice Chair. The documents provided to the Standards Committee reflect these revisions.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. Standard Authorization Request (SAR) posted for comment on January 20, 2010.
2. Revised SAR with supporting draft standard language posted for informal comment on September 10, 2013.
3. Draft standard posted for informal comment on March 17, 2014.

Description of Current Draft

The Undervoltage Load Shedding Standard Drafting Team is posting Draft 1 of PRC-010-1 – Undervoltage Load Shedding for a 45-day formal comment period and parallel (concurrent) initial ballot during the last 10 days of the comment period.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	June 2014
Final Ballot	September 2014
BOT Adoption	November 2014

Effective Dates

The standard shall become effective on the first day of the first calendar quarter that is 12 months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is 12 months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Version History

Version	Date	Action	Change Tracking
1.0	TBD	Completed revision, merging and updating PRC-010-0, PRC-020-1, PRC-021-1, and PRC-022-1.	

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Undervoltage Load Shedding Program (UVLS Program): An automatic load shedding program consisting of distributed relays and controls used to mitigate undervoltage conditions leading to voltage instability, voltage collapse, or Cascading impacting the Bulk Electric System (BES). Centrally-controlled undervoltage-based load shedding is not included.

Rationale for Definition: As part of the development of PRC-010-1, the drafting team found it necessary to introduce the term Undervoltage Load Shedding Program (UVLS Program) to establish PRC-010-1's applicability. The following are critical defining elements of the proposed term:

1) The definition provides flexibility for the Planning Coordinator or Transmission Planner to determine if a UVLS system falls under the defined term with respect to the impact on the reliability of the BES. (See Guidelines and Technical Basis section for further discussion.)

2) Centrally-controlled undervoltage-based load shedding is excluded because its design and characteristics are commensurate with a Special Protection Systems (SPS) or Remedial Action Scheme (RAS) (wherein load shedding is the remedial action). As such, centrally-controlled undervoltage-based load shedding should therefore be subject to SPS/RAS-related Reliability Standards. (See Guidelines and Technical Basis section for rationale.)

Consequently, the drafting team has recommended that Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems) include centrally-controlled undervoltage-based load shedding in the definition of a Special Protection System/Remedial Action Scheme.

3) The definition of UVLS Program is independent of whether the undervoltage load shedding relays are armed manually or automatically since the arming is done in anticipation of extreme conditions and not during the events when load shedding needs to occur.

When this standard has received ballot approval, the text boxes will be moved to the Guidelines and Technical Basis section of the Standard.

A. Introduction

1. **Title: Undervoltage Load Shedding**

2. **Number: PRC-010-1**

3. **Purpose:** To establish an integrated and coordinated approach to the design, evaluation, and reliable operation of Undervoltage Load Shedding Programs (UVLS Programs).

Rationale for Applicability: This standard is applicable to Planning Coordinators and Transmission Planners that have or are developing a UVLS Program, and to Distribution Providers and Transmission Owners responsible for the ownership, operation, or control of UVLS equipment as required by the UVLS Program established by the Transmission Planner or Planning Coordinator. These Distribution Providers and Transmission Owners are referred to as UVLS entities for the purpose of this standard.

The applicability includes both the Planning Coordinator and Transmission Planner because either may be responsible for designing and coordinating the program based on agreements, memorandums of understanding, or tariffs.

The phrase "Planning Coordinator or Transmission Planner" provides the flexibility for applicability to the entity that will perform the action. The expectation is not that both parties will perform the action, but rather that the Planning Coordinator and Transmission Planner will engage in discussion to determine the appropriate responsible entity.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Planning Coordinator

   4.1.2 Transmission Planner

   4.1.3 Undervoltage load shedding (UVLS) entities – Distribution Providers and Transmission Owners responsible for the ownership, operation, or control of UVLS equipment as required by the UVLS Program established by the Transmission Planner or Planning Coordinator.

5. Background:

UVLS Programs must work correctly to properly protect system reliability. Evaluating program effectiveness and coordination, and ensuring accurate and timely program implementation, assessment, and data will improve UVLS Program performance.

PRC-010-1 – Undervoltage Load Shedding is a consolidation and revision of the following Reliability Standards:

- PRC-010-0 – Assessment of the Design and Effectiveness of UVLS Program
- PRC-020-1 – Under-Voltage Load Shedding Program Database
- PRC-021-1 – Under-Voltage Load Shedding Program Data
- PRC-022-1 – Under-Voltage Load Shedding Program Performance

The UVLS Standard Drafting Team (or drafting team) developed the revised PRC-010-1 to meet the following objectives:

- Address the FERC directive in Order No. 693, Paragraph 1509 to modify PRC-010-0 to require an integrated approach to all protection systems.
- Replace the applicability to and involvement of the Regional Reliability Organization (RRO) in PRC-020-1 and PRC-021-1.
- Consolidate the UVLS-related standards into one comprehensive standard (similar to the construct of FERC-approved PRC-006-1– Automatic Underfrequency Load Shedding).
- Clearly identify and separate centrally-controlled undervoltage-based load shedding due to the reliability requirements needed for this type of load shedding as compared to other UVLS systems.
- Create a single results-based standard that addresses current reliability issues associated with UVLS.

As noted above, the drafting team found it is necessary to establish a bright line with respect to the characteristics of centrally-controlled undervoltage-based load shedding with regard to its reliability requirement-related needs. Because the design and characteristics of a centrally-controlled undervoltage-based load shedding system are commensurate with a Special Protection System (SPS) or Remedial Action Scheme (RAS), the drafting team maintains that this type of load shedding should be covered by SPS/RAS-related Reliability Standards.

Therefore, PRC-010-1 introduces a new NERC Glossary term, UVLS Program, to establish PRC-010-1's applicability to automatic load shedding programs consisting of distributed relays and controls used to mitigate undervoltage conditions leading to voltage instability, voltage collapse, or Cascading impacting the Bulk Electric System (BES). It is noted that this term excludes centrally-controlled undervoltage-based load shedding.

Subsequently, since the current NERC Glossary definition of Special Protection System excludes UVLS, concurrent Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems) will adjust the definition to exclude only UVLS Programs as defined above and therefore include centrally-controlled undervoltage-based load shedding. Of note, the drafting team for Project 2010-05.2 is proposing to change the term from "Special Protection System" to "Remedial Action Scheme." Accordingly, PRC-010-1 uses the term Remedial Action Scheme instead of Special Protection System.

In the current inventory of NERC Reliability Standards, there is one instance of the term undervoltage load shedding program, which is in NUC-001-2.1. Project 2012-13 – Nuclear Plant Interface Coordination has adjusted the language of this reference in proposed NUC-001-3 to eliminate any potential confusion of a lowercase usage of a defined term. Likewise, future projects containing standards that feature variations of the term (e.g., undervoltage load shedding system) will also be advised to consider the newly defined term.

Requirements of the revised Reliability Standard PRC-010-1 meet the following objectives:

- Evaluate a UVLS Program's effectiveness prior to implementation, including the program's coordination with other protection systems and generator voltage ride-through capabilities.
- Adhere to UVLS Program specifications and implementation schedule.
- Perform periodic assessment and performance analysis of UVLS Programs and resolve identified deficiencies.
- Maintain and share UVLS Program data.

Also of note, Project 2009-03 – Emergency Operations is proposing EOP-011-1, which, as part of the overall revisions, retires specific requirements from EOP-003-2 – Load Shedding Plans to eliminate identified redundancy between PRC-010-1 and EOP-003-2. In addition, the UVLS drafting team's intention is for PRC-004 to address Misoperations of UVLS Programs that are intended to trip one or more BES Elements. A change to make these types of UVLS Programs explicitly applicable to PRC-004 will be addressed once PRC-004-3 – Protection System Misoperation Identification and Correction is completed under Project 2010-05.1 – Misoperations (Phase 1 of Protection Systems).

B. Requirements and Measures

Rationale for R1: In Paragraph 1509 from Order No. 693, FERC directed NERC to require an integrated and coordinated approach to all protection systems. The drafting team agrees that a lack of coordination among protection systems is a key risk to reliability, and that each Planning Coordinator or Transmission Planner that develops a UVLS Program should evaluate the program's viability and effectiveness prior to implementation. This evaluation should include studies and analyses used when developing the program that show implementation of the program resolves the identified undervoltage conditions that led to its design. These studies and analyses should also show that the UVLS Program is integrated through coordination with generator voltage ride-through capabilities and other protection and control systems. Though presented as separate items, the drafting team recognizes that the studies that show coordination considerations and that the program addresses undervoltage issues may be interrelated and presented as one comprehensive analysis.

In addition, Requirement R1 also requires the Planning Coordinator or Transmission Planner to provide the UVLS Program's specifications and implementation schedule to applicable UVLS entities to implement the program. It is noted that studies to evaluate the effectiveness of the program should be completed prior to providing the specifications and schedule.

R1. Each Planning Coordinator or Transmission Planner that is developing a UVLS Program shall evaluate its effectiveness and subsequently provide the UVLS Program's specifications and implementation schedule to the UVLS entities responsible for implementing the UVLS Program. The evaluation shall include, but is not limited to, studies and analyses that show: *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

1.1. The implementation of the UVLS Program resolves the identified undervoltage issues that led to its development and design.

1.2. The UVLS Program is integrated through coordination with generator voltage ride-through capabilities and other protection and control systems, including, but not limited to, transmission line protection, auto-reclosing, Remedial Action Schemes, and other undervoltage-based load shedding programs.

M1. Acceptable evidence may include, but is not limited to, date-stamped studies and analyses, reports, or other documentation detailing the effectiveness of the UVLS Program, and date-stamped communications showing that the UVLS Program specifications and implementation schedule were provided to UVLS entities.

Rationale for R2: UVLS entities must implement a UVLS Program or address any necessary corrective actions for a UVLS Program according to the specifications and schedule provided by the Planning Coordinator or Transmission Planner. If UVLS entities do not implement the UVLS Program according to the specifications and schedule provided, the UVLS Program may not be effective and may not achieve its intended goal.

R2. Each UVLS entity shall adhere to the UVLS Program specifications and implementation schedule determined by its Planning Coordinator or Transmission Planner associated with UVLS Program development per Requirement R1 or with any Corrective Action Plans per Requirement R5. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

M2. Acceptable evidence must include date-stamped documentation on the completion of actions and may include, but is not limited to, identifying the equipment armed with UVLS relays, the UVLS relay settings, associated Load summaries, work management program records, work orders, and maintenance records.

Rationale for R3: A periodic comprehensive assessment (detailed analysis) should be conducted to identify and catalogue the accumulated effects of minor changes to the system that have occurred since the last assessment was completed, and should include an evaluation of each UVLS Program to ensure the continued integration through coordination. This comprehensive assessment supplements the NERC Reliability Standard TPL-001-4 annual assessment requirement to evaluate the impact of protection systems.

Based on the drafting team's knowledge and experience, and in keeping with time frames contained in similar requirements from other PRC Reliability Standards, 60 calendar months was determined to be the maximum amount of time allowable between assessments. Assessments will be performed sooner than the end of the 60-calendar month period if the Planning Coordinator or Transmission Planner determines that there are material changes to system topology or operating conditions that affect the performance of a UVLS Program. Note that the 60-calendar month time frame would reset after each assessment.

R3. Each Planning Coordinator or Transmission Planner shall perform a comprehensive assessment to evaluate the effectiveness of each of its UVLS Programs at least once every 60 calendar months. Each assessment shall include, but is not limited to, studies and analyses that evaluate whether: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

3.1. The UVLS Program resolves the identified undervoltage issues for which the UVLS Program is designed.

3.2. The UVLS Program is integrated through coordination with generator voltage ride-through capabilities and other protection and control systems, including, but not limited to, transmission line protection, auto-reclosing, Remedial Action Schemes, and other undervoltage-based load shedding programs.

M3. Acceptable evidence may include, but is not limited to, date-stamped reports or other documentation detailing the assessment of the UVLS Program.

Rationale for R4: A UVLS Program not functioning as expected during a voltage excursion event for which the UVLS Program was designed to operate presents a critical risk to system reliability. Therefore, a timely assessment to evaluate whether the UVLS Program resolved the undervoltage issues associated with the applicable event is essential. The 12 calendar months (from the date of the event) provides adequate time to coordinate with other Planning Coordinators, Transmission Planners, Transmission Operators, and UVLS entities, simulate pre- and post-event conditions, and complete the performance assessment.

R4. Each Planning Coordinator or Transmission Planner shall, within 12 calendar months of an event that resulted in a voltage excursion for which its UVLS Program was designed to operate, perform an assessment to evaluate whether its UVLS Program resolved the undervoltage issues associated with the event. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M4. Acceptable evidence may include, but is not limited to, date-stamped event data, event analysis reports, or other documentation detailing the assessment of the UVLS Program.

Rationale for R5: If program deficiencies are identified during an assessment of a UVLS Program performed in either Requirement R3 or R4, the Planning Coordinator or Transmission Planner must develop a Corrective Action Plan (CAP) to address the deficiencies. Based on the drafting team's knowledge and experience with UVLS studies, three calendar months was determined to provide a judicious balance between the reliability need to address deficiencies expeditiously and the time needed to consider potential solutions, coordinate resources, develop a CAP and implementation schedule, and provide the CAP and schedule to UVLS entities.

It is noted that the three-month time frame is only to develop the CAP and provide it to UVLS entities and does not encompass the time UVLS entities have to implement the CAP. Requirement R2 requires UVLS entities to execute the CAP according to the schedule provided by the Planning Coordinator or Transmission Planner.

R5. Each Planning Coordinator or Transmission Planner that identifies deficiencies in its UVLS Program during an assessment performed in either Requirement R3 or R4 shall develop a Corrective Action Plan to address the deficiencies and subsequently provide the Corrective Action Plan, including an implementation schedule, to UVLS entities

within three calendar months of completing the assessment. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M5. Acceptable evidence must include a date-stamped Corrective Action Plan that addresses identified deficiencies and may also include date-stamped reports or other documentation supporting the Corrective Action Plan. Evidence should also include date-stamped communications showing that the Corrective Action Plan and an associated implementation schedule were provided to UVLS entities.

Rationale for R6: Having accurate and current data is required for the Planning Coordinator to perform undervoltage studies and for use in event analyses. Requirement R6 supports this reliability need by requiring the Planning Coordinator to update its UVLS Program database at least once each calendar year.

R6. Each Planning Coordinator that has a UVLS Program in its area shall update a database containing data necessary to model its UVLS Program for use in event analyses and assessments of the UVLS Program at least once each calendar year. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. Acceptable evidence may include, but is not limited to, date-stamped spreadsheets, database reports, or other documentation demonstrating a UVLS Program database was updated.

Rationale for R7: Having accurate and current data is required for the Planning Coordinator to perform undervoltage studies and for use in event analyses. Requirement R7 supports this reliability need by requiring the UVLS entity to provide UVLS Program data in accordance with specified parameters.

R7. Each UVLS entity shall provide data to its Planning Coordinator according to the format and schedule specified by the Planning Coordinator to support maintenance of a UVLS Program database. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M7. Acceptable evidence may include, but is not limited to, date-stamped emails, letters, or other documentation demonstrating data was provided to the Planning Coordinator as specified.

Rationale for R8: Requirement R8 supports the integrated and coordinated approach to UVLS programs directed by Paragraph 1509 of Order No. 693 by requiring that UVLS Program data be shared with neighboring Planning Coordinators and Transmission Planners within a reasonable time period. Requests for the database should also be fulfilled for those functional entities that have a reliability need for the data (such as the Transmission Operators that develop System Operating Limits and Reliability Coordinators that develop Interconnection Reliability Operating Limits).

R8. Each Planning Coordinator that has a UVLS Program in its area shall provide its UVLS Program database to other Planning Coordinators and Transmission Planners within its Interconnection, and other functional entities with a reliability need, within 30 calendar days of a written request. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M8. Acceptable evidence may include, but is not limited to, date-stamped emails, letters, or other documentation demonstrating that the UVLS Program database was provided within 30 calendar days of receipt of a written request.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

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

The Planning Coordinator, Transmission Planner, Distribution Provider, and Transmission Owner shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

The applicable entity shall retain documentation as evidence since the last audit.

If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	High	N/A	N/A	N/A	The applicable entity that developed the UVLS Program failed to evaluate the program's effectiveness and subsequently provide the UVLS Program's specifications and implementation schedule to UVLS entities in accordance with Requirement R1, including the items specified in parts 1.1 and 1.2.

R2	Long-term Planning	High	N/A	N/A	The applicable entity failed to adhere to the UVLS Program specifications in accordance with Requirement R2. OR The applicable entity failed to adhere to the implementation schedule in accordance with Requirement R2.	The applicable entity failed to adhere to the UVLS Program specifications and implementation schedule in accordance with Requirement R2.
R3	Long-term Planning	Medium	N/A	N/A	N/A	The applicable entity failed to perform an assessment at least once during the 60 calendar months in accordance with Requirement R3, including the items specified in parts 3.1 and 3.2.

R4	Operations Planning	Medium	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 12 calendar months but less than or equal to 13 calendar months after an applicable event.	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 13 calendar months but less than or equal to 14 calendar months after an applicable event.	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 14 calendar months but less than or equal to 15 calendar months after an applicable event.	The applicable entity performed an assessment in accordance with Requirement R4 within a time period greater than 15 calendar months after an applicable event. OR The applicable entity failed to perform an assessment in accordance with Requirement R4.
R5	Operations Planning	Medium	The applicable entity developed a Corrective Action Plan and provided it to UVLS entities in accordance with Requirement R5 but was late by less than or equal to 15 calendar days.	The applicable entity developed a Corrective Action Plan and provided it to UVLS entities in accordance with Requirement R5 but was late by more than 15 calendar days but less than or equal to 30 calendar days.	The applicable entity developed a Corrective Action Plan and provided it to UVLS entities in accordance with Requirement R5 but was late by more than 30 calendar days but less than or equal to 45 calendar days.	The applicable entity developed a Corrective Action Plan and provided it to UVLS entities in accordance with Requirement R5 but was late by more than 45 calendar days. OR The responsible entity failed to develop a Corrective Action Plan or provide it to UVLS entities in accordance with Requirement R5.

R6	Operations Planning	Lower	The applicable entity updated the database in accordance with Requirement R6 but was late by less than or equal to 30 calendar days.	The applicable entity updated the database in accordance with Requirement R6 but was late by more than 30 calendar days but less than or equal to 60 calendar days.	The applicable entity updated the database in accordance with Requirement R6 but was late by more than 60 calendar days but less than or equal to 90 calendar days.	The applicable entity updated the database in accordance with Requirement R6 but was late by more than 90 calendar days. OR The applicable entity failed to update the database in accordance with Requirement R6.
R7	Operations Planning	Lower	The applicable entity provided data in accordance with Requirement R7 but was late by less than or equal to 30 calendar days per the specified schedule. OR The applicable entity provided data in accordance with Requirement R7 but the data was not provided according to the specified format.	The applicable entity provided data in accordance with Requirement R7 but was late by more than 30 calendar days but less than or equal to 60 calendar days per the specified schedule.	The applicable entity provided data in accordance with Requirement R7 but was late by more than 60 calendar days but less than or equal to 90 calendar days per the specified schedule.	The applicable entity provided data in accordance with Requirement R7 but was late by more than 90 calendar days per the specified schedule. OR The applicable entity failed to provide data in accordance with Requirement R7.

R8	Operations Planning	Lower	The applicable entity provided its UVLS Program database in accordance with Requirement R8 but was late by less than or equal to 15 calendar days.	The applicable entity provided its UVLS Program database in accordance with Requirement R8 but was late by more than 15 calendar days but less than or equal to 30 calendar days.	The applicable entity provided its UVLS Program database in accordance with Requirement R8 but was late by more than 30 calendar days but less than or equal to 45 calendar days.	The applicable entity provided its UVLS Program database in accordance with Requirement R8 but was late by more than 45 calendar days. OR The applicable entity failed to provide its UVLS Program database in accordance with Requirement R8.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Introduction

PRC-010-1 is a single, comprehensive standard that addresses the same reliability principles outlined in its legacy standards, PRC-010-0, PRC-020-1, PRC-021-1, and PRC-022-1. The standard also addresses a FERC directive from Order No. 693, Paragraph 1509. This paragraph directs NERC to develop a modification to PRC-010-0 that requires an integrated and coordinated approach to all protection systems, including generators and transmission lines, generators' low voltage ride-through capabilities, and underfrequency load shedding (UFLS) and UVLS programs.

Since FERC-approved PRC-006-1 – Automatic Underfrequency Load Shedding was developed under a similar construct of combining existing standards and addressing a FERC Order No. 693 directive, the drafting team looked to this standard as a guide. With the understanding that UVLS and UFLS systems have fundamental differences, the drafting team adopted PRC-006-1's industry-vetted reliability principles and language as applicable to UVLS Programs.

The drafting team's established purpose for PRC-010-1 is to clearly define the responsibilities of applicable entities to pursue an integrated and coordinated approach to the design, evaluation, and reliable operation of UVLS Programs. Since the need for and design of UVLS Programs is unique to each system preservation footprint, the intent of the standard is to provide a framework of reliability requirements for such programs to which each individual entity can apply its program's specific considerations and characteristics. The drafting team emphasizes that PRC-010-1 does not require a mandatory UVLS Program, nor does this standard address the need to have a UVLS Program. PRC-010-1 applies only after an entity has determined the need for a UVLS Program as a result of its own planning studies.

The drafting team provides the following discussion to support the approach to the standard. The information is meant to enhance the understanding of the reliability needs and deliverable expectations of each requirement, supported as necessary by technical principles and industry experience.

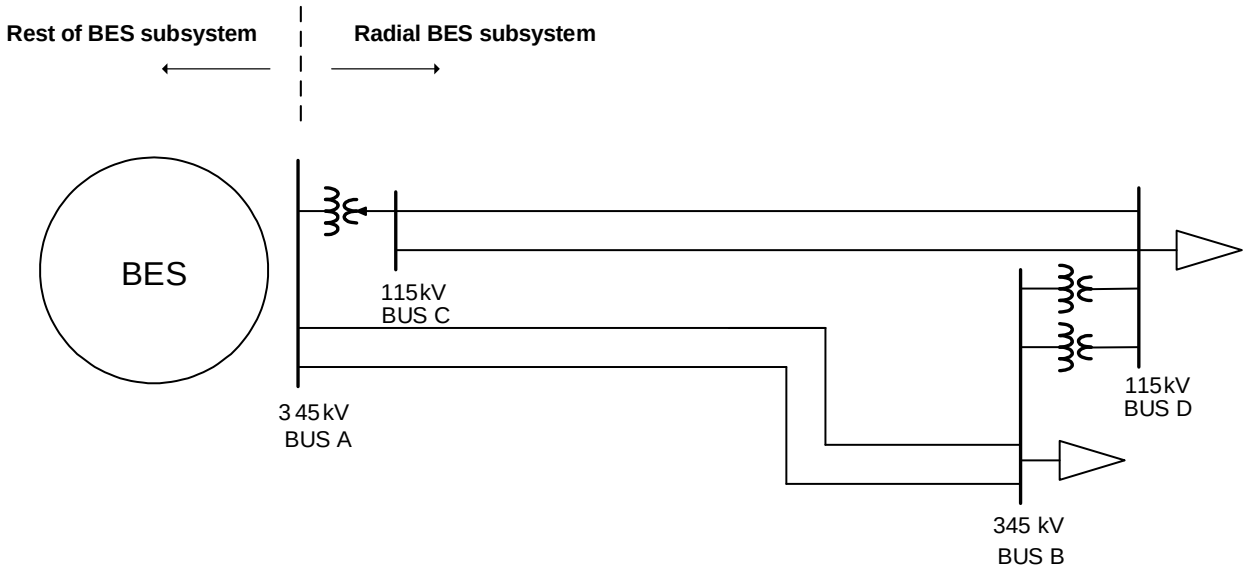
Guidelines for UVLS Program Definition

The definition for the term UVLS Program includes automatic load shedding programs that utilize only voltage inputs at locations where action is taken to shed load. As such, the failure of a single component is unlikely to affect the reliable operation of the program.

The definition for the term UVLS Program excludes centrally-controlled undervoltage-based load shedding, which utilizes inputs from multiple locations and may also utilize inputs other than voltages (such as generator reactive reserves, facility loadings, equipment statuses, etc.). The design and characteristics of a centrally-controlled undervoltage-based load shedding system are the same as that of a RAS, wherein load shedding is the remedial action. Therefore, just like for a RAS, the failure of a single component can compromise the reliable operation of centrally-controlled undervoltage-based load shedding.

To ensure that the UVLS Program standard's applicability is to only those undervoltage-based load shedding systems whose performance has an impact on system reliability, a UVLS Program must mitigate risk of one more of the following: voltage instability, voltage collapse, or Cascading impacting the BES. An example of a program that would not fall under this category is undervoltage-based load shedding installed to mitigate damage to equipment or local loads that are directly affected by the low voltage event.

Below is an example of a radial BES subsystem for which a UVLS system could be used as a solution to mitigate various issues following the loss of the 345 kV double circuit line between bus A and bus B. If the consequence of this Contingency is limited to undervoltage conditions, loss of load, or overloading of facilities within the contained area formed by buses A to D, a UVLS system (at buses B and D) used to mitigate this case would not fall under the definition of a UVLS Program. However, if this same UVLS system would be used to mitigate Adverse Reliability Impact outside this contained area, it would be classified as a wide-area undervoltage problem and would fall under the definition of UVLS Program.



High Level Requirement Overview

Requirement	Entity	Evaluate Program Effectiveness	Adhere to Program Specifications and Schedule	Perform Program Assessment (Periodic or Performance)	Develop a CAP to Address Program Deficiencies	Update and/or Share Program Data
R1	PC or TP	X				
R2	UVLS entity		X			
R3	PC or TP	X		X		
R4	PC or TP	X		X		
R5	PC or TP				X	
R6	PC					X
R7	UVLS entity					X
R8	PC					X

Guidelines for Requirement R1:

A UVLS Program may be developed and implemented to either serve as a safety net system protection measure against unforeseen extreme Contingencies or to achieve specific system performance for known transmission Contingencies for which dropping of load is allowed under Transmission Planning (TPL) Reliability Standards. Regardless of the purpose, it is important that the UVLS Program being implemented is effective in terms that it mitigates undervoltage conditions leading to voltage instability, voltage collapse, or Cascading. Consideration should be given to voltage set points and time delays, rate of voltage decay or recovery, power flow levels, etc. when designing a UVLS Program.

For the UVLS Program to be effective in achieving its goal, it is also necessary that the UVLS Program is coordinated with generator voltage ride-through capabilities and other protection and control systems that may have an impact on the performance of the UVLS Program. Some of these protection and control systems may include, but are not limited to, transmission line protection, RAS, other undervoltage-based load shedding programs, auto-reclosing, and controls of shunt capacitors, reactors, and static Var systems (SVSs).

For example, if the purpose of a UVLS Program is to mitigate fault-induced delayed voltage recovery (FIDVR) events in a large load center that also includes local generation, it is important that such a UVLS Program is coordinated with local generators' voltage ride-through capabilities. Generators in the vicinity of a load center are critical to providing dynamic voltage support to the system during FIDVR events. To maximize the benefit of online generation, the best practice may be to shed load prior to generation trip. However, occasionally, it may be best to let generation trip prior to load shed. Therefore, the impact of generation tripping should be considered while designing a UVLS Program.

Another example that can be highlighted is the coordination of a UVLS Program with automatic shunt reactor tripping devices if there are any on the system. Most likely, any shunt reactors on the system will trip off automatically after some time delay during low voltage conditions. In such cases, shunt reactors should be tripped before the load is shed to preserve the system. This may require coordination of time delays associated with the UVLS Program with shunt reactor tripping devices.

Examples given above demonstrate that, for a UVLS Program to be effective, proper consideration should be given to coordination of a UVLS Program with generator ride-through capabilities and other protection and control systems.

Guidelines for Requirement R2:

Once a Planning Coordinator or Transmission Planner has identified a need for a UVLS Program, the Planning Coordinator or Transmission Planner will develop a program that includes specifications and an implementation schedule, which are then provided to UVLS entities per Requirement R1. Specifications may include voltage set points, time delays, amount of load to be shed, the location at which load needs to be shed, etc. If UVLS entities do not implement the UVLS Program according to the specifications and schedule provided, the UVLS Program may not be effective and may not achieve its intended goal. The UVLS entity must document that all necessary actions were completed to implement the UVLS Program.

Similarly, when a Corrective Action Plan (CAP) to address UVLS Program deficiencies is developed by the Planning Coordinator or Transmission Planner and provided to UVLS entities per Requirement R5, UVLS entities must comply with the CAP and its associated implementation schedule to ensure that the UVLS Program is effective. The UVLS entity is required to complete the actions specified in the CAP, document the plan implementation, and retain the appropriate evidence to demonstrate implementation and completion.

Deferrals or other relevant changes to the UVLS Program specifications or CAP need to be documented so that the record includes not only what was planned, but what was implemented. Depending on the planning and documentation format used by the responsible entity, evidence of a successful execution could consist of signed-off work orders, printouts from work management systems, spreadsheets of planned versus completed work, timesheets, work inspection reports, paid invoices, photographs, walk-through reports, or other evidence.

For example, documentation of a CAP provides an auditable progress and completion confirmation for the identified UVLS Program deficiency:

> CAP Example 1 - Corrective actions for a quick triggering problem; preemptive actions for similar installations:
>
> > Fault records showed that a group of UVLS relays did trigger at the right undervoltage level but with shorter delays that expected. On-site inspections were completed in three weeks, confirming that the delay

time programmed on the relays was 60 cycles instead of 90 cycles. A plan was scheduled for the next eight weeks to correct to a 90-cycle time delay setting of those UVLS relays identified to have shorter time delay settings.

Applicability to other UVLS relays: Based on our risk assessment, we scheduled to verify and adjust all remaining UVLS relays time delay settings within a one-year period.

CAP Example 2 - Corrective actions for a firmware problem; preemptive actions for similar installations:

Fault records were provided to the manufacturer on 6/4/2014. On 6/11/2014, the manufacturer responded that the misoperation of the UVLS relay was caused by a bug in version 2 firmware, and recommended installing version 3 firmware. Version 3 firmware was installed on 6/12/2014.

Applicability to other UVLS relays: Based on our risk assessment, we plan to install firmware version 3 at all of our installations that are determined to be version 2. Proposed completion date is 12/31/2014.

The firmware replacements were completed on 12/4/2014.

Guidelines for Requirement R3:

In addition to the initial studies required to develop a UVLS Program, periodic comprehensive assessments (detailed analyses) are required to ensure its continued effectiveness. This assessment should be completed at least once every 60 calendar months to capture the accumulated effects of minor changes to the system that have occurred since the last assessment was completed. However, at any point in time, a Planning Coordinator or Transmission Planner may also determine that a material change to system topology or operating conditions affects the performance of the UVLS Program and therefore necessitates the same comprehensive assessment. Regardless of the trigger, each assessment should include an evaluation of each UVLS Program to ensure the continued integration through coordination.

This comprehensive assessment supplements the TPL-001-4 annual assessment requirement to evaluate the impact of protection systems. The 60-month period is the same time frame used in TPL-001-4 and in PRC-006-1.

With respect to situations in which a material change to system and topology or operating conditions would necessitate a comprehensive assessment of the UVLS Program, it is understood that the term material change is not transportable on a continent-wide basis. This determination must be made by the Planning Coordinator or Transmission Planner and should

be accompanied by documentation to support the technical rationale for determining material changes.

As specified in Requirement R3, a comprehensive assessment must be performed at least once every 60 calendar months. If a Planning Coordinator or Transmission Planner conducts a comprehensive assessment sooner for the reasons discussed above, the 60-month time period would restart upon completion of this assessment.

Guidelines for Requirement R4:

The goal of the assessment required in Requirement R4 is to evaluate whether the UVLS Program resolved the undervoltage issues for an event that occurred on the system. It is expected that the assessment should include event data analysis, such as the relevant sequence of events leading to the undervoltage conditions (e.g., Contingencies, operation of protection systems, and RAS) and field measurements useful to analyzing the behavior of the system. A comprehensive description of the UVLS Program operation should be presented, including conditions of the trigger (e.g., voltage levels, time delays) and amount of load shed for each affected substation. Simulations of the event shall be performed to evaluate the level of performance of the program for the event of interest and to identify deficiencies to be included in a CAP per Requirement R5.

The studies and analyses showing the effectiveness of the UVLS Program can be similar to what is required in Requirements R1 and R3, but should include a clear link between the evaluation of effectiveness (in studies using simulations) and the analysis of the event (with measurements and event data) that actually occurred. For example, differences between the expected and actual system behavior for the event of interest should be discussed and modeling assumptions should be evaluated. Important discrepancies between the simulations and the actual event should be investigated.

Considering the importance of an event that involves the operation of a UVLS Program, the 12-calendar-month period provides adequate time to analyze the event and perform an assessment while identifying deficiencies within a reasonable time. This time period is also required in PRC-006-1.

Guidelines for Requirement R5:

Requirement R5 promotes the prudent correction of an identified problem during assessment evaluations of each UVLS Program. Per Requirements R3 and R4, an assessment of an active UVLS Program is triggered:

- After material changes are made to system topology or operating conditions. Since every UVLS is unique, the Planning Coordinator or Transmission Planner will decide the degree to which the change in topology or operating condition becomes a material change sufficient to trigger an assessment of the existing UVLS Program.

- Within 12 calendar months of an event that resulted in a voltage excursion for which the program was designed to operate.

- At least once every 60 months. The default time frame of 60 months or less between assessments has the intention to assure that the cumulative changes to the network and operating condition affecting the UVLS Program are evaluated.

A CAP is a list of actions and an associated timetable for implementation to remedy a specific problem. It is a proven tool for resolving operational problems. Per Requirement R5, the Planning Coordinator or Transmission Planner is required to develop a CAP and provide it to UVLS entities to accomplish the purpose of this requirement, which is to prevent future deficiencies in the UVLS Program, thereby minimizing risk to the system. Determining the cause of the deficiency is essential in developing an effective CAP to avoid future re-occurrence of the same problem. A CAP can be revised if additional causes are found.

Based on industry experience and operational coordination timeframes, the drafting team believes that within three calendar months from the date an assessment is completed is a reasonable time frame for development of a CAP, including time to consider alternative solutions and coordination of resources. The "within three calendar months" time frame is solely to develop a CAP, including its implementation schedule, and provide it to UVLS entities. It does not include the time needed for its implementation by UVLS entities. This implementation time frame is dictated within the CAP's associated timetable for implementation, and the execution of the CAP according to its schedule is required in Requirement R2.

Guidelines for Requirements R6–R8

An accurate UVLS Program database is necessary for the Planning Coordinator or Transmission Planner to perform system reliability assessment studies and event analysis studies. Without accurate data, there is a possibility that annual reliability assessment studies that are performed by the Planning Coordinator can lead to erroneous results and therefore impact reliability. Also, without the accurate data, it is very difficult for the Planning Coordinator or Transmission Planner to duplicate a UVLS event and determine the root cause of the problem.

To support a UVLS Program database, it is necessary for each UVLS entity to provide accurate data to its Planning Coordinator. Each UVLS entity will provide the data according to the specified format and schedule provided by the Planning Coordinator. This is required in order for the Planning Coordinator to maintain and support a comprehensive UVLS Program database. By having a comprehensive database, the Planning Coordinator can embark on a reliability assessment or event analysis/benchmarking studies, identify the issues with the UVLS Program, and develop remedial action plans.

Items to be included in the UVLS Program database are as follows:

- Owner and operator of the UVLS Program
- Size and location of customer load, or percent of connected load, to be interrupted

- Corresponding voltage set points and clearing times
- Time delay from initiation to trip signal
- Breaker operating times
- Any other schemes that are part of or impact the UVLS Programs, such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS, and RAS.

Additionally, the UVLS Program database should be updated annually (once every calendar year) by the Planning Coordinator. The intent here is for UVLS entities to review the data annually and provide changes to the Planning Coordinators so that Planning Coordinators can keep the databases current and accurate for performing event analysis and other assessments.

Finally, a Planning Coordinator is required to provide information to other Planning Coordinators and Transmission Planners within its Interconnection, and other functional entities with a reliability need, within 30 calendar days of receipt of a written request. Thirty calendar days was selected as the time frame as it is considered to be reasonable and well-accepted by the industry. Also, this requirement of sharing the database with applicable functional entities supports the directive provided by FERC that requires an integrated and coordinated approach to UVLS programs (Paragraph 1509 of FERC Order No. 693).

Implementation Plan

PRC-010-1 – Undervoltage Load Shedding

Standards Involved

Approval:

- PRC-010-1 – Undervoltage Load Shedding

Retirements:

- PRC-010-0 – Assessment of the Design and Effectiveness of UVLS Program
- PRC-020-1 – Under-Voltage Load Shedding Program Database
- PRC-021-1 – Under-Voltage Load Shedding Program Data
- PRC-022-1 – Under-Voltage Load Shedding Program Performance

Prerequisite Approvals

- Revised definition of "Remedial Action Scheme" in Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems)

  Approval of the proposed definition of "Remedial Action Scheme" in Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems) is required to align the classification of centrally-controlled undervoltage-based load shedding with the proposed definition of "Undervoltage Load Shedding Program (UVLS Program)" below. The term "UVLS Program" excludes centrally-controlled undervoltage-based load shedding because the design and characteristics of centrally-controlled undervoltage-based load shedding are commensurate with Special Protection Systems or Remedial Action Schemes. The proposed definition of "Remedial Action Scheme" excludes "UVLS Programs." As a result, the proposed definition of "Remedial Action Scheme" clarifies that centrally-controlled undervoltage-based load shedding is included in its scope.

- EOP-011-1 in Project 2009-03 – Emergency Operations

  Project 2009-03 – Emergency Operations (EOP-011-1) proposes to retire EOP-003-2. Requirements R2, R4, and R7 of EOP-003-2 are not included in EOP-011-1, since these requirements map to PRC-010-1, Requirement R1. As a result, approval of EOP-011-1 is necessary to prevent overlap with Requirement R1 of PRC-010-1.

Revisions to the NERC Glossary of Terms

The following new term is proposed for addition:

Undervoltage Load Shedding Program (UVLS Program): An automatic load shedding program consisting of distributed relays and controls used to mitigate undervoltage conditions leading to voltage instability, voltage collapse, or Cascading impacting the Bulk Electric System (BES). Centrally-controlled undervoltage-based load shedding is not included.

Applicable Entities

- Planning Coordinator
- Transmission Planner
- UVLS entities – Distribution Providers and Transmission Owners responsible for the ownership, operation, or control of UVLS equipment as required by the UVLS Program established by the Transmission Planner or Planning Coordinator.

General Considerations

The effective dates of PRC-010-1 and its proposed new NERC Glossary term, EOP-011-1, the revised NERC Glossary definition of "Remedial Action Scheme," and each of the associated retirements are intended to align to accommodate the needed transitions of standard coverage noted above.

The implementation plan for the revised definition of "Remedial Action Scheme" addresses entities that will have newly identified Remedial Action Schemes resulting from the application of the defined term with respect to the inclusion of centrally-controlled undervoltage-based load shedding. Please refer to the implementation plan posted with the definition of "Remedial Action Scheme" in Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems) for more information.

Effective Date

PRC-010-1 and the definition of "Undervoltage Load Shedding Program (UVLS Program)" shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date that the standard and definition are approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard and the definition shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date the standard and definition are adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Retirement of Existing Standards:

PRC-010-0, PRC-020-1, PRC-021-1, and PRC-022-1 shall be retired at midnight of the day immediately prior to the effective date of PRC-010-1 in the particular jurisdiction in which the new standard is becoming effective.

PRC-010-1 is a consolidation of PRC-010-0 – Assessment of the Design and Effectiveness of UVLS Program, PRC-020-1 – Under-Voltage Load Shedding Program Database, PRC-021-1 – Under-Voltage Load Shedding Program Data, and PRC-022-1 – Under-Voltage Load Shedding Program Performance.

Project 2010-05.2 – Special Protection Systems

Action

Authorize posting of the revised definition of "Remedial Action Scheme" ("RAS"), the forty-three (43) Reliability Standards revised to reflect use of the single term RAS, and the associated Implementation Plan for an initial 45-day formal comment period with ballot pool formation during the first 30 days and initial ballot during the last 10 days of the comment period. A complete set of redlined and clean Reliability Standards has been included in the posting for convenience rather than forty-three (43) individual Reliability Standards.

Other supporting documents will be posted on the Project webpage. These include: an FAQ and Background document, a quick-reference guide for the changes to other Reliability Standards, and the redlined and final SAR for the Project.

Background

Project 2010-05.2 – Special Protection Systems was established to address issues identified in the technical report produced by the System Analysis and Modeling Subcommittee (SAMS) and System Protection and Control Subcommittee (SPCS). Those issues are:

1. The existing NERC Glossary of Terms definition for a Special Protection System (SPS) or Remedial Action Scheme (RAS) lacks the clarity and specificity necessary for consistent identification and classification of protection schemes as SPS or RAS across the eight NERC Regions, which leads to inconsistent application of the related NERC Reliability Standards.
2. There are six NERC (PRC) Reliability Standards that specifically pertain to SPS. Three of these standards are not mandatory and enforceable because FERC identified them as fill-in-the-blank standards in Order No. 693, Mandatory Reliability Standards for the Bulk-Power System. These standards assign the Regional Reliability Organizations responsibility to establish regional procedures and databases, and to assess and document the operation, coordination, and compliance of SPS. The deference to regional practices, coupled with lack of clarity in the definition of SPS, preclude consistent application of requirements pertaining to SPS.

The goals for this project as stated in the SAR are to:

1. Establish a definition of an SPS or RAS that provides the specificity needed to consistently identify and classify protection schemes as SPS or RAS across all eight NERC Regions, thereby promoting the consistent application of the NERC Reliability Standards related to SPS/RAS.
2. Correct the applicability of the NERC Reliability Standards related to SPS/RAS by assigning responsibilities to the specific users, owners, and operators of the Bulk-Power System rather than the RROs.
3. Develop continent-wide standards to address all aspects of SPS/RAS, including but not limited to, the:
    - planning, coordination, and design of SPS/RAS,
    - review, assessment, and documentation of SPS/RAS,

- operational considerations for monitoring, status notification, and response to failures,
- analysis of SPS/RAS operations, and defining and reporting of SPS/RAS misoperations,
- testing of SPS/RAS, and maintenance of any non-protection system components used.

Project 2010-05.2 is being conducted in two phases:

Phase 1 will address the definition of "Special Protection System" ("SPS") or "Remedial Action Scheme" ("RAS"). A revised definition of a SPS/RAS is required to provide the clarity and specificity necessary for the consistent identification and classification of protection schemes as SPS/RAS across the eight NERC Regions. Consequently, establishing a comprehensive industry-approved definition is mandatory to the development of quality Reliability Standards.

Phase 2 will address the six SPS/RAS-related Reliability Standards. The standards will be consolidated and will address all aspects of SPS/RAS. The applicability issues in PRC-012-0, PRC-013-0, and PRC-014-0 will be corrected by assigning the pertinent reliability objectives to the specific users, owners, and operators of the Bulk-Power System.

Phase 1

The Project 2010-05.2 – Special Protection System SDT is recommending to retain the term "Remedial Action Scheme" (RAS) and revise its definition, while retiring the term "Special Protection System" (SPS). After significant outreach, the drafting team asserts that a single term promotes consistency and that RAS is more descriptive of the purpose for which the scheme is installed.

Currently, NERC Reliability Standards and the NERC Glossary of Terms use both terms, "Special Protection System" and "Remedial Action Scheme" interchangeably. The terms appear in forty-three (43) standards and in several definitions. In most cases, both terms are included in the standards and written as: "Special Protection Systems or Remedial Action Schemes." The SDT evaluated the existing standards and recommended any necessary revisions to retain the single term, "RAS." Many of the same changes would be required regardless of which single term is retained. A summary of the occurrences of the terms is included in the posted document *Uses of "Special Protection System" and "Remedial Action Scheme"* and complete versions of the standards are included in the posted document *Revised Reliability Standards for the Revised Definition of "Remedial Action Scheme."*

NOTE: *The standard numbers currently include an (X) to indicate the version numbering will be updated. Some standards are open in current projects and others are pending with governmental authorities. As a result, NERC will assign the appropriate version number prior to BOT adoption.*

The proposed definition of RAS must be broad to include the variety of System conditions monitored and corrective actions taken by RAS. This "broadness," however, necessitates an

exclusion list because without the exclusions, equipment and schemes that should not be considered RAS could be subject to the requirements of the RAS-related Reliability Standards. The exclusion list assures that commonly applied protection and control systems are not unintentionally included as RAS.

The Project 2010-05.2 SPS SDT is coordinating the development of the RAS definition with the development of PRC-010-1 by the SDT for Project 2008-02 – Undervoltage Load Shedding. The UVLS SDT is introducing a new NERC Glossary term, UVLS Program, to clearly establish the applicability of PRC-010-1. The proposed term UVLS Program is defined as: "An automatic load shedding program consisting of distributed relays and controls used to mitigate undervoltage conditions leading to voltage instability, voltage collapse, or Cascading impacting the Bulk Electric System (BES). Centrally controlled undervoltage-based load shedding is not included."

Note that the proposed definition excludes centrally controlled undervoltage-based load shedding. The UVLS SDT maintains that the design and characteristics of centrally controlled undervoltage-based load shedding are commensurate with RAS (wherein load shedding is the remedial action) and, as such, should be subject to RAS-related Reliability Standards. The Project 2010-05.2 SPS SDT agrees with this assessment and revised the definition of RAS to clarify that it is inclusive of centrally controlled undervoltage-based load shedding. Collectively, the two definitions will promote consistency in the identification of centrally controlled undervoltage-based load shedding as RAS. The coordination of these revisions is required to maintain coverage of those systems and prevent a reliability gap.

Building Consensus and Quality

During the development of the proposed definition and Implementation Plan, NERC technical, legal, and compliance staff worked together to facilitate a comprehensive approach to the development. Additionally, the drafting team regularly sought feedback on both quality and content of the definition from a variety of stakeholders through numerous outreach presentations with individual forums that included Regional standard review groups and Regional system protection committees. The drafting team consulted with members of various NERC technical committees and governmental authority staff. The draft definition was posted for a 30-day informal comment period and the revised definition reflects many of the changes suggested by stakeholders.

A final quality review of the definition, Implementation Plan, and associated documents was conducted May 27–June 2. All documents were reviewed by NERC staff from the Legal, Standards, and Reliability Assessments and Performance Analysis (RAPA) departments, as well as the SDT Chair, Vice Chair, and the PMOS liaison. Minor issues regarding clarity and consistency of language and general document formatting were identified and addressed. The documents provided to the Standards Committee reflect these revisions.

Standards Authorization Request Form

When completed, email this form to:
Valerie.Agnew@nerc.net
For questions about this form or for assistance in completing the form, call Valerie Agnew at 404-446-2566.

NERC welcomes suggestions for improving the reliability of the Bulk-Power System through improved Reliability Standards. Please use this form to submit your proposal for a new NERC Reliability Standard or a revision to an existing standard.

Request to propose a new or a revision to a Reliability Standard			
Proposed Project Number and Name	Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems)		
Proposed Project Purpose:	Revise NERC Glossary of Terms definition: Special Protection System (SPS) Revise SPS-related Reliability Standards		
Date Submitted:	02/12/2014		
SAR Requester Information			
Name:	Al McMeekin		
Organization:	NERC		
Telephone:	404-446-9675	E-mail:	Al.McMeekin@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard ☒ Revision to existing Standard		☒ Withdrawal of existing Standard ☐ Urgent Action	

SAR Information
Industry Need (What is the industry problem this request is trying to solve?):
The existing NERC Glossary of Terms definition for a Special Protection System (SPS) or, as used in the Western Interconnection, a Remedial Action Scheme (RAS), lacks the clarity and specificity necessary for consistent identification and classification of protection schemes as SPS or RAS across the eight NERC Regions, leading to inconsistent application of the related NERC Reliability Standards. In FERC Order No. 693 (dated March 16, 2007), the Commission identified three of the SPS-related Reliability Standards (PRC-012-0, PRC-013-0, and PRC-014-0) as fill-in-the-blank standards because they are applicable to the Regional Reliability Organizations (RROs). Consequently, the Commission did not approve or remand them, rendering them neither mandatory nor enforceable. This project also addresses, in part, four recommendations related to identification and coordination of SPS from the joint FERC-NERC inquiry of the September 2011 Southwest Blackout Event. NOTE: Detailed information is included in the NERC Planning Committee report "Special Protection Systems (SPS) and Remedial Action Schemes (RAS): Assessment of Definition, Regional Practices, and Application of Related Standards" Revision 0.1 – April 2013.
Purpose or Goal (How does this request propose to address the problem described above?):
1) Establish a definition of an SPS or RAS that provides the specificity needed to consistently identify and classify protection schemes as SPS or RAS across all eight NERC Regions, thereby promoting the consistent application of the NERC Reliability Standards related to SPS. 2) Correct the applicability of the NERC Reliability Standards related to SPS/RAS by assigning responsibilities to the specific users, owners, and operators of the Bulk-Power System rather than the RROs. 3) Develop continent-wide standards to address all aspects of SPS/RAS, including but not limited to, the: • planning, coordination, and design of SPS/RAS, • review, assessment, and documentation of SPS/RAS, • operational considerations for monitoring, status notification, and response to failures, • analysis of SPS/RAS operations, and defining and reporting of SPS/RAS misoperations, • testing of SPS/RAS, and maintenance of any non-protection system components used.

SAR Information
Identify the Objectives of the proposed standard's requirements (What specific reliability deliverables are required to achieve the goal?):
Successful implementation of a modified definition for an SPS/RAS, with the revised SPS/RAS-related Reliability Standards will improve Bulk-Power System reliability by providing continent-wide consistency in the identification and classification of SPS or RAS, and by promoting the consistent application of the related Reliability Standards.
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The project will develop a revised definition of SPS or RAS, as well as revise the NERC Reliability Standards that address the: • review of new or modified SPS/RAS, • annual assessments of SPS/RAS in transmission planning studies, • periodic comprehensive SPS/RAS assessments, • analysis and reporting of SPS/RAS misoperations, • maintenance, testing and operational aspects of SPS/RAS.
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
The SDT will revise the definition of SPS/RAS to provide the clarity and specificity necessary for consistent identification and classification of protection schemes as SPS/RAS across the eight NERC Regions. The SDT will revise or retire the six existing SPS/RAS-related Reliability Standards: • PRC-012-0 Special Protection System Review Procedure • PRC-013-0 Special Protection System Database • PRC-014-0 Special Protection System Assessment • PRC-015-0 Special Protection System Data and Documentation • PRC-016-0.1 Special Protection System Misoperations • PRC-017-0 Special Protection System Maintenance and Testing

SAR Information
The SDT will correct the applicability in PRC-012-0, PRC-013-0, and PRC-014-0 by assigning the requirements to the specific users, owners, and operators of the Bulk Power System. The SDT will combine appropriate requirements from PRC-012-0, PRC-013-0, PRC-014-0, PRC-015-0, PRC-016-0.1, and PRC-017-0 into one or more Reliability Standard(s). The new standard(s) will provide specific requirements for: • review of new or modified SPS/RAS; • annual assessments of SPS/RAS in transmission planning studies; • periodic comprehensive SPS/RAS assessments; • design of SPS/RAS; • operations and misoperations; • maintenance and testing of SPS/RAS; and • maintenance and testing of non-Protection System components used in SPS/RAS; and • coordination of SPS/RAS with other SPS/RAS, UFLS, UVLS, and Protection Systems. Due to the significant difference between Protection Systems and SPS, the subject of SPS misoperation is not addressed in the revision of Reliability Standard PRC-004. This SDT will develop a definition for SPS/RAS misoperation and revise PRC-016-0.1. The new Reliability Standard will provide specific requirements for the analysis of SPS operations and reporting of SPS misoperations. The SDT will address the complexity of maintaining and testing SPS, as well as the maintenance and testing of non-Protection System components used in SPS in a Reliability Standard. This SDT will coordinate with the PRC-005-4 SDT to prevent any overlaps or gaps in coverage. The SDT also will consider operational considerations for monitoring, status notification, and response to failures of SPS/RAS; and, if necessary, modify other related standards. The SDT will retire requirements that are administrative in nature that are not necessary for reliability of the Bulk-Power System, or that are superseded by other requirements; i.e., the new Reliability Standards will qualify as steady-state. No market interface impacts are anticipated.

Reliability Functions		
The Standard will Apply to the Following Functions (Check each one that applies.)		
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☐	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☒	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☒	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.

Reliability Functions	
☐ Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber-attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Reliability and Market Interface Principles	
Related Standards	
Standard No.	Explanation
IRO-005-3.1a	The SDT may decide not to change this standard, but the SDT should keep the standard in mind since it contains potentially overlapping requirements.
PRC-001-1.1	The SDT may decide not to change this standard, but the SDT should keep the standard in mind since it contains potentially overlapping requirements.
PRC-005-2	The SDT may decide not to change this standard, or subsequently approved versions, but the SDT should keep the standard in mind to avoid any gaps or overlap between this standard and PRC-017-1.
PRC-010-1	The SDT may adjust the definition of Special Protection System to include centrally-controlled undervoltage-based load shedding or exclude UVLS Programs.
CIP-002, CIP-003, CIP-004, CIP-005, CIP-006 CIP-007, CIP-008, CIP-009, CIP-010 CIP-011, EOP-004, FAC-010, FAC-011, IRO-005, IRO-014, MOD-029, MOD-030, NUC-001, PRC-001, PRC-004-WECC, PRC-005, PRC-006, PRC-012, PRC-013, PRC-014, PRC-015, PRC-016, PRC-017, PRC-020, PRC-021, PRC-023, PRC-024, PRC-025, TOP-005, TPL-001, TPL-002, TPL-003,	The SDT will review all current standards that include the term SPS or RAS to ensure the modified term and definition are congruent.

Reliability and Market Interface Principles	
TPL-004; NERC Glossary of Terms: Special Protection System, Remedial Action Scheme; WECC Regional Term: Dependability-Based Misoperation, WECC Regional Term: Functionally Equivalent RAS, WECC Regional Term: Security-Based Misoperation	

Related SARs	
Project	Explanation
Project 2008-02 – Undervoltage Load Shedding	The UVLSSDT is recommending that Project 2010-05.2 – Special Protection Systems adjust the definition of Special Protection System to include centrally-controlled undervoltage-based load shedding or exclude UVLS Programs.

Regional Variances	
Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
RFC	
SERC	
SPP	
WECC	Communicate recommended changes to Regional Reliability Standard PRC-004-WECC-1, regional criteria PRC-(012 through 014)-WECC-CRT-2, and PRC-013 RAS Reporting Template; or, if necessary, incorporate a regional variance in the NERC Reliability Standards developed by this project. All changes to any WECC standards and documents will be coordinated with WECC.

Standards Authorization Request Form

When completed, email this form to:
Valerie.Agnew@nerc.net
For questions about this form or for assistance in completing the form, call Valerie Agnew at 404-446-2566.

NERC welcomes suggestions for improving the reliability of the Bulk-Power System through improved Reliability Standards. Please use this form to submit your proposal for a new NERC Reliability Standard or a revision to an existing standard.

Request to propose a new or a revision to a Reliability Standard			
Proposed Project Number and Name	Project 2010-05.2 – Special Protection Systems (Phase 2 of Protection Systems)		
Proposed Project Purpose:	Revise NERC Glossary of Terms definition: Special Protection System (SPS) Revise SPS-related Reliability Standards		
Date Submitted:	02/12/2014		
SAR Requester Information			
Name:	Al McMeekin		
Organization:	NERC		
Telephone:	404-446-9675	E-mail:	Al.McMeekin@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard ☒ Revision to existing Standard		☒ Withdrawal of existing Standard ☐ Urgent Action	

SAR Information
Industry Need (What is the industry problem this request is trying to solve?):
The existing NERC Glossary of Terms definition for a Special Protection System (SPS) or, as used in the Western Interconnection, a Remedial Action Scheme (RAS), lacks the clarity and specificity necessary for consistent identification and classification of protection schemes as SPS or RAS across the eight NERC Regions, leading to inconsistent application of the related NERC Reliability Standards. In FERC Order No. 693 (dated March 16, 2007), the Commission identified three of the SPS-related Reliability Standards (PRC-012-0, PRC-013-0, and PRC-014-0) as fill-in-the-blank standards because they are applicable to the Regional Reliability Organizations (RROs). Consequently, the Commission did not approve or remand them, rendering them neither mandatory nor enforceable. This project also addresses, in part, four recommendations related to identification and coordination of SPS from the joint FERC-NERC inquiry of the September 2011 Southwest Blackout Event. NOTE: Detailed information is included in the NERC Planning Committee report "Special Protection Systems (SPS) and Remedial Action Schemes (RAS): Assessment of Definition, Regional Practices, and Application of Related Standards" Revision 0.1 – April 2013.
Purpose or Goal (How does this request propose to address the problem described above?):
1) Establish a definition of an SPS or RAS that provides the specificity needed to consistently identify and classify protection schemes as SPS or RAS across all eight NERC Regions, thereby promoting the consistent application of the NERC Reliability Standards related to SPS. 2) Correct the applicability of the NERC Reliability Standards related to SPS/RAS by assigning responsibilities to the specific users, owners, and operators of the Bulk-Power System rather than the RROs. 3) Develop continent-wide standards to address all aspects of SPS/RAS, including but not limited to, the: • planning, coordination, and design of SPS/RAS, • review, assessment, and documentation of SPS/RAS, • operational considerations for monitoring, status notification, and response to failures, • analysis of SPS/RAS operations, and defining and reporting of SPS/RAS misoperations, • testing of SPS/RAS, and maintenance of any non-protection system components used.

SAR Information
Identify the Objectives of the proposed standard's requirements (What specific reliability deliverables are required to achieve the goal?):
Successful implementation of a modified definition for an SPS/RAS, with the revised SPS/RAS-related Reliability Standards will improve Bulk-Power System reliability by providing continent-wide consistency in the identification and classification of SPS or RAS, and by promoting the consistent application of the related Reliability Standards.
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The project will develop a revised definition of SPS or RAS, as well as revise the NERC Reliability Standards that address the: • review of new or modified SPS/RAS, • annual assessments of SPS/RAS in transmission planning studies, • periodic comprehensive SPS/RAS assessments, • analysis and reporting of SPS/RAS misoperations, • maintenance, testing and operational aspects of SPS/RAS.
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
The SDT will revise the definition of SPS/RAS to provide the clarity and specificity necessary for consistent identification and classification of protection schemes as SPS/RAS across the eight NERC Regions. The SDT will revise or retire the six existing SPS/RAS-related Reliability Standards: • PRC-012-0 Special Protection System Review Procedure • PRC-013-0 Special Protection System Database • PRC-014-0 Special Protection System Assessment • PRC-015-0 Special Protection System Data and Documentation • PRC-016-0.1 Special Protection System Misoperations • PRC-017-0 Special Protection System Maintenance and Testing

SAR Information
The SDT will correct the applicability in PRC-012-0, PRC-013-0, and PRC-014-0 by assigning the requirements to the specific users, owners, and operators of the Bulk Power System. The SDT will combine appropriate requirements from PRC-012-0, PRC-013-0, PRC-014-0, PRC-015-0, PRC-016-0.1, and PRC-017-0 into one or more Reliability Standard(s). The new standard(s) will provide specific requirements for: • review of new or modified SPS/RAS; • annual assessments of SPS/RAS in transmission planning studies; • periodic comprehensive SPS/RAS assessments; • design of SPS/RAS; • operations and misoperations; • maintenance and testing of SPS/RAS; and • maintenance and testing of non-Protection System components used in SPS/RAS; and • coordination of SPS/RAS with other SPS/RAS, UFLS, UVLS, and Protection Systems. Due to the significant difference between Protection Systems and SPS, the subject of SPS misoperation is not addressed in the revision of Reliability Standard PRC-004. This SDT will develop a definition for SPS/RAS misoperation and revise PRC-016-0.1. The new Reliability Standard will provide specific requirements for the analysis of SPS operations and reporting of SPS misoperations. The SDT will address the complexity of maintaining and testing SPS, as well as the maintenance and testing of non-Protection System components used in SPS in a Reliability Standard. This SDT will coordinate with the PRC-005-4 SDT to prevent any overlaps or gaps in coverage. The SDT also will consider operational considerations for monitoring, status notification, and response to failures of SPS/RAS; and, if necessary, modify other related standards. The SDT will retire requirements that are administrative in nature that are not necessary for reliability of the Bulk-Power System, or that are superseded by other requirements; i.e., the new Reliability Standards will qualify as steady-state. No market interface impacts are anticipated.

Reliability Functions		
The Standard will Apply to the Following Functions (Check each one that applies.)		
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☐	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☒	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☒	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.

Reliability Functions	
☐ Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber-attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Reliability and Market Interface Principles	
Related Standards	
Standard No.	Explanation
IRO-005-3.1a	The SDT may decide not to change this standard, but the SDT should keep the standard in mind since it contains potentially overlapping requirements.
PRC-001-1.1	The SDT may decide not to change this standard, but the SDT should keep the standard in mind since it contains potentially overlapping requirements.
PRC-005-2	The SDT may decide not to change this standard, or subsequently approved versions, but the SDT should keep the standard in mind to avoid any gaps or overlap between this standard and PRC-017-1.
PRC-010-1	The SDT may adjust the definition of Special Protection System to include centrally-controlled undervoltage-based load shedding or exclude UVLS Programs.
CIP-002, CIP-003, CIP-004, CIP-005, CIP-006 CIP-007, CIP-008, CIP-009, CIP-010 CIP-011, EOP-004, FAC-010, FAC-011, IRO-005, IRO-014, MOD-029, MOD-030, NUC-001, PRC-001, PRC-004-WECC, PRC-005, PRC-006, PRC-012, PRC-013, PRC-014, PRC-015, PRC-016, PRC-017, PRC-020, PRC-021, PRC-023, PRC-024, PRC-025, TOP-005, TPL-001, TPL-002, TPL-003,	The SDT will review all current standards that include the term SPS or RAS to ensure the modified term and definition are congruent.

Reliability and Market Interface Principles	
TPL-004; NERC Glossary of Terms: Special Protection System, Remedial Action Scheme; WECC Regional Term: Dependability-Based Misoperation, WECC Regional Term: Functionally Equivalent RAS, WECC Regional Term: Security-Based Misoperation	

Related SARs	
Project	Explanation
Project 2008-02 – Undervoltage Load Shedding	The UVLSSDT is recommending that Project 2010-05.2 – Special Protection Systems adjust the definition of Special Protection System to include centrally-controlled undervoltage-based load shedding or exclude UVLS Programs.

Regional Variances	
Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
RFC	
SERC	
SPP	
WECC	Communicate recommended changes to Regional Reliability Standard PRC-004-WECC-1, regional criteria PRC-(012 through 014)-WECC-CRT-2, and PRC-013 RAS Reporting Template; or, if necessary, incorporate a regional variance in the NERC Reliability Standards developed by this project. All changes to any WECC standards and documents will be coordinated with WECC.

Proposed Definition of "Remedial Action Scheme"

Remedial Action Scheme (RAS)

A scheme designed to detect predetermined System conditions and automatically take corrective actions that may include, but are not limited to, curtailing or tripping generation or other sources, curtailing or tripping load, or reconfiguring a System(s). RAS accomplish one or more of the following objectives:

- Meet requirements identified in the NERC Reliability Standards;
- Maintain System stability;
- Maintain acceptable System voltages;
- Maintain acceptable power flows;
- Limit the impact of Cascading; or
- Address other Bulk Electric System (BES) reliability concerns.

These schemes are not Protection Systems; however, they may share components with Protection Systems.

The following do not individually constitute a RAS:

a. Out-of-step tripping and power swing blocking
b. Automatic underfrequency load shedding (UFLS) programs
c. Undervoltage Load Shedding Programs (UVLS Programs)
d. Autoreclosing schemes
e. Schemes applied on an Element for non-Fault conditions, such as, but not limited to, generator loss-of-field, transformer top-oil temperature, high voltage, or overload to protect the Element against damage by removing it from service
f. Controllers that switch or regulate series or shunt reactive devices, flexible alternating current transmission system (FACTS) devices, phase-shifting transformers, variable-frequency transformers, tap-changing transformers, or generation excitation, and that are located at and monitor quantities solely at the same station as the Element being switched or regulated
g. FACTS controllers that remotely switch static shunt reactive devices located at other stations to regulate the output of a single FACTS device
h. Schemes or controllers that remotely switch shunt reactors and shunt capacitors for voltage regulation that would otherwise be manually switched
i. Schemes that automatically de-energize a line for a non-Fault operation when one end of the line is open

j. Schemes that provide anti-islanding protection (e.g., protect load from effects of being isolated with generation that may not be capable of maintaining acceptable frequency and voltage)

k. Automatic sequences that proceed when manually initiated solely by an operator

l. Modulation of HVdc or FACTS via supplementary controls, such as angle damping or frequency damping applied to damp local or inter-area oscillations

m. Sub-synchronous resonance (SSR) protection schemes that directly detect sub-synchronous quantities (e.g., currents or torsional oscillations)

Existing NERC Glossary of Terms Definitions

Special Protection System (Remedial Action Scheme)

An automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability. Such action may include changes in demand, generation (MW and Mvar), or system configuration to maintain system stability, acceptable voltage, or power flows. An SPS does not include (a) underfrequency or undervoltage load shedding or (b) fault conditions that must be isolated or (c) out-of-step relaying (not designed as an integral part of an SPS). Also called Remedial Action Scheme.

Remedial Action Scheme

See “Special Protection System”

Uses of "Special Protection System" and "Remedial Action Scheme" in Reliability Standards

This document provides a summary of the occurrences of "Special Protection System" ("SPS") and "Remedial Action Scheme" ("RAS") in the existing NERC Reliability Standards to assist entities in assessing the impact of the proposed definition of "Remedial Action Scheme." The existing Reliability Standards and certain NERC Glossary of Terms use the terms interchangeably.[1] Changes are proposed in this Project for each applicable standard and NERC Glossary term to align the use of the terminology in each instance. Where only the term SPS occurs, it was replaced with RAS. Where both terms, SPS and RAS, occur, the drafting team deleted the references to SPS. Where only the term RAS occurs, no change was made. In all cases, entities should apply the proposed definition of RAS to its own schemes, and determine any impact.

General Description of Definition Change

The revised definition of RAS will create one definition to replace both existing definitions in the NERC Glossary of Terms, for use throughout the NERC Reliability Standards. The revised definition of RAS addresses ambiguities within the existing definition and provides clarity to promote consistency in the application of the standards by the responsible entities and the auditing of the standards by compliance staff. The revised definition of RAS recasts the existing definition of SPS to:

- more precisely describe the objectives of the schemes;
- more precisely describe exclusions;
- state the relationship between Protection Systems and RAS; and
- clarify that centrally controlled undervoltage-based load shedding is included in the definition.

Uses of SPS and RAS in Existing Reliability Standards and NERC Glossary of Terms

The table below includes each occurrence of SPS and RAS found in the applicability sections, requirements, tables, and attachments of the existing NERC Reliability Standards (as of May 16, 2014). The table does not reflect any associated occurrences in other sections of the standard such as the measures, compliance information, and Violation Severity Levels. All occurrences have been reflected in the separate document *Revised Reliability Standards for the Revised Definition of "Remedial Action Scheme."*

[1] NERC, *Reliability Standards for the Bulk Electric Systems of North America* (Updated May 16, 2014).

Standard No.	Existing Standard Language
CIP-002-3 **CIP-002-3b**	**B. Requirements** **R1.** Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets. **R1.1.** The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria. **R1.2.** The risk-based assessment shall consider the following assets: **R1.2.6.** Special Protection Systems that support the reliable operation of the Bulk Electric System.
CIP-002-5.1	**4. Applicability:** **4.1.2.** Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES: **4.1.2.2.** Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.
	B. Requirements and Measures **R1.** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: [*Violation Risk Factor: High][Time Horizon: Operations Planning*] **v.** Special Protection Systems that support the reliable operation of the Bulk Electric System;…
	Attachment 1: Impact Rating Criteria **2. Medium Impact Rating (M)** **2.9.** Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.
	3. Low Impact Rating (L) **3.5.** Special Protection Systems that support the reliable operation of the Bulk Electric System.

<table>
<tr><th>Standard No.</th><th>Existing Standard Language</th></tr>
<tr><td>CIP-003-5
CIP-004-5.1
CIP-005-5
CIP-006-5
CIP-007-5
CIP-008-5
CIP-009-5
CIP-010-1
CIP-011-1</td><td>(All standards)

4. Applicability:
4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.</td></tr>
<tr><td>EOP-004-2</td><td>Attachment 1: Reportable Events
<table><tr><td>BES Emergency resulting in automatic firm load shedding</td><td>DP, TOP</td><td>Automatic firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS).</td></tr></table></td></tr>
<tr><td rowspan="2">FAC-010-2.1</td><td>B. Requirements

R3. The Planning Authority’s methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:

R3.4. Allowed uses of Special Protection Systems or Remedial Action Plans.</td></tr>
<tr><td>E. Regional Differences

1.1. As governed by the requirements of R2.5 and R2.6, starting with all Facilities in service,
shall require the evaluation of the following multiple Facility Contingencies when establishing SOLs:
1.1.4 The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.</td></tr>
<tr><td rowspan="2">FAC-011-2</td><td>B. Requirements

R3. The Reliability Coordinator’s methodology for determining SOLs, shall include, as a minimum, a description of the following, along with any reliability margins applied for each:

R3.5. Allowed uses of Special Protection Systems or Remedial Action Plans.</td></tr>
<tr><td>E. Regional Differences

1.1. As governed by the requirements of R3.3, starting with all Facilities in service, shall
require the evaluation of the following multiple Facility Contingencies when establishing
SOLs:
1.1.4 The failure of a circuit breaker associated with a Special Protection System to operate when required following: the loss of any element without a Fault; or a</td></tr>
</table>

Standard No.	Existing Standard Language
	permanent phase to ground Fault, with Normal Clearing, on any transmission circuit, transformer or bus section.
IRO-005-3.1a	**B. Requirements:** **R1.** Each Reliability Coordinator shall monitor its Reliability Coordinator Area parameters, including but not limited to the following: **R1.1.** Current status of Bulk Electric System elements (transmission or generation including critical auxiliaries such as Automatic Voltage Regulators and Special Protection Systems) and system loading.
	R9. Whenever a Special Protection System that may have an inter-Balancing Authority, or inter-Transmission Operator impact (e.g., could potentially affect transmission flows resulting in a SOL or IROL violation) is armed, the Reliability Coordinators shall be aware of the impact of the operation of that Special Protection System on inter-area flows. The Transmission Operator shall immediately inform the Reliability Coordinator of the status of the Special Protection System including any degradation or potential failure to operate as expected.
IRO-014-1	**B. Requirements** **R1.** The Reliability Coordinator shall have Operating Procedures, Processes, or Plans in place for activities that require notification, exchange of information or coordination of actions with one or more other Reliability Coordinators to support Interconnection reliability. These Operating Procedures, Processes, or Plans shall address Scenarios that affect other Reliability Coordinator Areas as well as those developed in coordination with other Reliability Coordinators. **R1.1.** These Operating Procedures, Processes, or Plans shall collectively address, as a minimum, the following: **R1.1.1.** Communications and notifications, including the conditions **[FN1]** under which one Reliability Coordinator notifies other Reliability Coordinators; the process to follow in making those notifications; and the data and information to be exchanged with other Reliability Coordinators. **[FN1]:** Examples of conditions when one Reliability Coordinator may need to notify another Reliability Coordinator may include (but aren't limited to) sabotage events, Interconnection Reliability Operating Limit violations, voltage reductions, insufficient resources, arming of special protection systems, etc.
MOD-029-1a	**B. Requirements** **R1.1.8.** Uses Special Protection System (SPS) models where currently existing or projected for implementation within the studied time horizon.
	R2.2. Where it is impossible to actually simulate a reliability-limited flow in a direction counter to prevailing flows (on an alternating current Transmission line), set the TTC for the non-prevailing direction equal to the TTC in the prevailing direction. If the TTC in the prevailing flow direction is dependent on a Special Protection System (SPS), set the TTC for the non-prevailing flow direction equal to the greater of the maximum

Standard No.	Existing Standard Language
	flow that can be simulated in the non-prevailing flow direction or the maximum TTC that can be achieved in the prevailing flow direction without use of a SPS.
MOD-030-02	**B. Requirements** **R2.1.1.1.** Use first Contingency criteria consistent with those first Contingency criteria used in planning of operations for the applicable time periods, including use of Special Protection Systems.
	R2.1.2.1. Use first Contingency criteria consistent with those first Contingency criteria used in planning of operations for the applicable time periods, including use of Special Protection Systems.
NUC-001-2.1	**B. Requirements** **R9.** The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2: **R9.3.7.** Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.
PRC-001-1.1	**B. Requirements** **R6.** Each Transmission Operator and Balancing Authority shall monitor the status of each Special Protection System in their area, and shall notify affected Transmission Operators and Balancing Authorities of each change in status.
WECC Regional Standard PRC-004-WECC-1	**A. Introduction** **1. Title:** Protection System and Remedial Action Scheme Misoperation **2. Number:** PRC-004-WECC-1 **3. Purpose:** Regional Reliability Standard to ensure all transmission and generation Protection System and Remedial Action Scheme (RAS) Misoperations on Transmission Paths and RAS defined in section 4 are analyzed and/or mitigated. **4. Applicability** **4.1.**Transmission Owners of selected WECC major transmission path facilities and RAS listed in tables titled "Major WECC Transfer Paths in the Bulk Electric System" provided at http://www.wecc.biz/Standards/Approved%20Standards/Supporting%20Tables/Table%20Major%20Paths%204-28-08.pdf and "Major WECC Remedial Action Schemes (RAS)" provided at http://www.wecc.biz/Standards/Approved%20Standards/Supporting%20Tables/Table%20Major%20RAS%204-28-08.pdf. **4.2.**Generator Owners that own RAS listed in the Table titled "Major WECC Remedial Action Schemes (RAS)" provided at http://www.wecc.biz/Standards/Approved%20Standards/Supporting%20Tables/Table%20Major%20RAS%204-28-08.pdf. **4.3.**Transmission Operators that operate major transmission path facilities and RAS listed in Tables titled "Major WECC Transfer Paths in the Bulk Electric System" provided at

Standard No.	Existing Standard Language
	http://www.wecc.biz/Standards/Approved%20Standards/Supporting%20Tables/Table%20Major%20Paths%204-28-08.pdf and "Major WECC Remedial Action Schemes (RAS)" provided at http://www.wecc.biz/Standards/Approved%20Standards/Supporting%20Tables/Table%20Major%20RAS%204-28-08.pdf.
	B. Requirements The requirements below only apply to the major transmission paths facilities and RAS listed in the tables titled "Major WECC Transfer Paths in the Bulk Electric System" and "Major WECC Remedial Action Schemes (RAS)." **R.1.** System Operators and System Protection personnel of the Transmission Owners and Generator Owners shall analyze all Protection System and RAS operations. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment]* **R1.1.** System Operators shall review all tripping of transmission elements and RAS operations to identify apparent Misoperations within 24 hours. **R1.2.** System Protection personnel shall analyze all operations of Protection Systems and RAS within 20 business days for correctness to characterize whether a Misoperation has occurred that may not have been identified by System Operators. **R.2.** Transmission Owners and Generator Owners shall perform the following actions for each Misoperation of the Protection System or RAS. It is not intended that Requirements R2.1 through R2.4 apply to Protection System and/or RAS actions that appear to be entirely reasonable and correct at the time of occurrence and associated system performance is fully compliant with NERC Reliability Standards. If the Transmission Owner or Generator Owner later finds the Protection System or RAS operation to be incorrect through System Protection personnel analysis, the requirements of R2.1 through R2.4 become applicable at the time the Transmission Owner or Generator Owner identifies the Misoperation: **R2.1.** If the Protection System or RAS has a Security-Based Misoperation and two or more Functionally Equivalent Protection Systems (FEPS) or Functionally Equivalent RAS (FERAS) remain in service to ensure Bulk Electric System (BES) reliability, the Transmission Owners or Generator Owners shall remove from service the Protection System or RAS that misoperated within 22 hours following identification of the Misoperation. Repair or replacement of the failed Protection System or RAS is at the Transmission Owners' and Generator Owners' discretion. **R2.2.** If the Protection System or RAS has a Security-Based Misoperation and only one FEPS or FERAS remains in service to ensure BES reliability, the Transmission Owner or Generator Owner shall perform the following. **R2.2.1.** Following identification of the Protection System or RAS Misoperation, Transmission Owners and Generator Owners shall remove from service within 22 hours for repair or modification the Protection System or RAS that misoperated.

Standard No.	Existing Standard Language
	R2.2.2. The Transmission Owner or Generator Owner shall repair or replace any Protection System or RAS that misoperated with a FEPS or FERAS within 20 business days of the date of removal. The Transmission Owner or Generator Owner shall remove the Element from service or disable the RAS if repair or replacement is not completed within 20 business days. **R2.3.** If the Protection System or RAS has a Security-Based or Dependability-Based Misoperation and a FEPS and FERAS is not in service to ensure BES reliability, Transmission Owners or Generator Owners shall repair and place back in service within 22 hours the Protection System or RAS that misoperated. If this cannot be done, then Transmission Owners and Generator Owners shall perform the following. **R2.3.1.** When a FEPS is not available, the Transmission Owners shall remove the associated Element from service. **R2.3.2.** When FERAS is not available, then **2.3.2.1.** The Generator Owners shall adjust generation to a reliable operating level, or **2.3.2.2.** Transmission Operators shall adjust the SOL and operate the facilities within established limits. **R2.4.** If the Protection System or RAS has a Dependability-Based Misoperation but has one or more FEPS or FERAS that operated correctly, the associated Element or transmission path may remain in service without removing from service the Protection System or RAS that failed, provided one of the following is performed. **R2.4.1.** Transmission Owners or Generator Owners shall repair or replace any Protection System or RAS that misoperated with FEPS and FERAS within 20 business days of the date of the Misoperation identification, or **R2.4.2.** Transmission Owners or Generator Owners shall remove from service the associated Element or RAS. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment]* **R.3.** Transmission Owners and Generation Owners shall submit Misoperation incident reports to WECC within 10 business days for the following. **R3.1.** Identification of a Misoperation of a Protection System and/or RAS, **R3.2.** Completion of repairs or the replacement of Protection System and/or RAS that misoperated.
PRC-005-2	**4. Applicability:** **4.2.4** Protection Systems installed as a Special Protection System (SPS) for BES reliability.
PRC-005-2 Table 1-4(a) header	Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).
PRC-005-2 Table 1-4(b) header	Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).

Standard No.	Existing Standard Language
PRC-005-2 Table 1-4(c) header	Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).
PRC-005-2 Table 1-4(d) header	Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).
PRC-005-2 Table 1-4(e) header and Component Attributes	Component Type - Protection System Station dc Supply for non-BES Interrupting Devices for SPS, non-distributed UFLS, and nondistributed UVLS systems Component Attributes: Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a SPS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).
PRC-005-2 Table 1-5 header and Component Attributes and Maintenance Activities	Component Type - Control Circuitry Associated With Protective Functions Note: Table requirements apply to all Control Circuitry Components of Protection Systems, and SPSs except as noted. Component Attributes: Unmonitored control circuitry associated with SPS. Maintenance Activities: Verify all paths of the control circuits essential for proper operation of the SPS. Component Attributes: Control circuitry associated with protective functions and/or SPS whose integrity is monitored and alarmed (See Table 2).
PRC-005-3	**4. Applicability:** **4.2.4** Protection Systems installed as a Special Protection System (SPS) for BES reliability. **4.2.6.3** Automatic Reclosing applied as an integral part of an SPS specified in Section 4.2.4.
PRC-005-3 Table 1-4(a) header	Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).
PRC-005-3 Table 1-4(b) header	Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).
PRC-005-3 Table 1-4(c) header	Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).
PRC-005-3 Table 1-4(d)	Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).
PRC-005-3 Table 1-4(e)	Component Type - Protection System Station dc Supply for non-BES Interrupting Devices for SPS, non-distributed UFLS, and non-distributed UVLS systems. Component Attributes: Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a SPS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).
PRC-005-3 Table 1-5 header and Component Attributes and	Note: Table requirements apply to all Control Circuitry Components of Protection Systems, and SPSs except as noted. Component Attributes: Unmonitored control circuitry associated with SPS (See Table 4-2(b) for SPS which include Automatic Reclosing.)

Standard No.	Existing Standard Language
Maintenance Activities	Maintenance Activities: Verify all paths of the control circuits essential for proper operation of the SPS Component Attributes: Control circuitry associated with protective functions and/or SPS whose integrity is monitored and alarmed (See Table 2).
PRC-005-3 Table 4-2(a) header and Component Attributes	Component Type - Control Circuitry Associated with Reclosing Relays that are NOT an Integral Part of an SPS Component Attributes: Unmonitored Control circuitry associated with Automatic Reclosing that is not an integral part of an SPS Component Attributes: Control circuitry associated with Automatic Reclosing that is not part of an SPS and is monitored and alarmed for conditions that would result in a premature closing command. (See Table 2)
PRC-005-3 Table 4-2(b) header and Component Attributes and Maintenance Activities	Component Type - Control Circuitry Associated with Reclosing Relays that ARE an Integral Part of an SPS Component Attributes: Close coils or actuators of circuit breakers or similar devices that are used in conjunction with Automatic Reclosing as part of an SPS (regardless of any monitoring of the control circuitry). Component Attributes: Unmonitored close control circuitry associated with Automatic Reclosing used as an integral part of an SPS. Maintenance Activities: Verify all paths of the control circuits associated with Automatic Reclosing that are essential for proper operation of the SPS. Component Attributes: Control circuitry associated with Automatic Reclosing that is an integral part of an SPS whose integrity is monitored and alarmed. (See Table 2)
PRC-006-1	**B. Requirements** **R. 2.2.** Any portions of the BES designed to detach from the Interconnection (planned islands) as a result of the operation of a relay scheme or Special Protection System, and
	E.B. Regional Variance for the Western Electricity Coordinating Council **E.B.2.2.** Any portions of the BES designed to detach from the Interconnection (planned islands) as a result of the operation of a relay scheme or Special Protection System.
PRC-012-0	**A. Introduction** **1.** Title: Special Protection System Review Procedure **3.** Purpose: To ensure that all Special Protection Systems (SPS) are properly designed, meet performance requirements, and are coordinated with other protection systems. To ensure that maintenance and testing programs are developed and misoperations are analyzed and corrected.

Standard No.	Existing Standard Language
	B. Requirements **R1.** Each Regional Reliability Organization with a Transmission Owner, Generator Owner, or Distribution Providers that uses or is planning to use an SPS shall have a documented Regional Reliability Organization SPS review procedure to ensure that SPSs comply with Regional criteria and NERC Reliability Standards. The Regional SPS review procedure shall include: **R1.1.** Description of the process for submitting a proposed SPS for Regional Reliability Organization review. **R1.2.** Requirements to provide data that describes design, operation, and modeling of an SPS. **R1.3.** Requirements to demonstrate that the SPS shall be designed so that a single SPS component failure, when the SPS was intended to operate, does not prevent the interconnected transmission system from meeting the performance requirements defined in Reliability Standards TPL-001-0, TPL-002-0, and TPL-003-0. **R1.4.** Requirements to demonstrate that the inadvertent operation of an SPS shall meet the same performance requirement (TPL-001-0, TPL-002-0, and TPL-003-0) as that required of the contingency for which it was designed, and not exceed TPL-003-0. **R1.5.** Requirements to demonstrate the proposed SPS will coordinate with other protection and control systems and applicable Regional Reliability Organization Emergency procedures. **R1.7.** Requirements for analysis and documentation of corrective action plans for all SPS misoperations. **R2.** The Regional Reliability Organization shall provide affected Regional Reliability Organizations and NERC with documentation of its SPS review procedure on request (within 30 calendar days).

Standard No.	Existing Standard Language
PRC-013-0	**A. Introduction** **1. Title:** Special Protection System Database. **3. Purpose:** To ensure that all Special Protection Systems (SPSs) are properly designed, meet performance requirements, and are coordinated with other protection systems. **B. Requirements** **R1.** The Regional Reliability Organization that has a Transmission Owner, Generator Owner, or Distribution Provider with an SPS installed shall maintain an SPS database. The database shall include the following types of information: **R1.1.** Design Objectives — Contingencies and system conditions for which the SPS was designed, **R1.2.** Operation — The actions taken by the SPS in response to Disturbance conditions, and **R1.3.** Modeling — Information on detection logic or relay settings that control operation of the SPS.
PRC-014-0	**A. Introduction** **1. Title:** Special Protection System Assessment **3. Purpose:** To ensure that all Special Protection Systems (SPS) are properly designed, meet performance requirements, and are coordinated with other protection systems. To ensure that maintenance and testing programs are developed and misoperations are analyzed and corrected. **B. Requirements** **R1.** The Regional Reliability Organization shall assess the operation, coordination, and effectiveness of all SPSs installed in its Region at least once every five years for compliance with NERC Reliability Standards and Regional criteria **R2.** The Regional Reliability Organization shall provide either a summary report or a detailed report of its assessment of the operation, coordination, and effectiveness of all SPSs installed in its Region to affected Regional Reliability Organizations or NERC on request (within 30 calendar days). **R3.** The documentation of the Regional Reliability Organization's SPS assessment shall include the following elements: **R3.3.** Identification of SPSs that were found not to comply with NERC standards and Regional Reliability Organization criteria. **R3.4**. Discussion of any coordination problems found between a SPS and other protection and control systems. **R3.5**. Provide corrective action plans for non-compliant SPSs.

Standard No.	Existing Standard Language
PRC-015-0	**A. Introduction** **1. Title:** Special Protection System Data and Documentation **3. Purpose:** To ensure that all Special Protection Systems (SPS) are properly designed, meet performance requirements, and are coordinated with other protection systems. To ensure that maintenance and testing programs are developed and misoperations are analyzed and corrected. **4. Applicability:** **4.1.** Transmission Owner that owns an SPS **4.2.** Generator Owner that owns an SPS **4.3.** Distribution Provider that owns an SPS **B. Requirements** **R1.** The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall maintain a list of and provide data for existing and proposed SPSs as specified in Reliability Standard PRC-013-0_R1. **R2.** The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have evidence it reviewed new or functionally modified SPSs in accordance with the Regional Reliability Organization's procedures as defined in Reliability Standard PRC-012-0_R1 prior to being placed in service. **R3.** The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of SPS data and the results of Studies that show compliance of new or functionally modified SPSs with NERC Reliability Standards and Regional Reliability Organization criteria to affected Regional Reliability Organizations and NERC on request (within 30 calendar days).

Standard No.	Existing Standard Language
PRC-016-0.1	**A. Introduction** **1.** Title: Special Protection System Misoperations **3.** Purpose: To ensure that all Special Protection Systems (SPS) are properly designed, meet performance requirements, and are coordinated with other protection systems. To ensure that maintenance and testing programs are developed and misoperations are analyzed and corrected. **4. Applicability:** **4.1.** Transmission Owner that owns an SPS **4.2.** Generator Owner that owns an SPS **4.3.** Distribution Provider that owns an SPS **B. Requirements** **R1.** The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall analyze its SPS operations and maintain a record of all misoperations in accordance with the Regional SPS review procedure specified in Reliability Standard PRC-012-0_R1. **R2.** The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall take corrective actions to avoid future misoperations. **R3.** The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the misoperation analyses and the corrective action plans to its Regional Reliability Organization and NERC on request (within 90 calendar days).

Standard No.	Existing Standard Language
PRC-017-0	**A. Introduction** **1. Title:** Special Protection System Maintenance and Testing **3. Purpose:** To ensure that all Special Protection Systems (SPS) are properly designed, meet performance requirements, and are coordinated with other protection systems. To ensure that maintenance and testing programs are developed and misoperations are analyzed and corrected. **4. Applicability:** **4.1.** Transmission Owner that owns an SPS **4.2.** Generator Owner that owns an SPS **4.3.** Distribution Provider that owns an SPS **B. Requirements** **R1.** The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have a system maintenance and testing program(s) in place. The program(s) shall include: **R1.1.** SPS identification shall include but is not limited to: **R2.** The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the program and its implementation to the appropriate Regional Reliability Organizations and NERC on request (within 30 calendar days).
PRC-020-1	**B. Requirements** **R1.6.** Any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.
PRC-021-1	**B. Requirements** **R1.5.** Any other schemes that are part of or impact the UVLS programs such as related generation protection, islanding schemes, automatic load restoration schemes, UFLS and Special Protection Systems.
PRC-023-2 Attachment A	**2.** The following protection systems are excluded from requirements of this standard: **2.5.** Relay elements used only for Special Protection Systems applied and approved in accordance with NERC Reliability Standards PRC-012 through PRC-017.
PRC-023-3 Attachment A	**2.** The following protection systems are excluded from requirements of this standard: **2.5.** Relay elements used only for Special Protection Systems applied and approved in accordance with NERC Reliability Standards PRC-012 through PRC-017.
PRC-024-1	**B. Requirements** **R2.** Each Generator Owner that has generator voltage protective relaying activated to trip its applicable generating unit(s) shall set its protective relaying such that the generator voltage protective relaying does not trip the applicable generating unit(s) as a result of a voltage excursion (at the point of interconnection2) caused by an event on the transmission system

Standard No.	Existing Standard Language
	external to the generating plant that remains within the "no trip zone" of PRC-024 Attachment 2. If the Transmission Planner allows less stringent voltage relay settings than those required to meet PRC-024 Attachment 2, then the Generator Owner shall set its protective relaying within the voltage recovery characteristics of a location-specific Transmission Planner's study. Requirement R2 is subject to the following exceptions: • Generating unit(s) may trip in accordance with a Special Protection System (SPS) or Remedial Action Scheme (RAS).
PRC-025-1 Attachment 1	**Relay Settings:** **Exclusions:** The following protection systems are excluded from the requirements of this standard: **5**. Protective relay elements used only for Special Protection Systems that are subject to one or more requirements in a NERC or Regional Reliability Standard.
TOP-005-2a Attachment 1	**Electric System Reliability Data** This Attachment lists the types of data that Balancing Authorities, and Transmission Operators are expected to share with other Balancing Authorities and Transmission Operators. **2.6.** New or degraded Special Protection Systems.
TPL-001-0.1 Category D	**Table 1. Transmission System Standards - Normal and Emergency Conditions** **12.** Failure of a fully redundant Special Protection System (or remedial action scheme) to operate when required **13.** Operation, partial operation, or misoperation of a fully redundant Special Protection System (or Remedial Action Scheme) in response to an event or abnormal system condition for which it was not intended to operate
TPL-001-4	**B. Requirements** **2.7.1.** List System deficiencies and the associated actions needed to achieve required System performance. Examples of such actions include: • Installation, modification, or removal of Protection Systems or Special Protection Systems **4.1.1.** For planning event P1: No generating unit shall pull out of synchronism. A generator being disconnected from the System by fault clearing action or by a Special Protection System is not considered pulling out of synchronism.
TPL-002-0b Category D	**Table I. Transmission System Standards — Normal and Emergency Conditions** **12.** Failure of a fully redundant Special Protection System (or remedial action scheme) to operate when required **13.** Operation, partial operation, or misoperation of a fully redundant Special Protection System (or Remedial Action Scheme) in response to an event or abnormal system condition for which it was not intended to operate

Standard No.	Existing Standard Language
TPL-003-0b Category D	**Table I. Transmission System Standards — Normal and Emergency Conditions** **12.** Failure of a fully redundant Special Protection System (or remedial action scheme) to operate when required **13.** Operation, partial operation, or misoperation of a fully redundant Special Protection System (or Remedial Action Scheme) in response to an event or abnormal system condition for which it was not intended to operate
TPL-004-0a Category D	**Table I. Transmission System Standards — Normal and Emergency Conditions** **12.** Failure of a fully redundant Special Protection System (or remedial action scheme) to operate when required **13.** Operation, partial operation, or misoperation of a fully redundant Special Protection System (or Remedial Action Scheme) in response to an event or abnormal system condition for which it was not intended to operate
WECC Regional Glossary Term:	**Definition: Dependability-Based Misoperation** Is the absence of a Protection System or RAS operation when intended. Dependability is a component of reliability and is the measure of a device's certainty to operate when required.
WECC Regional Glossary Term:	**Definition: Functionally Equivalent RAS (FERAS)** A Remedial Action Scheme ("RAS") that provides the same performance as follows: • Each RAS can detect the same conditions and provide mitigation to comply with all Reliability Standards. • Each RAS may have different components and operating characteristics
WECC Regional Glossary Term:	**Definition: Security-Based Misoperation** A Misoperation caused by the incorrect operation of a Protection System or RAS. Security is a component of reliability and is the measure of a device's certainty not to operate falsely.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Item 6
Attachment E

"Remedial Action Scheme" Definition Development

Background and Frequently Asked Questions

Project 2010-05.2 – Special Protection Systems

June 2014

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction 1
Background – RAS Definition Development 2
Existing NERC Glossary of Terms Definitions 2
Revision of the NERC Glossary of Terms Definition 2
Proposed Definition of RAS 3
Exclusion List Explanations 4
Explanations Regarding Changes from the Exclusion List Cited in the SAMS-SPCS Report 6
Frequently Asked Questions 6
Coordination with Project 2008-02 – Undervoltage Load Shedding 7
Attachment A – SDT Members 8

Introduction

The Project 2010-05.2 – Special Protection Systems Standard Drafting Team (SDT) thanks all commenters who submitted comments on the proposed revision to the NERC Glossary term "Special Protection System" ("SPS") or "Remedial Action Scheme" ("RAS") definition from the SAMS-SCPS SPS Technical Reference report. The revised definition was posted for a 30-day informal comment period from March 11, 2014 through April 9, 2014. NERC asked stakeholders to provide feedback on the proposed definition through a special electronic comment form.

The SDT appreciates the stakeholder comments on the revised definition. The SDT reviewed all of the comments and made numerous changes to the definition based on the feedback received. These changes are reflected in the first formal posting of the proposed revised definition for comment and ballot. The SDT developed this background and Frequently Asked Questions (FAQ) document to explain the key concepts incorporated in the revised definition, as well as the team's approach and intent.

Contact the Standards Developer, Al McMeekin, at 404-446-9675 or at al.mcmeekin@nerc.net with any comments or questions.

Background – RAS Definition Development

Existing NERC Glossary of Terms Definitions

The existing NERC Glossary of Terms defines **SPS** or **RAS** as: "An automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability. Such action may include changes in demand, generation (MW and Mvar), or system configuration to maintain system stability, acceptable voltage, or power flows. An SPS does not include (a) underfrequency or undervoltage load shedding or (b) fault conditions that must be isolated or (c) out-of-step relaying (not designed as an integral part of an SPS). Also called Remedial Action Scheme."

The NERC Glossary of Terms defines a **Protection System** as:

- Protective relays which respond to electrical quantities,
- Communications systems necessary for correct operation of protective functions,
- Voltage and current sensing devices providing inputs to protective relays,
- Station dc supply associated with protective functions (including batteries, battery chargers, and non-battery-based dc supply), and
- Control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.

Revision of the NERC Glossary of Terms Definition

Purpose of Revision of the NERC Glossary Terms SPS or RAS

The existing NERC Glossary of Terms definition for an SPS or RAS lacks the clarity and specificity necessary to consistently identify what equipment or schemes qualify as an SPS or RAS across the eight NERC Regions. This confusion leads to inconsistent application of the SPS or RAS-related NERC Reliability Standards.

The existing definition also lacks clarity in the actions stipulated as characteristics of an SPS or RAS. The actions listed in the definition are so broad that the definition may unintentionally include schemes whose purpose is not expressly related to preserving system reliability in response to predetermined system conditions. Inclusion of any scheme taking "corrective action other than isolation of faulted components to maintain system reliability" could be interpreted to mean that devices such as voltage regulators and switching controls for shunt capacitors should be included. This inclusion would then make these devices subject to requirements such as those addressing single-component failure considerations (sometimes referred to as redundancy considerations) in the SPS or RAS-related NERC Reliability Standards.

Recommendation to Change the Term to RAS Only

Currently, both terms, SPS and RAS, are used in the eight NERC Regions. The SDT contends that a single term promotes consistency. The SDT therefore recommends that the term RAS be retained as the industry-recognized term and that the term SPS be retired. The term RAS is more descriptive of the purpose for which the scheme is installed.

The term RAS also eliminates the confusion associated with the two defined terms, "Special Protection System" and "Protection System." The inclusion of Protection System in the term Special Protection System implies that SPS are a subset of Protection Systems. RAS are not Protection Systems; however, they may share components with Protection Systems.

Effects of Using Only the Term RAS in the Existing NERC Reliability Standards

The existing NERC Reliability Standards and NERC Glossary of Terms use the terms, SPS and RAS interchangeably. In most cases, both terms are included in the standards and written as: "SPS or RAS." The SDT evaluated the existing standards and recommended any necessary revisions to retain the single term, RAS. Many of the same changes would be required regardless of which single term is retained. A summary of the occurrences of the terms is included in the posted document *Uses of "Special Protection System" and "Remedial Action Scheme" in Reliability Standards.*

Proposed Definition of RAS

Remedial Action Scheme: A scheme designed to detect predetermined System conditions and automatically take corrective actions that may include, but are not limited to, curtailing or tripping generation or other sources, curtailing or tripping load, or reconfiguring a System(s). RAS accomplish one or more of the following objectives:

- Meet requirements identified in the NERC Reliability Standards;
- Maintain System stability;
- Maintain acceptable System voltages;
- Maintain acceptable power flows;
- Limit the impact of Cascading; or
- Address other Bulk Electric System (BES) reliability concerns.

These schemes are not Protection Systems; however, they may share components with Protection Systems.

The following do not individually constitute a RAS:

a. Out-of-step tripping and power swing blocking

b. Automatic underfrequency load shedding (UFLS) programs

c. Undervoltage Load Shedding Programs (UVLS Programs)

d. Autoreclosing schemes

e. Schemes applied on an Element for non-Fault conditions, such as, but not limited to, generator loss-of-field, transformer top-oil temperature, high voltage, or overload to protect the Element against damage by removing it from service

f. Controllers that switch or regulate series or shunt reactive devices, flexible alternating current transmission system (FACTS) devices, phase-shifting transformers, variable-frequency transformers, tap-changing transformers, or generation excitation, and that are located at and monitor quantities solely at the same station as the Element being switched or regulated

g. FACTS controllers that remotely switch static shunt reactive devices located at other stations to regulate the output of a single FACTS device

h. Schemes or controllers that remotely switch shunt reactors and shunt capacitors for voltage regulation that would otherwise be manually switched

i. Schemes that automatically de-energize a line for a non-Fault operation when one end of the line is open

j. Schemes that provide anti-islanding protection (e.g., protect load from effects of being isolated with generation that may not be capable of maintaining acceptable frequency and voltage)

k. Automatic sequences that proceed when manually initiated solely by an operator

l. Modulation of HVdc or FACTS via supplementary controls such as angle damping or frequency damping applied to damp local or inter-area oscillations

m. Sub-synchronous resonance (SSR) protection schemes that directly detect sub-synchronous quantities (e.g., currents or torsional oscillations)

Exclusion List Explanations

a. Out-of-step tripping and power swing blocking

The existing NERC Glossary of Terms definition of SPS or RAS excludes out-of-step relaying because it is a protective function. The SDT maintained the exclusion but changed the wording from "out-of-step relaying" to "out-of-step tripping and power swing blocking" to reflect current industry terminology.

b. Automatic underfrequency load shedding (UFLS) programs

The existing NERC Glossary of Terms definition of SPS or RAS excludes UFLS because it is a protective function that has unique design and implementation considerations that are covered by NERC Reliability Standard PRC-006-1. The SDT maintained the exclusion.

c. Undervoltage Load Shedding Programs (UVLS Programs)

The existing NERC Glossary of Terms definition of SPS or RAS excludes undervoltage load shedding (UVLS) because it is a protective function. The SDT maintained the exclusion but is using the new term UVLS Program proposed by the SDT for NERC Project 2008-02 – Undervoltage Load Shedding. UVLS Programs are addressed in proposed NERC Reliability Standard PRC-010-1.

d. Autoreclosing schemes

Autoreclosing schemes locally monitor and locally close interrupting devices to restore elements for the purpose of improving electric service availability. These schemes are deployed primarily as a convenience to supplement manual restoration activities. Autoreclosing is a common and understood industry function that has not previously been regarded as a RAS. The SDT accepts the exclusion consistent with industry practice.

e. Schemes applied on an Element for non-Fault conditions, such as, but not limited to, generator loss of field, transformer top-oil temperature, high voltage, or overload to protect the Element against damage by removing it from service

The SDT contends that these schemes are applied on an Element to protect it from damage. They are protective functions and are not RAS. The SDT accepts this exclusion consistent with industry practice.

f. Controllers that switch or regulate series or shunt reactive devices, FACTS devices, phase-shifting transformers, variable-frequency transformers, tap-changing transformers, or generation excitation, and that are located at and monitor quantities solely at the same station as the Element being switched or regulated

The SDT contends these devices are not RAS. The SDT accepts this exclusion consistent with industry practice.

g. FACTS controllers that remotely switch static shunt reactive devices located at other stations to regulate the output of a single FACTS device

The SDT contends these devices are not RAS. The SDT accepts this exclusion consistent with industry practice.

h. Schemes or controllers that remotely switch shunt reactors and shunt capacitors for voltage regulation that would otherwise be manually switched

Schemes or controllers that assist a System Operator in coordinating the switching of shunt reactors and shunt capacitors that would otherwise be manually switched are not remedial in the sense of being mitigations in response to predetermined System conditions, but are for general application to all System conditions.

i. Schemes that automatically de-energize a line for a non-Fault operation when one end of the line is open

When one end of a line is open, unacceptable voltage levels can occur. Opening the remote terminal(s) to de-energize the transmission line removes this voltage rise. These schemes have not historically been regarded as RAS, and the SDT accepts this exclusion consistent with industry practice.

j. Schemes that provide anti-islanding protection (e.g., protect load from effects of being isolated with generation that may not be capable of maintaining acceptable frequency and voltage)

These schemes are designed to protect load in an electrical island that might otherwise operate at an off-nominal frequency or voltage, or facilitate restoration. Actions taken on islanded facilities will not impact the interconnected BES because they are isolated. The SDT accepts this exclusion consistent with industry practice.

k. Automatic sequences that proceed when manually initiated solely by an operator

Automated sequences created to simplify the actions of an operator are not RAS because the decision to activate a specific sequence is left to the operator. If the automated sequence fails to execute correctly, the operator has the option to manually set those actions in motion. The SDT accepts this exclusion consistent with industry practice.

l. Modulation of HVdc or FACTS via supplementary controls such as angle damping or frequency damping applied to damp local or inter-area oscillations

Modulation of HVdc and FACTS via supplementary controls is occasionally used for damping local or inter-area oscillations. They perform a similar function as a Power System Stabilizer (PSS), which is a component of excitation controls in a generating unit. PSS are not classified as RAS. The SDT accepts this exclusion consistent with industry practice.

m. Sub-synchronous resonance (SSR) protection schemes that directly detect sub-synchronous quantities; (e.g., currents or torsional oscillations)

The SDT contends that directly detected SSR conditions and related mitigation are not RAS. The SDT accepts this exclusion consistent with industry practice.

Explanations Regarding Changes from the Exclusion List Cited in the SAMS-SPCS Report

The SDT revised the straw man definition proposed in the SAMS-SPCS report; however, the proposed definition is consistent with the SAMS-SPCS intent. The drafting team revised the definition in response to stakeholder comments from the informal posting. As a result, it is no longer necessary to explicitly state some of the exclusions.

1. **Schemes that prevent high line voltage by automatically switching the affected line**

   This scheme is now addressed by exceptions "e" (protection from high voltage) and "i" (automatic de-energization of a line when one end is open) in the proposed definition.

2. **Protection schemes that operate local breakers other than those on the faulted circuit to facilitate Fault clearing, such as, but not limited to, opening a circuit breaker to remove infeed so protection at a remote terminal can detect a Fault or to reduce fault duty**

   The scheme described in this exclusion is a Protection System. The proposed definition excludes Protection Systems from RAS.

3. **Blanket exclusion for SSR protection schemes**

   The proposed definition excludes schemes that directly detect sub-synchronous quantities; however, SSR mitigation schemes installed to detect distinct System configurations and loading conditions (that studies have shown may make a generator vulnerable to SSR), and take action to trip the generator or bypass the series capacitor, are classified as RAS.

4. **A Protection System that includes multiple elements within its zone of protection, or that isolates more than the faulted element because an interrupting device is not provided between the faulted element and one or more other elements**

   The scheme described in this exclusion is a Protection System. The proposed definition excludes Protection Systems from RAS.

Frequently Asked Questions

Why does the proposed definition have an exclusion list?

The definition must be broad enough to include the variety of System conditions monitored and corrective actions taken by RAS. Without the exclusions, equipment and schemes that should not be considered RAS could be subject to the requirements of the RAS-related NERC Reliability Standards. The exclusion list also assures that commonly applied protection and control systems are not unintentionally included as RAS.

Why did the SDT not propose a screening process to identify RAS?

The SDT contends that a comprehensive definition with specific exclusions is the best way to achieve consistency and immediacy in RAS identification. The SDT asserts that a study-based screening process would be labor-intensive and dependent on assumptions that could vary among the entities performing the studies.

Why does the proposed definition not include the classification types suggested in the SPCS-SAMS report?

The classification of a RAS is not necessary for defining whether or not a scheme qualifies as a RAS. Informal feedback from many stakeholders indicated uncertainty about the classification types. Therefore, the SDT decided not to include RAS classification types within the definition. The classifications are more appropriately addressed concurrently with revisions to the RAS-related Reliability Standards.

Why did the SDT not specifically reference the Transmission Planning (TPL) standards in the proposed definition?

The SDT acknowledges that many RAS are installed to address the performance requirements of the TPL standards; however, they are also installed to address other reliability concerns.

Would automatic actions taken by an Energy Management System (EMS), Supervisory Control and Data Acquisition (SCADA), or Distribution Control System (DCS) be considered a RAS?
The above-mentioned control systems support and enable grid operations by issuing control commands mostly to geographically distributed power System devices. In this normal application, these systems are not considered to be RAS. However, if these systems are configured to detect predetermined conditions and take corrective actions consistent with the RAS definition, these automatic functions would be considered RAS. The identification of RAS is not dependent upon the specific hardware or platform utilized in the scheme.

What are the Implementation Plan time frames?
The Implementation Plan provides RAS owners a minimum of twelve (12) months beyond the date of approval by a governmental authority to evaluate their current schemes for determining whether they are RAS, based on the new definition. The drafting team contends that twelve (12) months is an adequate period of time to review existing schemes to determine whether they are RAS.

The Implementation Plan also provides owners of newly identified RAS twenty-four (24) calendar months beyond the date of approval by a governmental authority to be fully compliant with all standards applicable to the revised definition of Remedial Action Scheme. The drafting team contends that twenty-four (24) calendar months provides the RAS owner sufficient time to become compliant with the revised standards proposed in the Implementation Plan.

Coordination with Project 2008-02 – Undervoltage Load Shedding

As part of the current development of PRC-010-1, the Project 2008-02 UVLS SDT is introducing a new NERC Glossary term, UVLS Program, to clearly establish applicability of PRC-010-1:

Undervoltage Load Shedding Program (UVLS Program): An automatic load shedding program consisting of distributed relays and controls used to mitigate undervoltage conditions leading to voltage instability, voltage collapse, or Cascading impacting the Bulk Electric System (BES). Centrally controlled undervoltage-based load shedding is not included.

Note that the definition excludes centrally controlled undervoltage-based load shedding. The UVLS SDT maintains that the design and characteristics of centrally controlled undervoltage-based load shedding are commensurate with RAS (wherein load shedding is the remedial action) and, as such, centrally controlled undervoltage-based load shedding should be subject to RAS-related Reliability Standards.

The Project 2010-05.2 SPS SDT agrees with the Project 2008-02 UVLS SDT that the design and characteristics of centrally controlled undervoltage-based load shedding are more appropriately categorized as RAS. The SPS SDT has therefore revised the definition of RAS to clarify that the definition is exclusive of only the newly defined term UVLS Program, and is therefore inclusive of centrally controlled undervoltage-based load shedding. The SDT is coordinating this change with the Project 2008-02 UVLS SDT. Collectively, the two definitions will promote consistency in the identification of centrally controlled undervoltage-based load shedding as a RAS. As a result, all NERC Reliability Standards that include the term RAS will be applicable to centrally controlled undervoltage-based load shedding upon the effective date of the revised definition of RAS.

Attachment A – SDT Members

Project 2010-05.2 – Special Protection Systems SDT		
	Participant	**Entity**
Chair	Gene Henneberg	NV Energy / Berkshire Hathaway Energy
Vice Chair	Bobby Jones	Southern Company
Member	Amos Ang	Southern California Edison
	John Ciufo	Hydro One Inc.
	Alan Engelmann	ComEd / Exelon
	Davis Erwin	Pacific Gas and Electric
	Sharma Kolluri	Entergy
	Charles-Eric Langlois	Hydro-Quebec TransEnergie
	Robert J. O'Keefe	American Electric Power
	Hari Singh	Xcel Energy
NERC Staff	Al McMeekin (Standards Developer)	NERC
	Erika Chanzes (Standards Developer)	NERC
	Phil Tatro (Technical Advisor)	NERC
	Bill Edwards (Legal Counsel)	NERC

Implementation Plan for the Revised Definition of "Remedial Action Scheme"

Project 2010-05.2 – Special Protection Systems

Background

The existing NERC Glossary of Terms definition for "Special Protection System" ("SPS") or "Remedial Action Scheme" ("RAS") lacks the specificity necessary to consistently identify what equipment or protection schemes qualify as SPS or RAS across the eight NERC Regions. The existing definition also does not clearly stipulate the characteristics of a SPS or RAS. The actions listed in the definition of SPS, which are incorporated by cross reference (NERC Glossary of Terms) into the definition of RAS, are ambiguous and may unintentionally include equipment whose purpose is not expressly related to preserving System reliability in response to predetermined System conditions. Employing a single term, i.e., RAS, and clarifying its definition will lead to more consistent application of the NERC Reliability Standards related to RAS.

The proposed definition of RAS must be broad to include the variety of System conditions monitored and corrective actions taken by RAS. This "broadness," however, necessitates an exclusion list because without the exclusions, equipment and schemes that should not be considered RAS could be subject to the requirements of the RAS-related Reliability Standards. The exclusion list assures that commonly applied protection and control systems are not unintentionally included as RAS.

The Project 2010-05.2 SPS SDT is coordinating the development of the RAS definition with the development of PRC-010-1 by the SDT for Project 2008-02 – Undervoltage Load Shedding. The UVLS SDT is introducing a new NERC Glossary term, UVLS Program, to clearly establish applicability of PRC-010-1. The proposed term UVLS Program is defined as: "An automatic load shedding program consisting of distributed relays and controls used to mitigate undervoltage conditions leading to voltage instability, voltage collapse, or Cascading impacting the Bulk Electric System (BES). Centrally controlled undervoltage-based load shedding is not included."

Note that the proposed definition excludes centrally controlled undervoltage-based load shedding. The UVLS SDT maintains that the design and characteristics of centrally controlled undervoltage-based load shedding are commensurate with RAS (wherein load shedding is the remedial action) and, as such, should be subject to RAS-related Reliability Standards. The Project 2010-05.2 SPS SDT agrees with this assessment and revised the definition of RAS to clarify that it is inclusive of centrally controlled undervoltage-based load shedding. Collectively, the two definitions will promote consistency in the identification of centrally controlled undervoltage-based load shedding as RAS. The coordination of these revisions is required to maintain coverage of those systems and prevent a reliability gap. As a result of these revisions, all NERC Reliability Standards that include the term RAS will be applicable to centrally

controlled undervoltage-based load shedding upon the effective dates of the revised definitions of RAS and UVLS Program.

Requested Approvals

Definition of "**Remedial Action Scheme**" and the standards listed below

The following standards are proposed for approval to align the use of RAS. This list is intended to reflect Reliability Standards currently in effect at the time of Project development. In certain cases, a standard listed below for approval may already be retired pursuant to an implementation plan of a successor version by the time the definition of "Remedial Action Scheme" becomes effective in a particular jurisdiction. In these cases, the standard below will not become effective.

> The standard numbers below currently include an (X) to indicate the version numbering will be updated. Some standards are open in current projects and others are pending with governmental authorities. As a result, NERC will assign the appropriate version number prior to BOT adoption.

CIP-002-3(X)
CIP-002-3b(X)
CIP-002-5.1(X)
CIP-003-5(X)
CIP-004-5.1(X)
CIP-005-5(X)
CIP-006-5(X)
CIP-007-5(X)
CIP-008-5(X)
CIP-009-5(X)
CIP-010-1(X)
CIP-011-1(X)
EOP-004-2(X)
FAC-010-2.1(X)
FAC-011-2(X)
IRO-005-3.1a(X)
IRO-014-1(X)
MOD-029-1a(X)
MOD-030-2(X)
NUC-001-2.1(X)
PRC-001-1.1(X)
PRC-004-WECC-1(X)
PRC-005-2(X)
PRC-005-3(X)
PRC-006-1(X)
PRC-012-0(X)
PRC-013-0(X)
PRC-014-0(X)
PRC-015-0(X)
PRC-016-0.1(X)
PRC-017-0(X)
PRC-020-1(X)
PRC-021-1(X)
PRC-023-2(X)
PRC-023-3(X)
PRC-024-1(X)
PRC-025-1(X)
TOP-005-2a(X)
TPL-001-0.1(X)
TPL-001-4(X)
TPL-002-0b(X)
TPL-003-0b(X)
TPL-004-0a(X)

Requested Retirements

Definition of "**Special Protection System**" and the standards listed below

CIP-002-3
CIP-002-3b
CIP-002-5.1
CIP-003-5
CIP-004-5.1
CIP-005-5
CIP-006-5
CIP-007-5
CIP-008-5
CIP-009-5
CIP-010-1
CIP-011-1
EOP-004-2
FAC-010-2.1
FAC-011-2
IRO-005-3.1a
IRO-014-1
MOD-029-1a
MOD-030-02
NUC-001-2.1
PRC-001-1.1

PRC-004-WECC-1	PRC-016-0.1	TOP-005-2a
PRC-005-2	PRC-017-0	TPL-001-0.1
PRC-005-3	PRC-020-1	TPL-001-4
PRC-006-1	PRC-021-1	TPL-002-0b
PRC-012-0	PRC-023-2	TPL-003-0b
PRC-013-0	PRC-023-3	TPL-004-0a
PRC-014-0	PRC-024-1	
PRC-015-0	PRC-025-1	

General Considerations

The entity shall modify its processes as necessary to account for the revised definition. The revised definition of RAS clarifies that it is inclusive of centrally controlled undervoltage-based load shedding. Entities may have additional changes to the classification of certain schemes to align them with the revised definition. This Implementation Plan provides additional time for entities with newly-identified RAS to become compliant with the Reliability Standards during the transition to the revised definition.

Prerequisite Approvals

NERC Reliability Standard PRC-010-1 – Undervoltage Load Shedding
Definition of "Undervoltage Load Shedding Program (UVLS Program)" in Project 2008-02 Undervoltage Load Shedding

Revisions to the NERC Glossary of Terms

The drafting team proposes the following revised definition:

Remedial Action Scheme (RAS)

A scheme designed to detect predetermined System conditions and automatically take corrective actions that may include, but are not limited to, curtailing or tripping generation or other sources, curtailing or tripping load, or reconfiguring a System(s). RAS accomplish one or more of the following objectives:

- Meet requirements identified in the NERC Reliability Standards;
- Maintain System stability;
- Maintain acceptable System voltages;
- Maintain acceptable power flows;
- Limit the impact of Cascading; or
- Address other Bulk Electric System (BES) reliability concerns.

These schemes are not Protection Systems; however, they may share components with Protection Systems.

The following do not individually constitute a RAS:

a. Out-of-step tripping and power swing blocking

b. Automatic underfrequency load shedding (UFLS) programs

c. Undervoltage Load Shedding Programs (UVLS Programs)

d. Autoreclosing schemes

e. Schemes applied on an Element for non-Fault conditions, such as, but not limited to, generator loss-of-field, transformer top-oil temperature, high voltage, or overload to protect the Element against damage by removing it from service

f. Controllers that switch or regulate series or shunt reactive devices, flexible alternating current transmission system (FACTS) devices, phase-shifting transformers, variable-frequency transformers, tap-changing transformers, or generation excitation, and that are located at and monitor quantities solely at the same station as the Element being switched or regulated

g. FACTS controllers that remotely switch static shunt reactive devices located at other stations to regulate the output of a single FACTS device

h. Schemes or controllers that remotely switch shunt reactors and shunt capacitors for voltage regulation that would otherwise be manually switched

i. Schemes that automatically de-energize a line for a non-Fault operation when one end of the line is open

j. Schemes that provide anti-islanding protection (e.g., protect load from effects of being isolated with generation that may not be capable of maintaining acceptable frequency and voltage)

k. Automatic sequences that proceed when manually initiated solely by an operator

l. Modulation of HVdc or FACTS via supplementary controls such as angle damping or frequency damping applied to damp local or inter-area oscillations

m. Sub-synchronous resonance (SSR) protection schemes that directly detect sub-synchronous quantities (e.g., currents or torsional oscillations)

Conforming Changes to Other Standards

The existing Reliability Standards proposed for retirement contain references to SPS or RAS or both. The revised Reliability Standards will reflect the use of the single term RAS. The revised Reliability Standards noted above for approval are included in a separate document *Revised Reliability Standards for the Revised Definition of "Remedial Action Scheme."*

Effective Date for Revised Reliability Standards and Definition

The revised Reliability Standards and the revised definition of "Remedial Action Scheme" shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date that the standards and definition are approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard and the definition shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date the standards and definition are adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Implementation Plan for Newly-Identified RAS

Entities with newly-identified RAS resulting from the application of the definition must be fully compliant with all Reliability Standards applicable to the revised definition of "Remedial Action Scheme" twenty-four (24) months from the Effective Date of the revised definition of "Remedial Action Scheme." This additional time applies only to existing schemes that must transition to RAS due to the revised definition. The additional time does not apply to future RAS that may be created following implementation of the revised definition.

Retirement of Existing Standards and Definitions

The requested Reliability Standards for retirement, the current definition of "Special Protection System," and the current definition of "Remedial Action Scheme" shall be retired at midnight of the day immediately prior to the Effective Date of the revised definition of "Remedial Action Scheme" in the particular jurisdiction in which the revised definition is becoming effective.

Project 2010-14.2 Periodic Review of BAL Standards

Action

- Accept the work of the BAL Periodic Review Team (PRT), as provided in these materials
- Accept the SAR prepared by the BAL PRT as superseding the original SAR; and authorize posting the SAR for informal comment
- Set a medium priority to Project 2010-14.2 based on the following factors: BAL-005-0.2b is a high RISC Standard family (BAL-006-2 not ranked); and the standards to be revised have outstanding regulatory directives and a number of P81 candidates, as well as Independent Experts content and quality issues.
- Appoint the BAL PRT as the standard drafting team for the new Project 2010-14.2 Implementation of BAL Periodic Review Recommendations.

Background

Project 2010-14 was approved by the NERC Standards Committee as a merger of Project 2007-05 Balancing Authority Controls and Project 2007-18 Reliability-based Control on July 28, 2010. The NERC Standards Committee also approved the separation of Project 2010-14 into two phases, moving Phase 1 into formal development on July 13, 2011. Subsequently, in June 2013, the Standards Committee approved retiring the previously-scoped Project 2010-14.2, which lacked sufficient focus for a drafting team to proceed, in order to allow a periodic review to take place first.

On October 17, 2013 the NERC Standards Committee appointed ten subject matter experts to serve on the BAL PRT. As part of its review, the BAL PRT referenced background documents, including 1) the currently-enforceable BAL-005-0.2b and BAL-006-2 standards; 2) outstanding issues and directives pertaining to the BAL-005-0.2b and BAL-006-2 standards; 3) the Independent Experts Report; and 4) Paragraph 81 criteria.

Based on this review, the BAL PRT developed a set of recommendations for revising BAL-005-0.2b and BAL-006-2. The BAL PRT recommendations for BAL-005-0.2b and BAL-006-2 were posted for a 45-day comment period from February 21, 2014 through April 7, 2014. There were 23 sets of comments, including comments from approximately 84 different people from approximately 62 companies, representing 8 of the 10 Industry Segments.

The BAL PRT carefully reviewed and considered the comments received during the posting period and, based on stakeholder comments, made revisions to its recommendations. To support implementation of these recommendations, the BAL PRT developed a new SAR intended to supersede the original SAR, which contains outdated information. To further support its recommendations, the BAL PRT developed redlined versions of the standards. Many improvements suggested by stakeholders during the comment period were incorporated into the final recommendations and redlined standards being provided to the Standards Committee.

The recommendations of the BAL PRT are in the attached Periodic Review Templates and SAR. The redlined standards are posted on the project page and will be included as part of the SAR for this project. Additional documents developed to support the team's recommendations have been posted on the project page, including 1) the BAL PRT's consideration of comments on the draft recommendation; 2) a list of directives and stakeholder-identified issues associated with the standards; and 3) the IERP recommendations associated with the standards, containing the BAL PRT's consideration of those recommendations.

This project addresses directives in Paragraphs 406[1], 415[2], 418[3], 419[4], 428 [5] and 438[6] of FERC Order 693, and provides additional clarity to many requirements, as well as retiring requirements that meet the criteria developed in the Paragraph 81 project.
Because the project will address outstanding FERC Order No. 693 directives, provide clarity to the requirements of the two standards, and apply Paragraph 81 criteria to ensure that all requirements in the two standards are necessary for reliability, the PRT considers this project to be medium priority.

Note that the BAL PRT has developed a separate recommendation for BAL-004, which is in the process of being finalized and will be posted for a 45-day stakeholder comment period following additional outreach to non-industry stakeholders. These non-industry stakeholders are potentially affected by the recommendation and NERC and the team want to ensure that the team considers the concerns of this unique group of stakeholders prior to posting a recommendation for stakeholder comment.

[1] "Given that most of the commenters' concerns over the inclusion of DSM as part of regulating reserves relate to the technical requirements, the Commission clarifies that to qualify as regulating reserves, these resources must be technically capable of providing the service. In particular, all resources providing regulation must be capable of automatically responding to real-time changes in load on an equivalent basis to the response of generation equipped with automatic generation control. From the examples provided above, the Commission understands that it may be technically possible for DSM to meet equivalent requirements as conventional generators and expects the Reliability Standards development process to provide the qualifications they must meet to participate. These qualifications will be reviewed by the Commission when the revised Reliability Standard is submitted to the Commission for approval."

[2] "Both Xcel and FirstEnergy question Requirement R17 but do not oppose the Commission's proposal to approve this Reliability Standard. Earlier in this Final Rule, we direct the ERO to consider the comments received to the NOPR in its Reliability Standards development process. Thus, the comments of Xcel and FirstEnergy should be addressed by the ERO when this Reliability Standard is revisited as part of the ERO's Work Plan."

[3] "The Commission adopts the NOPR proposal to require the ERO to modifiy the Reliability Standards to include a Measure that provides for a verification process over the minimum required automatic generation control or regulating reserves a balancing authority maintains."

[4] "FirstEnergy has a number of suggestions to improve the existing Reliability Standard and the ERO is directed to consider those suggestions in its Reliability Standards development process."

[5] "The Commission directs the ERO to develop a modification to BAL-006-1 that adds Measures concerning the accumulation of large inadvertent imbalances and Levels of Non-Compliance. . . [W]e are concerned that large imbalances represent dependence by some balancing authorities on their neighbors and are an indication of less than desirable balancing of generation with load. The Commission also notes that the stated purpose of this Reliability Standard is to define a process for monitoring balancing authorities to ensure that, over the long term, balancing authorities do not excessively depend on other balancing authorities in the Interconnection for meeting their demand or interchange obligations."

[6] "Since the ERO indicates that the reliability aspects of this issue will be addressed in a Reliability Standards filing later this year, the Commission asks the ERO, when filing the new Reliability Standard, to explain how the new Reliability Standard satisfies the Commission's concerns."

Periodic Review of BAL-005-0.2b – Automatic Generation Control and BAL-006-2 – Inadvertent Interchange (Recommendation to Revise both Standards)

~~April 25~~May 22~~0~~, 2014

Introduction

The North American Electric Reliability Corporation (NERC) is required to conduct a periodic review of each NERC Reliability Standard at least once every ten years, or once every five years for Reliability Standards approved by the American National Standards Institute as an American National Standard.[1] Project 2010-14.2 - Phase 2 of Balancing Authority Reliability-based Controls (BARC 2) was included in the current cycle of periodic reviews.

The NERC Standards Committee appointed ten industry subject matter experts to serve on the BARC 2 periodic review team (BARC 2 PRT) on September 19, 2013.[2] The BARC 2 PRT used background information on the standards and the questions set forth in the Periodic Review Template developed by NERC and approved by the Standards Committee, along with associated worksheets and reference documents, to determine whether BAL-005-0_2b and BAL-006-2 should be: (1) affirmed as is (i.e., no changes needed); (2) revised (which may include revising or retiring one or more requirements); or (3) withdrawn.

As a result of that examination, the BARC 2 PRT recommends to **REVISE** BAL-005-0_2b and BAL-006-2, and has therefore developed a draft Standard Authorization Request (SAR) outlining the proposed scope and technical justification for the revisions. **The purpose of all documents contained in this posting is to elicit feedback from industry on the BARC 2 PRT's recommendations.**

Applicable Reliability Standards: BAL-005-0.2b and BAL-006-2

Note: BAL-005-0 was filed for FERC approval on April 4, 2006 in Docket No. RM06-16-000 and was approved on March 16, 2007 in Order No. 693.6. Also, FERC accepted an errata filing to BAL-005-0.1b on September 13, 2012, which replaced Appendix 1 with a corrected version of a FERC-approved interpretation, and made an internal reference

[1] NERC Standard Processes Manual 45 (2013), posted at http://www.nerc.com/pa/Stand/Documents/Appendix_3A_StandardsProcessesManual.pdf.
[2] The Standards Committee subsequently appointed Scott Brooks of Manitoba Hydro to the BARC 2 PRT.

correction in the interpretation, thus resulting in BAL-005-0.2b. On March 16, 2007 FERC issued Order Number 693 approving Reliability Standard BAL-006-1. BAL-006-2, which removed the MISO waivers found in BAL-006-1, was approved by FERC on January 6, 2011 in Docket No. RD10-04-000.
Team Members (include name and organization): 1. Doug Hils, Duke Energy (Chair) 2. Thomas W. (Tom) Siegrist, Brickfield Burchette Ritts and Stone, PC (Vice Chair) 3. Scott Brooks, Manitoba Hydro 4. Ron Carlsen, Southern Company 5. Howard F. Illian, Energy Mark, Inc. 6. Mike Potishnak, Representing NPCC 7. Jerry Rust, Northwest Power Pool 8. Robert Staton, Xcel Energy 9. Glenn Stephens, Santee Cooper 10. Stephen Swan, MISO 11. Mark Trumble, Omaha Public Power District
Date Review Completed: February 14, 2014

Background Information *(initially completed by NERC staff)*

1. Are there any outstanding Federal Energy Regulatory Commission (FERC) directives associated with the Reliability Standards? (If so, NERC staff will attach a list of the directives with citations to associated FERC orders for inclusion in a SAR.)

   ☒ Yes

   ☐ No

   Please see the attached *Consideration of Issues and Directives*.

2. Have stakeholders requested clarity on the Reliability Standards in the form of an Interpretation (outstanding, in progress, or approved), Compliance Application Notice (CAN) (outstanding, in progress, or approved), or an outstanding submission to NERC's Issues Database? (If there are, NERC staff will include a list of the Interpretation(s), CAN(s), or stakeholder-identified issue(s) contained in the NERC Issues Database that apply to the Reliability Standard.)

   ☒ Yes (See BAL-005-0.2b, Appendix 1 - Interpretation of Requirement R17)

   ☐ No

3. Are the Reliability Standards one of the most violated Reliability Standards? If so, does the root cause of the frequent violation appear to be a lack of clarity in the language?

   ☐ Yes

   ☒ No

   Please explain:

4. Do the Reliability Standards need to be modified or converted to the results-based standard (RBS) format as outlined in *Attachment 1: Results-Based Standards*? Note that this analysis is twofold and requires collaboration among NERC staff and the Review Team. First, determine whether the *substance* of the Reliability Standard comports to the RBS principles described in Attachment 1. Second, ensure that, as Reliability Standards are reviewed, the *formatting* is changed as necessary to comply with the current format of a Reliability Standard. If the answer to either part of this question is "Yes," the standard should be revised.

   ☒ Yes

☐ No

Note: The BARC 2 PRT reviewed BAL-005-0.2b and BAL-006-2 and determined that many of the requirements were similar in nature and could be simplified to provide a clear and measurable expected outcome, such as: (1) a stated level of reliability performance; (2) a reduction in a specified reliability risk; or (3) a necessary competency.

Additional Questions Considered by the BARC 2 PRT

If NERC staff answered "Yes" to any of the questions above, the Reliability Standard probably requires revision. The questions below are intended to further guide your review. Some of the questions reference documents provided by NERC staff as indicated in the Background questions above.

1. **Paragraph 81**: Does one or more of the requirements in the Reliability Standard meet criteria for retirement or modification based on Paragraph 81 concepts? Use *Attachment 2: Paragraph 81 Criteria* to make this determination.

   ☒ Yes

   ☐ No

   Please summarize your application of Paragraph 81 Criteria, if any: The BARC 2 PRT applied the criteria specified in *Attachment 2: Paragraph 81 Criteria* in reviewing BAL-005 and BAL-006. As that document more fully explains, for a Reliability Standard requirement to be proposed for retirement or modification based on Paragraph 81 concepts, it must satisfy both an overarching criterion, specifically, whether the requirement does little, if anything, to benefit or protect the reliable operation of the Bulk Electric System (BES), and at least one other criterion specified therein. The PRT concluded that eight requirements should be retired under Paragraph 81 concepts as detailed in Table 1:

Table 1 - PRT Recommended Paragraph 81 Retirements

Requirement	Rationale
BAL-005, Requirement R4	The basis for coordination of common values between adjacent BAs is covered in Requirement R3, and correction of information not available has also been addressed. Therefore, this requirement is redundant and does little, if anything, to benefit or protect the reliable operation of the BES.
BAL-005, Requirement R5	The requirements placed upon the implementation of Dynamic Transfers are covered within Requirement R3. Therefore, this requirement is redundant and does little, if anything, to benefit or protect the reliable operation of the BES.
BAL-005, Requirement R7	The first sentence covers having a functional EMS or other system capable of calculating Reporting ACE and controlling resources, which can be done manually without any detriment to reliability. EOP-008-1 Requirement R1 recognizes that such automated capability may not be available for up to two hours for loss of control center functionality. In addition, the second sentence is not needed, as such actions would be covered under EOP-008. The PRT believes that the term "Operating AGC" in Requirement R7 refers to the

	capability to continuously calculate ACE (not automatic control of resources), which should be considered one of the BAs functional obligations with regard to the reliable operations and situational awareness of the BES. Though redundancy and other provisions may be in place to maintain EMS functionality, there are times when the information may not be available where the provisions under EOP-008-1 would apply. In light of these unnecessary redundancies, this requirement does little, if anything, to benefit or protect the reliable operation of the BES.
BAL-005, Requirement R9, Part 9.1	The Actual Net Interchange and Scheduled Net Interchange values in the Reporting ACE calculation include provisions for the Balancing Authority to include its high voltage direct (HVDC) link to another asynchronous interconnection. By assuring the values are handled consistently in the actual and scheduled Interchange terms included in the real-time Reporting ACE by definition, the Balancing Authority is not being instructed "how" to implement the HVDC link, but allowed to decide the method it will use. By focusing on real-time Reporting ACE, we are assuring reliability is addressed and maintained at all times. Because the Reporting ACE addresses the reliability concerns originally contemplated in this requirement, the requirement is needlessly redundant and does little, if anything, to benefit or protect the reliable operation of the BES.
BAL-005, Requirement R10	The definition of Reporting ACE includes the provision that Scheduled Net Interchange (NIs) used in the Reporting ACE calculation include Dynamic Schedules. Therefore, this requirement is redundant and does little, if anything, to benefit or protect the reliable operation of the BES.
BAL-005, Requirement R11	The definition of Reporting ACE includes the provision that the effect of schedule ramps be included in the value Scheduled Net Interchange (NIs) used in the Reporting ACE calculation. Therefore, this requirement is redundant and does little, if anything, to benefit or protect the reliable operation of the BES.
BAL-006, Requirement R1	Requirement R1 is written only as an energy accounting requirement. The Requirement is administrative in nature and does little, if anything to benefit or protect the reliable operation of the BES. However, the SDT should determine if there is merit in developing a reliability metric specific to this standard including the calculation of Inadvertent Interchange in a reliability metric to measure performance to certain requirements under BAL-0065, where the SDT may consider including the calculation of Inadvertent Interchange.
BAL-006, Requirement R2	Requirement R2 is written only as an energy accounting requirement. The Requirement is administrative in nature and does little, if anything to benefit or protect the reliable operation of the BES. However, the PRT recommends that the SDT incorporate Requirement R2 into a revised definition of Inadvertent Interchange.

The BARC 2 PRT carefully considered each recommendation made in the Independent Expert Review Report (IERR) as detailed in Table 2 below. Based on the BARC 2 PRT's discussions and expertise on the matter, including some having been involved in the development and revisions to NERC Policy 1 used as the basis for the NERC BAL Standards, the BARC 2 PRT determined that the balance of the requirements recommended for retirement by the Independent Expert Review Report are necessary to retain in some form for reliability:

Table 2 - PRT Consideration of IERR Recommendations

Requirement	IERR Recommendation	PRT Response
BAL-005, Requirement R2	Retire, P81. Phase 1	Requirement removed under Paragraph 81 Phase 1.
BAL-005, Requirement R3	Retire, P81. Duplicative of R1.	The PRT **disagreed** with the IERR, as the intent of Requirement R1 is to ensure that all load, resources and transmission facilities are accounted for within the BAs in an Interconnection, whereas Requirement R3 was intended to cover the metering communications, etc., when load or resources may be Dynamically Transferred. The PRT recommendations include treating the implementation of Tie-Lines, Pseudo-Ties, and Dynamic Schedules in a similar manner, as all require agreement on the common information that will be used between the Adjacent BAs and the implementation of dynamically changing data in the Reporting ACE. The PRT recommends that the SDT not use the term "Regulation Service," as in general this statement could apply to implementation of Dynamic Schedules or Pseudo-Ties, and the desire to have a common point for the data shared between the BAs implementing the Dynamic Transfer. Entities must have a process in place to always have common and agreed-upon information even when primary facilities are not available. The PRT recommends removing "adequate" and "Burden" from the requirement.

BAL-005, Requirement R8	Retire, P81. Outdated due to technology.	The PRT **disagreed** with the IERR, as Requirement R8 establishes the minimum expectation of how often ACE must be calculated by all Balancing Authorities. However, as written, Requirement R8 provides no provisions for abnormal or emergency operations when the automated calculation of ACE may not be available. The PRT recommendations include that the SDT revise the Requirement with the proper context of a minimum normal scan rate and clarify how frequently all components must be factored into the Reporting ACE equation under normal operation. With respect to the sub-requirements, the SDT should ensure that any proposed revisions accommodate abnormal and emergency operations, including the possibility that the EMS or supporting telemetry may not be available, such as during an evacuation to a backup site. The PRT notes that the SDT should consider a requirement focused on a minimum scan-rate expectation under normal operations, rather than a requirement that could be interpreted as if systems have 100% availability.
BAL-005, Requirement R9	Retire, P81. This is a definition not a requirement.	The PRT **agreed** with the IERR to retire Requirement R9, as the Interchange values are included the definition of Reporting ACE.
BAL-005, Requirement R10	Retire, P81. This is a definition not a requirement.	The PRT **agreed** with the IERR as the definition of Reporting ACE includes the provision that Scheduled Net Interchange (NIs) used in the Reporting ACE calculation include Dynamic Schedules.
BAL-005, Requirement R11	Retire, P81. This is a business practice and is automated in most EMS software.	The PRT **agreed** with the IERR, as the definition of Reporting ACE includes the provision that the effect of schedule ramps be included in the value Scheduled Net Interchange (NIs) used in the Reporting ACE calculation.
BAL-005, Requirement R12	Retire, P81. This in the ACE equation so does not need to be repeated.	The PRT **agreed** with the IERR to retire Requirement R12 as written. However, the intent of certain sub requirements still needs to be captured and written as applicable to Tie-Line, Pseudo-Ties and Dynamic Schedules. The PRT recommends a new requirement where each respective Adjacent BAalancing Authority has agreed to common

		measuring points that produce an agreed-to common value to be included in the calculation of Reporting ACE. Accuracy and review of the agreed-to common value is reflected in the new requirement requiring comparison of hourly megawatt-hour values against the integrated data operated to for Tie-Lines, Dynamic Schedules, and Pseudo-Ties. The SDT should review the requirement as it relates to current practices to ensure the reliability needs are met.
BAL-005, Requirement R13	Retire, P81. This is after the fact and is automated in most EMS software.	The PRT **disagreed** with the IERR on some aspects of R13. The PRT suggests deleting the first sentence of R13, and suggests that the SDT include in a guideline document the practice of performing hourly error checks of the NIA operated to for the hour against an end-of-the-hour reference. The PRT also recommends a separate requirement specific to adjustments as needed to the Reporting ACE to reflect the meter error adjustment. However, the PRT is concerned that requiring correction of a component of ACE when in error (no matter how negligible) would be problematic in that not all errors require correction. The PRT recommends that the SDT consider stating the requirement in such a manner that I_{ME} is required to be zero except during times needed to compensate for any data or equipment error affecting a component of the Reporting ACE calculation (Interchange or frequency). The SDT should also allow in this requirement for other means of addressing metering corrections, which may include possible revision to real-time metering data. Uses of the I_{ME} term in the Reporting ACE may also be an appropriate subject for the guideline document the PRT is recommending that the SDT develop to accompany BAL-005 covering some of the suggested best practices.

BAL-005, Requirement R16	Retire, This is a guide for the quality of the EMS system. Provide to the 2009-02 team for consideration.	The PRT **agreed** with the IERR to retire Requirement R16 contingent upon addressing one provision. The PRT recommends moving the requirement for flagging bad data to revisions made in Requirement R14.
BAL-006, Requirement R1	Retire. This is only for energy accounting. Covered by tagging requirements	The PRT **agreed** with the IERR that R1 is an energy accounting requirement and should be retired; however, the PRT recommends that the SDT determine if there is merit in developing a reliability metric specific to this standard to measure performance to certain requirements under BAL-006, where the SDT may consider including the calculation of Inadvertent Interchange. In development of any metric, the PRT recommends that the SDT determine the appropriate time-frame for reliability (as close to real-time as possible). Similar to how BAL-001-2 has CPS1 and BAAL measures dependent upon the BA calculating its Reporting ACE without a stated requirement that "Each BA shall calculate its Reporting ACE", the PRT felt that if the industry supports a measure being developed that uses Inadvertent Interchange in the measure of performance, that the BA would calculate Inadvertent Interchange as needed to comply. Also, similar to the approach taken for defining Reporting ACE in the Glossary with all of the components necessary for the calculation, the PRT is recommending in Requirement R2 below that the definition of Inadvertent Interchange also be updated so that all components necessary for the calculation are identified.
BAL-006, Requirement R2	Retire. This is only for energy accounting. Covered by tagging requirements.	The PRT **agreed** with the IERR that R2 is an energy accounting requirement and recommends retirement contingent upon the SDT incorporating Requirement R2 into a revised definition of Inadvertent Interchange. The PRT recommends that this definition be modified to capture that the calculation is on an hourly basis and includes the megawatt-hour values for Tie-Lines, Pseudo-Ties, and Dynamic Schedules, along with other scheduled

		interchange implemented under block scheduling, which does not include the effect of the ramps. The PRT recommends that the definition also include the NERC definitions of On-Peak Accounting and Off-Peak Accounting, which reference the NAESB business practice for inadvertent interchange accounting. The PRT also recommends that the definition clarify the treatment of scheduled and actual interchange associated with asynchronous ties between Interconnections.
BAL-006, Requirement R3	Retire. This is only for energy accounting. Covered by tagging requirements (automated).	The PRT **disagreed** with the IERR but recommends incorporating Requirement R3 into BAL-005, as the requirement relates to the agreement on common values used in Real-time and also recommends developing a guideline to cover the practice of comparing the hourly megawatt-hour values gathered at the end of the hour against the hourly integrated values of the scan-rate data operated to, in order to determine if significant error exists.
BAL-006, Requirement R4	Retire. This is only for energy accounting. Covered by tagging requirements (automated).	The PRT **disagreed** with the IERR, as it is important to reliability that Adjacent Balancing Authorities agree on the scheduled and actual Interchange between them on a timely basis as a means to detect when errors may exist so that they can be corrected in operations. The PRT recommends that the SDT review current practices for confirmation for interchange after-the-fact to determine and justify a shorter duration for agreement on such values for reliability purposes. The PRT also recommends that Requirement R4 be restated to require that the agreement is based upon the aggregate net schedules and net actuals by adjacent BAs as further defined in the new definition of Inadvertent Interchange. In concept, every Tie-Line, Pseudo-Tie, and Interchange Schedule (including Dynamic Schedules), implemented in the Reporting ACE calculation should have an accompanying after-the-fact megawatt-hour value accounted for in the calculation of Inadvertent Interchange. Requirement R4 Part 4.2 might be addressed in the

		new definition of Inadvertent Interchange by the proposed reference to On-Peak Accounting and Off-Peak Accounting. The SDT should review this requirement to determine what elements of the requirement are necessary to support reliability. The SDT also should consider including in a guideline document a practice to support providing operations personnel with information on the comparison of monthly revenue class meters to meters used for real-time operation.
BAL-006, Requirement R5	Retire. This is only for energy accounting. Covered by tagging requirements (automated).	The PRT **could not agree** with the IERR without investigation by the SDT. The SDT should review whether the practice that requires BAs to mutually agree by the 15th calendar day is needed for reliability. The PRT believes there may be merit in requiring BAs to identify the cause of the dispute, and to either correct it within a prescribed number of days, or follow a dispute resolution process. The SDT should ensure that the requirement is clear and distinct, which may require modifying or striking the language regarding dispute resolution.

2. **Clarity:** If the Reliability Standard has an Interpretation, CAN, or issue associated with it, or is frequently violated because of ambiguity, it probably needs to be revised for clarity. Beyond these indicators, is there any reason to believe that the Reliability Standard should be modified to address a lack of clarity? Consider:

   a. Is this a Version 0 Reliability Standard?
   b. Does the Reliability Standard have obviously ambiguous language or language that requires performance that is not measurable?
   c. Are the requirements consistent with the purpose of the Reliability Standard?

   ☒ Yes

   ☐ No

Please summarize your assessment: The BARC 2 PRT recommends the development of a reference document to clarify the requirements in BAL-005 and BAL-006, and recommends revising the following sections of BAL-005 and BAL-006 to improve clarity of the standards:

BAL-005

The BARC2 PRT has completed its review of BAL-005, and among other recommendations, proposes certain revisions below which would remove references to the types of resources and reserves utilized by the Balancing Authority to balance resources and demand. The PRT recommendations focus on the components that make up the Reporting ACE, and not on the ancillary service aspects of resource control that drew criticism from the industry for being specific to generation when BAL-005 was originally filed with the FERC. Among other recommendations, for the implementation of Tie-Lines, Pseudo-Ties, and Dynamic Schedules (all similar in that they utilize real-time data from an agreed-upon common source between Adjacent BAs), the PRT recommends requirements focused on the real-time values operated to. The PRT recommendations for BAL-005 are:

1) **Title**: The PRT recommends changing the title of BAL-005 to "Balancing Authority Control" to remove the implication that BAL-005 pertains exclusively to generation, and better reflect the focus on the BA acquiring necessary data to calculate Reporting ACE so that balancing of resources and demand can be achieved under Tie-Line Bias Control. Based upon the input from the industry, the PRT recommends that the SDT consider whether the term AGC should be retained within any requirements. The PRT also recommends that the SDT pursue revisions to the definition of AGC as proposed below to be resource-neutral.

   AGC: Equipment that automatically adjusts ~~generation~~ resources utilized in a Balancing Authority Area from a central location to maintain the Balancing Authority's Reporting ACE within the bounds required under the NERC Reliability Standards. Resources utilized under AGC may include conventional generation, variable energy resources, storage devices and loads acting as resources, such as Demand Response. ~~may interchange schedule plus Frequency Bias. AGC may also accommodate automatic inadvertent payback and time error correction.~~

2) **Purpose**: The Standards Drafting Team (SDT) tasked with implementing the SAR developed by the PRT should consider revising the "Purpose" statement to focus on acquiring the information necessary for calculating Reporting ACE, while remaining neutral on the types of reserves or resources utilized. The PRT recommends the following for SDT consideration:

   This standard establishes requirements for acquiring necessary data for the Balancing Authority so that balancing of resources and demand can be achieved under Tie-Line Bias Control~~This standard establishes requirements for acquiring necessary data for the~~

~~Balancing Authority to calculate Reporting ACE so that balancing of resources and demand can be achieved.~~

The PRT also recommends that the SDT consider addressing the Hydro Quebec exception for tie line bias control in some form, or a single-BA exception.

3) **Applicability**: The SDT should remove "Generator Operators", "Transmission Operators", and "Load Serving Entities" as applicable entities unless used in the SDT's suggested revisions of this standard. For example, the SDT discussed that the ownership of metering and other factors may drive why the LSE is included in this standard, along with other entities, however consideration should be given to moving requirements for facilities to be within a BA Area to a FAC standard. The PRT is concerned that removing any requirements of the LSE, TOP, and GOP and not reflecting them within another standard may inadvertently transfer certain obligations to the BA to ensure that such loads, resources, and facilities are within their metered boundaries. The SDT should ensure that any suggested revisions address this concern and should also consider placing a comparable requirement in a FAC Standard.

4) **Requirement R1**: The PRT recommends that the content of Requirement R1 be split between what is needed for ensuring facilities are within a BA Area prior to MW being generated or consumed, and what is needed for ensuring balanced operation within an Interconnection. First, the PRT recommends that the SDT consider continuing discussions with the FAC SDT on moving and restating or clarifying the TOP, LSE, and GOP requirements in a~~n~~ FAC Standard to ensure facilities are within the metered boundaries of a BA prior to transmission operation, resource operation, or load being served. The SDT should explore whether the role of the TOP would appropriately cover the loads interconnected to that TOP~~,~~ such that the LSE requirement may not be necessary. Second, the PRT recommends that the SDT revise Requirements R1 and R2 to be BA requirements that all Actual Net Interchange and Scheduled Net Interchange used by the BA in its Reporting ACE calculation, have an Adjacent BA, as proposed in the redlined Requirements R1 and R2. Note that the PRT does not intend ~~with~~ the proposed language to impose any additional requirements on the BA that currently apply to the LSE, GOP, and TOP, but believes that the requirements to identify the applicable BA should perhaps be in the interconnection agreements or a~~n~~ FAC requirement. With respect to proposed Requirement R2, the SDT should ensure that the requirement cannot be misinterpreted to imply that Dynamic Schedules can only be with physically adjacent BAs. The intent is to address adjacency in a manner consistent with the scheduling path no differently than used for interchange schedules.

5) **Requirement R2**: ~~The PRT recommends that the SDT review this requirement to ensure that it is appropriately worded so that adjacency is clearly defined~~Retirement approved by FERC effective January 21, 2014.

~~5)~~6) **Requirement R3**: The PRT recommends that the SDT not use the term "Regulation Service," as in general this statement could apply to implementation of Dynamic Schedules or Pseudo-Ties, and the desire to have a common point for the data shared between the BAs implementing the Dynamic Transfer. The PRT recommends removing "adequate" and "Burden" from the requirement. The PRT recommends expanding Requirement R3 to be applicable to the implementation of tie lines, Pseudo-Ties, and Dynamic Schedules, as all require agreement between adjacent BAs on the agreed-upon points to be implemented. The PRT recommends that the SDT review the other standards such as TOP-005 to assure there is no duplication or redundancy. Specific to the concern on swapping hourly values in BAL-005, the PRT recommends deleting the proposed R3.2 and the first sentence of the proposed R3.5.2, the PRT also recommends the SDT develop a guideline document to accompany BAL-005 covering some of the suggested best practices.

~~6)~~7) **Requirement R4**: The PRT reviewed Requirement R4 with respect to what notification or coordination is necessary that could be considered with the other requirements around Interchange. Initially the PRT was considering a recommendation that the SDT consider the requirement as it applies to Dynamic Transfer implementation as discussed in the Dynamic Transfer reliability guideline, and as it applies to the practice of implementing multiple-BA Dynamic Transfers under a process referred to as ACE Diversity Interchange. The PRT also considered recommendations to delete or modify Requirement R4 so that it requires communication with not only the BAs but any other affected entities, and to strike "providing Regulation Service." However, after further review, the PRT recommends retiring Requirement R4, as the basis for coordination of common values between adjacent BAs is covered in Requirement R3, and correction of information not available has also been addressed. These requirements should ensure that any failure to perform would be reflected in the BA performance under BAL-001-2.

~~7)~~8) **Requirement R5**: The PRT recommends retiring Requirement R5, as the requirements placed upon the implementation of Dynamic Transfers are covered within Requirement R3. With respect to having a backup plan to the extent that a service may no longer be provided, the PRT believes this would be in the terms of the business arrangement. As proposed by the PRT, the requirements remaining in BAL-005 would ensure that any failure to perform would be reflected in the BA performance under BAL-001-2.

~~8)~~9) **Requirement R6**: The PRT recommends that the sentence "Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control" be captured in the definition of "Reporting ACE.". The terms used in the Requirement R6 need to be consistent with those used in Reporting ACE if the Requirement is retained. The SDT should consider whether the 30-minute requirement for RC notification is

sufficient or excessive. The PRT recommends that if a timing requirement remains in the standard that it be structured in a manner to not require communication with the RC if the capability to calculate Reporting ACE is restored within the defined notification period.

~~9)~~10) **Requirement R7**: The PRT recommends retiring this Requirement under Paragraph 81. The first sentence covers having a functional EMS or other system capable of calculating Reporting ACE and controlling resources, which can be done manually without any detriment to reliability. EOP-008-1 Requirement R1 recognizes that such automated capability may not be available for up to two hours for loss of control center functionality. In addition, the second sentence is not needed, as such actions would be covered under EOP-008. The PRT believes that the term "Operating AGC" in Requirement R7 refers to the capability to continuously calculate ACE (not automatic control of resources), which should be considered one of the BAs functional obligations with regard to the reliable operations and situational awareness of the BES. Though redundancy and other provisions may be in place to maintain EMS functionality, there are times when the information may not be available where the provisions under EOP-008-1 would apply.

~~10)~~11) **Requirement R8**: The PRT recommends that the SDT revise the Requirement with the proper context of a minimum normal scan rate and clarify how frequently all components must be factored into the Reporting ACE equation under normal operation. With respect to the sub-requirements, the SDT should ensure that any proposed revisions accommodate abnormal and emergency operations, including the possibility that the EMS or supporting telemetry may not be available, such as during an evacuation to a backup site. The PRT notes that the SDT should consider a requirement focused on a minimum scan-rate expectation under normal operations, rather than a requirement that could be interpreted as if systems have 100% availability.

~~11)~~12) **Requirement R8, Part 8.1**: The BA should have visibility of system frequency within parameters consistent with EOP-008, however the PRT recommends that the requirement not be prescriptive. The SDT should review EOP-008 to ensure the intent of this requirement is covered there, and to ensure consistency among the standards. In addition, the SDT should also consider remote and redundant frequency resources to the extent that the information otherwise available to the BA may not be available upon loss of control center functionality. Such capability may already be anticipated under EOP-008. The SDT should consider the following questions in the development of the revised requirement:

a) How much time is allowed to pass if the redundancy is lost before it must be restored?

b) Does the PRT believe it is acceptable for the second and independent frequency device to be one used by another Balancing Authority?

~~12)~~13) **Requirement R9, Part 9.1**: The PRT recommends retiring this Requirement. The Actual Net Interchange and Scheduled Net Interchange values in the Reporting ACE calculation include provisions for the Balancing Authority to include its high voltage direct (HVDC) link to another asynchronous interconnection. By assuring the values are handled consistently in the actual and scheduled Interchange terms included in the real-time Reporting ACE by definition, the Balancing Authority is not being instructed "how" to implement the HVDC link, but allowed to decide the method it will use. By focusing on real-time Reporting ACE, we are assuring reliability is addressed and maintained at all times. The PRT suggests that the Balancing Authority during an audit may be asked to provide evidence that its HVDC link was included or was not included in Reporting ACE under the provisions allowed by definition.

~~13)~~14) **Requirements R10 and R11**: The PRT recommends the retirement of these requirements, as the basics of both requirements are factored into the definition of Scheduled Net Interchange (NIs) used in the Reporting ACE calculation as defined in the NERC Glossary.

The PRT noted that Requirement R10 is written as if "Net Scheduled Interchange" is the value used in the ACE equation; however, Net Scheduled Interchange has two meanings – the algebraic sum of all Interchange Schedules across a given path, or between Balancing Authorities for a given period or instant in time. Aside from the concern of having a definition with two different meanings, the PRT believes that neither choice in the definition accurately depicts the value inserted into the ACE or Reporting ACE, which would be the algebraic sum of all Net Scheduled Interchange with all Adjacent Balancing Authorities, including Dynamic Schedules. In addition, the PRT could not find a definition of Scheduled Interchange as used in Requirement R11. Under Section 3 below, the PRT recommends changes to certain NERC definitions.

~~14)~~15) **Requirement R12**: The PRT took a holistic approach to Requirement R12 and other requirements related to the implementation of Tie-Lines, Pseudo-Ties, and Dynamic Schedules, as all relate to the information exchanged between adjacent BAs.

The PRT recommends a new ~~requirement~~ Requirement R3 related to the implementation of Tie-Lines, Pseudo-Ties, and Dynamic Schedules, where each respective Adjacent BA has agreed to common measuring points that produce an agreed-to value to be included in the calculation of Reporting ACE. The SDT should review the requirement as it relates to current practices to ensure the reliability needs are met.

The PRT suggests that the holistic approach shall only be achieved if there is a comprehensive definition of ACE. Therefore the PRT recommends the ACE and Reporting ACE definitions be reviewed (understanding and identifying as well why there is a difference) to assure that they are comprehensive (including items such as all AC Tie-Lines, Pseudo-ties, and all other

necessary Adjacent BA information). As the comprehensive details of the ACE calculation in BAL-001-1 will be retired upon implementation of BAL-001-2, where ACE will only be defined in the NERC Glossary, the PRT suggests that a complete review of all the NERC Standards is necessary to assure where ACE is utilized in a Standard, that any update to the ACE definition would not impact any other Standard.

~~15)~~16) **Requirement R13**: The PRT suggests deleting the first sentence of R13, and suggests that the SDT include in a guideline document the practice of performing hourly error checks of the NI_A operated to for the hour against an end-of-the-hour reference.

The PRT also recommends a separate requirement specific to adjustments as needed to the Reporting ACE to reflect the meter error adjustment. However, the PRT is concerned that requiring correction of a component of ACE when in error (no matter how negligible) would be problematic in that not all errors require correction. The PRT recommends that the SDT consider stating the requirement in such a manner that I_{ME} is required to be zero except during times needed to compensate for any data or equipment error affecting a component of the Reporting ACE calculation (Interchange or frequency). The SDT should also allow in this requirement for other means of addressing metering corrections, which may include possible revision to real-time metering data. Uses of the I_{ME} term in the Reporting ACE may also be an appropriate subject for the guideline document the PRT is recommending that the SDT develop to accompany BAL-005 covering some of the suggested best practices.

~~16)~~17) **Requirement R14**: The PRT recommends that the SDT delete the first sentence in R14 and revise the second sentence to cover the minimum amount of information expected for the BA to provide in real-time to its operatormade the recommendation reflected in the proposed redline to define minimum expectations for situational awareness of the BES. The PRT also recommends that the individual components of actual and scheduled interchange with each Adjacent Balancing Authority also be captured (Tie-Lines, Pseudo-Ties, Dynamic Schedules, block schedules as needed for coordination, and real-time schedules). Based on industry comments, the SDT should consider whether this requirement is needed in the BAL standards, whether it is adequately covered elsewhere in the standards, or whether it should be moved to the NERC Rules of Procedure for certification of the Functional Entity.

~~17)~~18) **Requirement R15**: The SDT should consider continued coordination with the Project 2010-02 FAC SDT on potentially placing a requirement in FAC with respect to supporting infrastructure or functionality, or review EOP-008 to determine if existing requirements adequately address primary control center functionality.

~~18)~~19) **Requirement R16**: The PRT recommends moving the requirement for flagging bad data to revisions made in Requirement R14.

~~19)~~20) **Requirement R17**: The PRT recommends that this requirement be written to be specific to the equipment used to determine the frequency component required for Reporting ACE. The PRT also recommends that the SDT recommend moving any accuracy requirements applicable to the needs of the Transmission Operator, which may include MW, MVAR, voltage, potential transformer, current transformer, and remote terminal unit or equivalent to a TOP or FAC standard. Further study would be needed on the ".25% of full scale" and the "appropriate accuracy" language.

BAL-006

The BARC2 PRT has completed its review of BAL-006 and recommends that it be revised. The recommendations below include moving any requirements with implications to real-time operations into BAL-005.

Among other work, the review team considered a FERC directive that recommended the development of a metric to bound the magnitude of inadvertent accumulations, as those accumulations may be indicative of a Balancing Authority excessively leaning on the resources of others in its Interconnection. The review team consensus was that an Inadvertent Interchange accumulation value alone cannot yield useful information concerning whether a Balancing Authority is operating reliably. The PRT document on the consideration of issues and directives more fully covers the PRT recommendations related to the FERC directives. The PRT recommendations for BAL-006 are:

1) **Purpose**: As the revisions proposed for BAL-006 focus on the minimum requirements for Adjacent Balancing Authorities to agree upon the hourly MW amounts of scheduled and actual Interchange between them, which reinforces that errors in coordination or process will be identified, the PRT recommends that the SDT revise the Purpose statement to be consistent with the Requirements as further developed under the SAR posted with this recommendation.

2) **Requirement R1**: The PRT recommends removing Requirement R1 as written and recommends that the SDT determine if there is merit in developing a reliability metric specific to this standard including the calculation of Inadvertent Interchange in a reliability metric to measure performance to certain requirements under BAL-0065, where the SDT may consider including the calculation of Inadvertent Interchange. In development of any metric, the PRT recommends that the SDT determine the appropriate time-frame for reliability (as close to real-time as possible). Similar to how BAL-001-2 has CPS1 and BAAL measures dependent upon the BA calculating its Reporting ACE without a stated requirement that "Each BA shall calculate its Reporting ACE", the PRT felt that if the industry supports a measure being developed that uses Inadvertent Interchange in the measure of performance, that the BA would calculate Inadvertent Interchange as needed to comply. Also, similar to the approach taken for defining Reporting ACE in the Glossary with all of the components necessary for the calculation, the PRT is recommending in Requirement R2 below that the definition of Inadvertent Interchange also be updated so that all components necessary for the calculation are identified.

3) **Requirement R2**: The PRT recommends incorporating R2 into a revised definition of Inadvertent Interchange: The PRT recommends that this definition be modified to capture that the calculation is on an hourly basis and includes the megawatt-hour values for Tie-Lines, Pseudo-Ties, and Dynamic Schedules, along with other scheduled interchange implemented under block scheduling, which does not include the effect of the ramps. The PRT recommends

that the definition also include the NERC definitions of On-Peak Accounting and Off-Peak Accounting, which reference the NAESB business practice for inadvertent interchange accounting. The PRT also recommends that the definition clarify the treatment of scheduled and actual interchange associated with asynchronous ties between Interconnections.

4) **Requirement R3**: The PRT recommends incorporating Requirement R3 into BAL-005, as the requirement relates to the agreement on common values used in Real-time and also recommends developing a guideline to cover the practice of comparing the hourly megawatt-hour values gathered at the end of the hour against the hourly integrated values of the scan-rate data operated to, in order to determine if significant error exists.

5) **Requirement R4**: With respect to Requirement R4, the SDT should review current practices for confirmation for interchange after-the-fact to determine and justify a shorter duration for agreement on such values for reliability purposes. The PRT also recommends that Requirement R4 be restated to require that the agreement is based upon the aggregate net schedules and net actuals by adjacent BAs as further defined in the new definition of Inadvertent Interchange. In concept, every Tie-Line, Pseudo-Tie, and Interchange Schedule (including Dynamic Schedules), implemented in the Reporting ACE calculation should have an accompanying after-the-fact megawatt-hour value accounted for in the calculation of Inadvertent Interchange.

6) **Requirement R4, Part 4.2:** The SDT should evaluate whether this requirement is addressed in the new definition of Inadvertent Interchange by the proposed reference to On-Peak Accounting and Off-Peak Accounting.

7) **Requirement R4, Part 4.3**: The SDT should review this requirement to determine what elements of the requirement are necessary to support reliability. The SDT also should consider including in a guideline document a practice to support providing operations personnel with information on the comparison of monthly revenue class meters to meters used for real-time operation.

8) **Requirement R5**: The SDT should review whether the practice that requires BAs to mutually agree by the 15th calendar day is needed for reliability. The PRT believes there may be merit in requiring BAs to identify the cause of the dispute, and to either correct it within a prescribed number of days, or follow a dispute resolution process. The SDT should ensure that the requirement is clear and distinct, which may require modifying or striking the language regarding dispute resolution.

3. **Definitions**: Do any of the defined terms used within the Reliability Standard need to be refined?

   ☒ Yes

☐ No

Please explain: The SDT should review definitions for consistency on Scheduled Interchange and clarification of Pseudo-Tie to indicate that it is treated no differently than tie line metering for a common point between two BAs, communication requirements, etc., and included in the calculation of Actual Net Interchange and the Reporting ACE equation. The SDT should also review proposed changes to the INT standards as part of this examination.

The use of multiple Interchange terms within the Standards prompted the PRT to reference the Glossary of Terms Used in NERC Reliability Standards. The PRT reviewed the definitions of Actual Net Interchange and Scheduled Net Interchange used within the definition of Reporting ACE, along with the definitions of Interchange Schedule, Net Interchange Schedule, Net Scheduled Interchange, and Net Actual Interchange. The PRT found it confusing to have multiple interchange definitions with similar titles, and some with similar meanings, and recommends the SDT consider the following:

a) Scan all of the NERC Standards, all terms in BAL-005 and -006, and the NERC Glossary to determine if the terms associated with the subject standards are used or defined appropriately (e.g., NI_S, NI_A, I_S, I_A, ACE, and Reporting ACE).
b) Ensure that any suggested revisions to scheduled interchange definitions retain the overall concepts that:
   - the schedule ramps must be reflected in the Reporting ACE;
   - the static schedules (any that are not Dynamic Schedules) coordinated between Adjacent BAs prior to implementation use block accounting ignoring the schedule ramps;
   - the estimated MW values of the Dynamic Schedules prior to implementation are typically not included in the scheduled interchange values coordinated and agreed to between Adjacent BAs; and
   - the megawatt-hour values of scheduled interchange agreed-to after the fact reflect the static schedules (any that are not Dynamic Schedules) operated to using block accounting integrated over the hour but ignoring the ramps, plus the hourly integrated values for any Dynamic Schedules.

Suggested Revisions to NERC Glossary Definitions:

Automatic Generation Control ("AGC")
Equipment that automatically adjusts ~~generation~~ **resources** utilized in a Balancing Authority Area from a central location to maintain the Balancing Authority's ACE within the bounds required under the NERC Reliability Standards**. Resources utilized under AGC may include conventional generation, variable energy resources, storage devices and loads acting as resources, such as Demand Response**. ~~may interchange schedule plus~~

~~Frequency Bias.~~ ~~AGC may also accommodate automatic inadvertent payback and time error correction.~~

Reporting ACE
The scan rate values of a Balancing Authority's Area Control Error (ACE) measured in MW, which includes the difference between the Balancing Authority's **Actual Net Interchange** and its **Scheduled Net Interchange**, plus its Frequency Bias obligation, plus any known meter error. In the Western Interconnection, Reporting ACE includes Automatic Time Error Correction (ATEC).

Reporting ACE is calculated as follows:
Reporting ACE = $(NI_A - NI_S) - 10B(F_A - F_S) - I_{ME}$
Reporting ACE is calculated in the Western Interconnection as follows:
Reporting ACE = $(NI_A - NI_S) - 10B(F_A - F_S) - I_{ME} + I_{ATEC}$

Where:
NI_A (Actual Net Interchange) is the algebraic sum of actual megawatt transfers across all Tie Lines and Pseudo-Ties ***with all Adjacent Balancing Authorities, which may use anti-aliasing filters as needed to more accurately represent the actual interchange as determined by the Adjacent Balancing Authorities.*** Balancing Authorities directly connected via asynchronous ties to another Interconnection may include or exclude ***the actual*** megawatt transfers on those Tie lines in ***the calculation of NI_A***, provided they are implemented in the same manner for ***Scheduled Net Interchange***.

NI_S (Scheduled Net Interchange) is the algebraic sum of all scheduled megawatt transfers, including Dynamic Schedules, with ***all A***djacent Balancing Authorities, and taking into account the effects of schedule ramps. Balancing Authorities directly connected via asynchronous ties to another Interconnection may include or exclude ***the scheduled*** megawatt transfers on those Tie Lines in the ***calculation of NI_S***, provided they are implemented in the same manner for ***Actual Net Interchange***.

B (Frequency Bias Setting) is the Frequency Bias Setting (in negative MW/0.1 Hz) for the Balancing Authority. **10** is the constant factor that converts the frequency bias setting units to MW/Hz.
F_A (Actual Frequency) is the measured frequency in Hz.
F_S (Scheduled Frequency) is 60.0 Hz, except during a time***-error*** correction.
I_{ME} (Interchange Meter Error) is the meter error correction factor and represents the difference between the integrated hourly average of the ~~net interchange actual~~ ***Actual Net Interchange*** (NI_A) and the cumulative hourly net Interchange energy measurement (in megawatt-hours).

4. **Compliance Elements:** Are the compliance elements associated with the requirements (Measures, Data Retention, Violation Risk Factors (VRF), and Violation Severity Levels (VSL)) consistent with the

direction of the Reliability Assurance Initiative and FERC and NERC guidelines? If you answered "No," please identify which elements require revision, and why:

☐ Yes

☒ No

The standard drafting team will address compliance elements.

5. **Consistency with Other Reliability Standards:** Does the Reliability Standard need to be revised for formatting and language consistency among requirements within the Reliability Standard or consistency with other Reliability Standards? If you answered "Yes," please describe the changes needed to achieve formatting and language consistency:

   ☒ Yes

   ☐ No

   As noted above, the PRT recommends a thorough review of all of the NERC Standards, all terms in BAL-005 and -006, and the NERC Glossary to determine if the Interchange-related terms associated with the subject standards are used or defined appropriately. For example, the PRT noted that BAL-005 R10 is written as if "Net Scheduled Interchange" is the value used in the ACE equation; however, Net Scheduled Interchange has two meanings – the algebraic sum of all Interchange Schedules across a given path, or between Balancing Authorities for a given period or instant in time. Also, the PRT could not find a definition of Scheduled Interchange as used in BAL-005 R11.

6. **Changes in Technology, System Conditions, or other Factors:** Does the Reliability Standard need to be revised to account for changes in technology, system conditions, or other factors? If you answered "Yes," please describe the changes and specifically what the potential impact is to reliability if the Reliability Standard is not revised:

   ☐ Yes

   ☒ No

7. **Consideration of Generator Interconnection Facilities:** Is responsibility for generator interconnection Facilities appropriately accounted for in the Reliability Standard?

   ☒ Yes

   ☐ No

Guiding Questions:

If the Reliability Standard is applicable to GOs/GOPs, is there any ambiguity about the inclusion of generator interconnection Facilities? (If generation interconnection Facilities could be perceived to be excluded, specific language referencing the Facilities should be introduced in the Reliability Standard.)

If the Reliability Standard is not applicable to GOs/GOPs, is there a reliability-related need for treating generator interconnection Facilities as transmission lines for the purposes of this Reliability Standard? (If so, GOs and GOPs that own or operate relevant generator interconnection Facilities should be explicit in the applicability section of the Reliability Standard.)

As indicated in the detail provided for BAL-005 R1, the PRT proposes that the GOP requirement to have its resource facilities within the metered boundaries of a BA be moved to an FAC requirement as no MWs should be generated prior to such arrangements.

Recommendation

The answers to the questions above, along with a preliminary recommendation of the Review Team, will be posted for a 45-day comment period, and the comments publicly posted. The Review Team will review the comments to evaluate whether to modify its initial recommendation, and will document the final recommendation which will be presented to the Standards Committee.

Preliminary Recommendation (to be completed by the Review Team after its review and prior to posting the results of the review for industry comment):

- ☐ REAFFIRM
- ☒ REVISE
- ☐ RETIRE

Technical Justification *(If the Review Team recommends that the Reliability Standard be revised, a draft SAR may be included and the technical justification included in the SAR)*: See the attached draft SAR.

Preliminary Recommendation posted for industry comment (date): February 21, 2014

Final Recommendation (to be completed by the Review Team after it has reviewed industry comments on the preliminary recommendation):

- ☐ REAFFIRM *(This should only be checked if there are no outstanding directives, interpretations or issues identified by stakeholders.)*
- ☐ REVISE
- ☐ RETIRE

Technical Justification *(If the Review Team recommends that the Reliability Standard be revised, a draft SAR may be included and the technical justification included in the SAR)*:

Date submitted to NERC Staff:

Attachment 1: Results-Based Standards

The fourth question for NERC staff and the Review Team asks if the Reliability Standard needs to be converted to the results-based standards (RBS) format. The information below will be used by NERC staff and the Review Team in making this determination.

Transitioning the current body of standards into a clear, concise, and effective body will require a comprehensive application of the RBS concept. RBS concepts employ a defense-in-depth strategy for Reliability Standards development where each requirement has a role in preventing system failures, and the roles are complementary and reinforcing. Reliability Standards should be viewed as a portfolio of requirements designed to achieve an overall defense-in-depth strategy and comply with the quality objectives identified in the resource document titled, "Acceptance Criteria of a Reliability Standard."

Accordingly, the Review Team shall consider whether the Reliability Standard contains results-based requirements with sufficient clarity to hold entities accountable without being overly prescriptive as to how a specific reliability outcome is to be achieved. The RBS concept, properly applied, addresses the clarity and effectiveness aspects of a standard.

A Reliability Standard that adheres to the RBS format should strive to achieve a portfolio of performance-, risk-, and competency-based mandatory reliability requirements that support an effective defense-in-depth strategy. Each requirement should identify a clear and measurable expected outcome, such as: a) a stated level of reliability performance, b) a reduction in a specified reliability risk, or c) a necessary competency.

a. **Performance-Based**—defines a particular reliability objective or outcome to be achieved. In its simplest form, a results-based requirement has four components: who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome?

b. **Risk-Based**—preventive requirements to reduce the risks of failure to acceptable tolerance levels. A risk-based reliability requirement should be framed as: who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome that reduces a stated risk to the reliability of the bulk power system?

c. **Competency-Based**—defines a minimum set of capabilities an entity needs to have to demonstrate it is able to perform its designated reliability functions. A competency-based reliability requirement should be framed as: who, under what conditions (if any), shall have what capability, to achieve what particular result or outcome to perform an action to achieve a result or outcome or to reduce a risk to the reliability of the bulk power system?

Additionally, each RBS-adherent Reliability Standard should enable or support one or more of the eight reliability principles listed below. Each Reliability Standard should also be consistent with all of the reliability principles.

1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.

5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected bulk power systems.

6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

7. The reliability of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.

8. Bulk power systems shall be protected from malicious physical or cyber attacks.

If the Reliability Standard does not provide for a portfolio of performance-, risk-, and competency-based requirements or consistency with NERC's reliability principles, NERC staff and the Review Team should recommend that the Reliability Standard be revised or reformatted in accordance with the RBS format.

Attachment 2: Paragraph 81 Criteria

The first question for the Review Team asks if one or more of the requirements in the Reliability Standard meet(s) criteria for retirement or modification based on Paragraph 81 concepts.[3] Use the Paragraph 81 criteria explained below to make this determination. Document the justification for the decisions throughout and provide them in the final assessment in the Periodic Review Template.

For a Reliability Standard requirement to be proposed for retirement or modification based on Paragraph 81 concepts, it must satisfy **both**: (i) Criterion A (the overarching criterion); and (ii) at least one of the Criteria B listed below (identifying criteria). In addition, for each Reliability Standard requirement proposed for retirement or modification, the data and reference points set forth below in Criteria C should be considered for making a more informed decision.

Criterion A (Overarching Criterion)

The Reliability Standard requirement requires responsible entities ("entities") to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES.

Section 215(a) (4) of the United States Federal Power Act defines "reliable operation" as: "… operating the elements of the bulk power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

Criteria B (Identifying Criteria)

B1. Administrative

The Reliability Standard requirement requires responsible entities to perform a function that is administrative in nature, does not support reliability and is needlessly burdensome.

This criterion is designed to identify requirements that can be retired or modified with little effect on reliability and whose retirement or modification will result in an increase in the efficiency of the ERO compliance program. Administrative functions may include a task that is related to developing procedures or plans, such as establishing communication contacts. Thus, for certain requirements, Criterion B1 is closely related to Criteria B2, B3 and B4. Strictly administrative functions do not inherently negatively impact reliability directly and, where possible, should be eliminated or modified for purposes of efficiency and to allow the ERO and entities to appropriately allocate resources.

[3] In most cases, satisfaction of the Paragraph 81 criteria will result in the retirement of a requirement. In some cases, however, there may be a way to modify a requirement so that it no longer satisfies Paragraph 81 criteria. Recognizing that, this document refers to both options.

B2. Data Collection/Data Retention
These are requirements that obligate responsible entities to produce and retain data which document prior events or activities, and should be collected via some other method under NERC's rules and processes.

This criterion is designed to identify requirements that can be retired or modified with little effect on reliability. The collection and/or retention of data do not necessarily have a reliability benefit and yet are often required to demonstrate compliance. Where data collection and/or data retention is unnecessary for reliability purposes, such requirements should be retired or modified in order to increase the efficiency of the ERO compliance program.

B3. Documentation
The Reliability Standard requirement requires responsible entities to develop a document (*e.g.,* plan, policy or procedure) which is not necessary to protect reliability of the bulk power system.

This criterion is designed to identify requirements that require the development of a document that is unrelated to reliability or has no performance or results-based function. In other words, the document is required, but no execution of a reliability activity or task is associated with or required by the document.

B4. Reporting
The Reliability Standard requirement obligates responsible entities to report to a Regional Entity, NERC or another party or entity. These are requirements that obligate responsible entities to report to a Regional Entity on activities which have no discernible impact on promoting the reliable operation of the BES and if the entity failed to meet this requirement there would be little reliability impact.

B5. Periodic Updates
The Reliability Standard requirement requires responsible entities to periodically update (*e.g.,* annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.

This criterion is designed to identify requirements that impose an updating requirement that is out of sync with the actual operations of the BES, unnecessary, or duplicative.

B6. Commercial or Business Practice
The Reliability Standard requirement is a commercial or business practice, or implicates commercial rather than reliability issues.

This criterion is designed to identify those requirements that require: (i) implementing a best or outdated business practice or (ii) implicating the exchange of or debate on commercially sensitive information while doing little, if anything, to promote the reliable operation of the BES.

B7. Redundant
The Reliability Standard requirement is redundant with: (i) another FERC-approved Reliability Standard requirement(s); (ii) the ERO compliance and monitoring program; or (iii) a governmental regulation (*e.g.,* Open Access Transmission Tariff, North American Energy Standards Board ("NAESB"), etc.).

This criterion is designed to identify requirements that are redundant with other requirements and are, therefore, unnecessary. Unlike the other criteria listed in Criterion B, in the case of redundancy, the task or activity itself may contribute to a reliable BES, but it is not necessary to have two duplicative requirements on the same or similar task or activity. Such requirements can be retired or modified with little or no effect on reliability and removal will result in an increase in efficiency of the ERO compliance program.

Criteria C (Additional data and reference points)
Use the following data and reference points to assist in the determination of (and justification for) whether to proceed with retirement or modification of a Reliability Standard requirement that satisfies both Criteria A and B:

C1. Was the Reliability Standard requirement part of a FFT filing?
The application of this criterion involves determining whether the requirement was included in a FFT filing.

C2. Is the Reliability Standard requirement being reviewed in an ongoing Standards Development Project?
The application of this criterion involves determining whether the requirement proposed for retirement or modification is part of an active Standards Development Project, with consideration for the status of the project. If the requirement has been approved by Registered Ballot Body and is scheduled to be presented to the NERC Board of Trustees, in most cases it will not need to be addressed in the periodic review. The exception would be a requirement, such as the Critical Information Protection (CIP) requirements for Version 3 and 4, that is not due to be retired for an extended period of time. Also, for informational purposes, whether the requirement is included in a future or pending Standards Development Project should be identified and discussed.

C3. What is the VRF of the Reliability Standard requirement?
The application of this criterion involves identifying the VRF of the requirement proposed for retirement or modification, with particular consideration of any requirement that has been assigned as having a Medium or High VRF. Also, the fact that a requirement has a Lower VRF is not dispositive that

it qualifies for retirement or modification. In this regard, Criterion C3 is considered in light of Criterion C5 (Reliability Principles) and C6 (Defense in Depth) to ensure that no reliability gap would be created by the retirement or modification of the Lower VRF requirement. For example, no requirement, including a Lower VRF requirement, should be retired or modified if doing so would harm the effectiveness of a larger scheme of requirements that are purposely designed to protect the reliable operation of the BES.

C4. In which tier of the most recent Actively Monitored List (AML) does the Reliability Standard requirement fall?

The application of this criterion involves identifying whether the requirement proposed for retirement or modification is on the most recent AML, with particular consideration for any requirement in the first tier of the AML.

C5. Is there a possible negative impact on NERC's published and posted reliability principles?

The application of this criterion involves consideration of the eight following reliability principles published on the NERC webpage.

Reliability Principles

NERC Reliability Standards are based on certain reliability principles that define the foundation of reliability for North American bulk power systems. Each reliability standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of reliability of the North American bulk power systems. Each reliability standard shall also be consistent with all of the reliability principles, thereby ensuring that no standard undermines reliability through an unintended consequence.

Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

Principle 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.

Principle 5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected bulk power systems.

Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

Principle 7. The reliability of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.

Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks. (footnote omitted).

C6. Is there any negative impact on the defense in depth protection of the BES?
The application of this criterion considers whether the requirement proposed for retirement or modification is part of a defense in depth protection strategy. In order words, the assessment is to verify whether other requirements rely on the requirement proposed for retirement or modification to protect the BES.

C7. Does the retirement or modification promote results or performance based Reliability Standards?
The application of this criterion considers whether the requirement, if retired or modified, will promote the initiative to implement results- and/or performance-based Reliability Standards.

Standards Authorization Request Form

When completed, please email this form to: sarcomm@nerc.com.

NERC welcomes suggestions to improve the reliability of the Bulk-Power System through improved Reliability Standards. Please use this Standard Authorization Request (SAR) form to submit your request to propose a new Reliability Standard, a revision to a Reliability Standard, or the retirement of a Reliability Standard.

Request to propose a new Reliability Standard, a revision to a Reliability Standard, or the retirement of a Reliability Standard			
Title of Proposed Reliability Standard:	BAL-005-3 – Automatic Generation Control and BAL-006-3 – Inadvertent Interchange		
Date Submitted:	February 18, 2014		
SAR Requester Information			
Name:	Doug Hils		
Organization:	Duke Energy		
Telephone:	513.287.2149	Email:	doug.hils@duke-energy.com
SAR Type (Check as many as applicable)			
☐ New Reliability Standard ☒ Revision to existing Reliability Standards		☐ Retirement of existing Reliability Standard ☐ Urgent Action	

SAR Information
Industry Need (What is the industry problem this request is trying to solve?):
The North American Electric Reliability Corporation (NERC) is required to conduct a periodic review of each NERC Reliability Standard at least once every ten years, or once every five years for Reliability Standards approved by the American National Standards Institute as an American National Standard. Project 2010-14.2 - Phase 2 of Balancing Authority Reliability-based Controls (BARC 2) was included in the current cycle of periodic reviews.

SAR Information
The NERC Standards Committee appointed eleven industry subject matter experts to serve on the BARC 2 periodic review team (BARC 2 PRT) in the fall of 2013. The BARC 2 PRT used background information on the standards and the questions set forth in the Periodic Review Template developed by NERC and approved by the Standards Committee, along with associated worksheets and reference documents, to determine whether BAL-005-0_2b and BAL-006-2 should be: (1) affirmed as is (i.e., no changes needed); (2) revised (which may include revising or retiring one or more requirements); or (3) withdrawn. As a result of that examination, the BARC 2 PRT recommends to REVISE BAL-005-0_2b and BAL-006-2, and has therefore developed this Standard Authorization Request (SAR) outlining the proposed scope and technical justification for the revisions.
Purpose or Goal (How does this request propose to address the problem described above?):
This SAR proposes revising BAL-005 and BAL-006 in line with the recommendations of the BARC 2 PRT as described in the *PRT Recommendation to Revise BAL-005 and BAL-006*, (Attachment 1). The proposed changes to the standards add clarity, remove redundancy, take into account technological changes since the last versions of the standards, address FERC directives, and bring compliance elements in accordance with NERC guidelines. A detailed description of the PRT's recommended changes are contained later in this SAR.
Identify the Objectives of the proposed Reliability Standard's requirements (What specific reliability deliverables are required to achieve the goal?):
The objective of BAL-005 is to establish requirements for acquiring necessary data for the Balancing Authority to calculate Reporting ACE so that balancing of resources and demand can be achieved under Tie-Line Bias Control. The current objective of BAL-006 is to define define a process for monitoring Balancing Authorities to ensure that, over the long term, Balancing Authority Areas do not excessively depend on other Balancing Authority Areas in the Interconnection for meeting their demand or Interchange obligations. As the revisions proposed for BAL-006 focus on the minimum requirements for Adjacent Balancing Authorities to agree upon the hourly MW amounts of scheduled and actual Interchange between them, which reinforces that errors in coordination or process will be identified, the PRT recommends that the SDT revise the Purpose statement to be consistent with the Requirements as further developed under this SAR.

SAR Information
Brief Description (Provide a paragraph that describes the scope of this Reliability Standard action.)
The scope of this standard action is to revise BAL-005 and BAL-006 in accordance with the recommendations made by the PRT in the *PRT Recommendation to Revise BAL-005 and BAL-006*, (Attachment 1), and consistent with industry consensus to make additional standard revisions to the extent such consensus develops.
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the Reliability Standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the Reliability Standard action.)

1. BAL-005

The BARC2 PRT has completed its review of BAL-005, and, among other recommendations, proposes certain revisions below which would remove references to the types of resources and reserves utilized by the Balancing Authority to balance resources and demand. The PRT recommendations focus on the components that make up the Reporting ACE, and not on the ancillary service aspects of resource control that drew criticism from the industry for being specific to generation when BAL-005 was originally filed with the FERC. Among other recommendations, for the implementation of Tie-Lines, Pseudo-Ties, and Dynamic Schedules (all similar in that they utilize real-time data from an agreed-upon common source between Adjacent BAs), the PRT recommends requirements focused on the real-time values operated to. The PRT's recommendations for BAL-005 are fully detailed below.

1) **Title**: The PRT recommends changing the title of BAL-005 to "Balancing Authority Control" to remove the implication that BAL-005 pertains exclusively to generation, and better reflect the focus on the BA acquiring necessary data to calculate Reporting ACE so that balancing of resources and demand can be achieved under Tie-Line Bias Control. Based upon the input from the industry, the PRT recommends that the SDT consider whether the term AGC should be retained within any requirements. The PRT also recommends that the SDT pursue revisions to the definition of AGC as proposed below to be resource-neutral.

AGC: Equipment that automatically adjusts ~~generation~~ resources utilized in a Balancing Authority Area from a central location to maintain the Balancing Authority's Reporting ACE within the bounds required under the NERC Reliability Standards. Resources utilized under AGC may include conventional generation, variable energy resources, storage devices and loads acting as resources, such as Demand Response. ~~may interchange~~

SAR Information

~~schedule plus Frequency Bias.~~ ~~AGC may also accommodate automatic inadvertent payback and time error correction.~~

2) **Purpose**: The SDT would also be tasked with consideration of revising the "Purpose" statement to focus on acquiring the information necessary for calculating Reporting ACE, while remaining neutral on the types of reserves or resources utilized. The PRT recommends the following revised Purpose statement for SDT consideration:

> This standard establishes requirements for acquiring necessary data for the Balancing Authority so that balancing of resources and demand can be achieved under Tie-Line Bias Control.

Within the Purpose statement or Applicability section, the PRT also recommends that the SDT consider addressing the Hydro Quebec exception for tie line bias control in some form, or a single-BA exception.

3) **Applicability**: The SDT should remove "Generator Operators", "Transmission Operators", and "Load Serving Entities" as applicable entities unless specificially added into a Standard requirement by the SDT.

4) **Requirement R1**: The PRT recommends that the content of Requirement R1 be split between what is needed for ensuring facilities are within a BA Area prior to MW being generated or consumed, and what is needed for ensuring balanced operation within an Interconnection. First, the PRT recommends that the SDT consider continuing discussions with the FAC SDT moving and restating or clarifying the TOP, LSE, and GOP requirements in a FAC Standard to ensure facilities are within the metered boundaries of a BA prior to transmission operation, resource operation, or load being served. The PRT discussed that the ownership of metering and other factors may drive why the LSE is included in this standard, along with other entities; however, consideration should be given to moving requirements for these facilities to be within a BA Area into a FAC standard. The PRT is concerned that removing any such requirements of the LSE, TOP, and GOP and not reflecting them within another standard may inadvertently transfer certain obligations to the BA to ensure that such loads, resources, and facilities are within the BA's metered boundaries. The SDT should explore whether the role of the TOP would appropriately cover the loads interconnected to that TOP, such that the LSE requirement may not be necessary. Second, the PRT recommends that the SDT revise Requirements R1 and R2 to be BA requirements that all Actual Net Interchange and Scheduled Net Interchange used by the BA in its Reporting ACE

SAR Information

calculation also have an Adjacent BA, as proposed in the redlined Requirements R1 and R2. Note that the PRT does not intend with the proposed language to impose any additional requirements on the BA that currently apply to the LSE, GOP, and TOP, but also believes that the requirements to identify the applicable BA should perhaps be in the interconnection agreements (via FERC's OATT or NAESB, for example) or a FAC requirement. With respect to proposed R2, the SDT should ensure that the requirement cannot be misinterpreted to imply that Dynamic Schedules can only be with physically adjacent BAs. The intent is to address adjacency in a manner consistent with the scheduling path no differently than used for interchange schedules.

5) **Requirement R2**: Retirement approved by FERC effective January 21, 2014.

6) **Requirement R3**: The PRT recommends that the SDT not use the term "Regulation Service," as in general this statement could apply to implementation of Dynamic Schedules or Pseudo-Ties, and the desire to have a common point for the data shared between the BAs implementing the Dynamic Transfer. The PRT recommends removing "adequate" and "Burden" from the requirement. The PRT recommends expanding Requirement R3 to be applicable to the implementation of tie lines, Pseudo-Ties, and Dynamic Schedules, as all require agreement between adjacent BAs on the agreed-upon points to be implemented. The PRT recommends that the SDT review the other standards such as TOP-005 to assure there is no duplication or redundancy. Specific to the concern on swapping hourly values in BAL-005 posted for industry comment. The PRT recommends deleting the proposed R3.2 and the first sentence of the proposed R3.5.2, the PRT also recommends the SDT develop a guideline document to accompany BAL-005 covering some of the suggested best practices.

7) **Requirement R4**: The PRT reviewed Requirement R4 with respect to what notification or coordination is necessary that could be considered with the other requirements in this Standard regarding Interchange. Initially the PRT was considering a recommendation that the SDT consider the requirement as it applies to Dynamic Transfer implementation as discussed in the Dynamic Transfer reliability guideline, and as it applies to the practice of implementing multiple-BA Dynamic Transfers under a process referred to as ACE Diversity Interchange. The PRT also considered recommendations to delete or modify Requirement R4 so that it requires communication with not only the BAs, but any other affected entities, and also to strike "providing Regulation Service." However, after further review, the PRT recommends retiring Requirement R4, as the basis for coordination of common values between adjacent BAs is covered in Requirement R3, and correction of information not available has also been addressed. These requirements should ensure that any failure to perform would be reflected in the BA performance under BAL-001-2.

SAR Information

8) **Requirement R5**: The PRT recommends retiring Requirement R5, as the requirements placed upon the implementation of Dynamic Transfers are covered within Requirement R3. With respect to having a backup plan to the extent that a service may no longer be provided, the PRT believes this would be covered in the terms agreed to between the parties implementing the Dynamic Transfer. As proposed by the PRT, the requirements remaining in BAL-005 would ensure that any failure to perform would be reflected in the BA performance under BAL-001-2.

9) **Requirement R6**: The PRT recommends that the sentence "Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control" be captured in the definition of "Reporting ACE.". The terms used in the Requirement R6 need to be consistent with those used in Reporting ACE if the Requirement is retained. The SDT should consider whether the 30-minute requirement for RC notification is sufficient or excessive. The PRT recommends that if a timing requirement remains in the standard that it be structured in a manner to not require communication with the RC if the capability to calculate Reporting ACE is restored within the defined notification period.

10) **Requirement R7**: The PRT recommends retiring this Requirement under Paragraph 81. The first sentence covers having a functional EMS or other system capable of calculating Reporting ACE and controlling resources, which can be done manually without any detriment to reliability. EOP-008-1 Requirement R1 recognizes that such automated capability may not be available for up to two hours for loss of control center functionality. In addition, the second sentence is not needed, as such actions would be covered under EOP-008. The PRT believes that the term "Operating AGC" in Requirement R7 refers to the capability to continuously calculate ACE (not automatic control of resources), which should be considered one of the BAs functional obligations with regard to the reliable operations and situational awareness of the BES. Though redundancy and other provisions may be in place to maintain EMS functionality, there are times when the information may not be available where the provisions under EOP-008-1 would apply.

11) **Requirement R8**: The PRT recommends that the SDT revise the Requirement with the proper context of a minimum normal scan rate and clarify how frequently all components must be factored into the Reporting ACE equation under normal operation. With respect to the sub-requirements, the SDT should ensure that any proposed revisions accommodate abnormal and emergency operations, including the possibility that the EMS or supporting telemetry may not be available, such as during an evacuation to a backup site. The PRT notes that the SDT should consider a requirement focused on a minimum scan-rate expectation under normal operations, rather than a requirement that could be interpreted as if systems have 100% availability.

SAR Information

12) **Requirement R8, Part 8.1**: The BA should have visibility of system frequency within parameters consistent with EOP-008, however the PRT recommends that the requirement not be prescriptive. The SDT should review EOP-008 to ensure that this requirement is covered there. In addition, the SDT should also consider remote and redundant frequency resources to the extent that the information that is otherwise available to the BA may not be available upon loss of control center functionality. Such capability may already be anticipated under EOP-008. The SDT should consider the following questions in the development of the revised requirement:

    a) How much time is allowed to pass if the redundancy is lost before it must be restored?

    b) Does the PRT believe it is acceptable for the second and independent frequency device to be one used by another Balancing Authority?

13) **Requirement R9, Part 9.1**: The PRT recommends retiring this Requirement. The Actual Net Interchange and Scheduled Net Interchange values in the Reporting ACE calculation include provisions for the Balancing Authority to include its high voltage direct (HVDC) link to another asynchronous interconnection. By assuring the values are handled consistently in the actual and scheduled Interchange terms included in the real-time Reporting ACE by definition, the Balancing Authority is not being instructed "how" to implement the HVDC link, but allowed to decide the method it will use. By focusing on real-time Reporting ACE, we are assuring reliability is addressed and maintained at all times.

14) **Requirement R10 and R11**: The PRT recommends retiring these requirements, as the basics of both requirements are factored into the definition of Scheduled Net Interchange used in the Reporting ACE calculation as defined in the NERC Glossary.

    The PRT noted that Requirement R10 is written as if "Net Scheduled Interchange" is the value used in the ACE equation; however, Net Scheduled Interchange has two meanings – the algebraic sum of all Interchange Schedules across a given path, or between Balancing Authorities for a given period or instant in time. Aside from the concern of having a definition with two different meanings, the PRT believes that neither choice in the definition accurately depicts the value inserted into the ACE or Reporting ACE, which would be the algebraic sum of all Net Scheduled Interchange with all Adjacent Balancing Authorities, including Dynamic Schedules. In addition, the PRT could not find a definition of Scheduled Interchange as used in Requirement R11. Under Section 3 below, the PRT recommends changes to certain NERC definitions.

SAR Information

15) **Requirement R12**: The PRT took a holistic approach to Requirement R12 and other requirements related to the implementation of Tie-Lines, Pseudo-Ties, and Dynamic Schedules, as all relate to the information exchanged between adjacent BAs.

The PRT recommends a new Requirement R3 related to the implementation of Tie-Lines, Pseudo-Ties, and Dynamic Schedules, where each respective Adjacent BA has agreed to common measuring points that produce an agreed-to value to be included in the calculation of Reporting ACE. The SDT should review the requirement as it relates to current practices to ensure the reliability needs are met.

The PRT suggests that the holistic approach shall only be achieved if there is a comprehensive definition of ACE. Therefore, the PRT recommends the ACE and Reporting ACE definitions be reviewed (understanding and identifying as well why there is a difference) to assure that they are comprehensive (including items such as all AC Tie-Lines, Pseudo-ties, and all other necessary Adjacent BA information). The PRT notes that the comprehensive details of the ACE calculation in BAL-001-1 will be retired upon implementation of BAL-001-2, where ACE will only be defined in the NERC Glossary. The PRT suggests that a complete review of all the NERC Standards for use of the term "ACE" is necessary to assure that any update to the ACE definition would not impact any other Standard.

16) **Requirement R13**: The PRT suggests deleting the first sentence of R13, and suggests that the SDT include in a guideline document the practice of performing hourly error checks of the Actual Net Interchange ($NI_{A)}$ operated to for the hour against an end-of-the-hour reference.

The PRT also recommends a separate requirement specific to adjustments as needed to the Reporting ACE to reflect the meter error adjustment. However, the PRT is concerned that requiring correction of a component of ACE when in error (no matter how negligible) would be problematic in that not all errors require correction. The PRT recommends that the SDT consider stating the requirement in such a manner that I_{ME} is required to be zero except during times needed to compensate for any data or equipment error affecting a component of the Reporting ACE calculation (interchange or frequency). When writing the requirement, the SDT should also consider that there are other means of addressing metering corrections besides use of the I_{ME} term, which may include possible revision to real-time metering data. Uses of the I_{ME} term in the Reporting ACE may also be an appropriate subject for the guideline document the PRT is

SAR Information

recommending that the SDT develop to accompany BAL-005 covering some of the suggested best practices.

Requirement R14: The PRT recommends that the SDT delete the first sentence in R14 and revise the second sentence to cover the minimum amount of information expected for the BA to provide in real-time to its operator. The PRT also recommends that the individual components of actual and scheduled interchange with each Adjacent Balancing Authority also be captured (Tie-Lines, Pseudo-Ties, Dynamic Schedules, block schedules as needed for coordination, and real-time schedules). Based on industry comments, the SDT should consider whether this requirement is needed in the BAL standards, whether it is adequately covered elsewhere in the standards, or whether it should be moved to the NERC Rules of Procedure for certification of the Functional Entity.

17) **Requirement R15**: The SDT should consider placing a requirement in a FAC Standard with respect to supporting infrastructure or functionality, or review EOP-008 to determine if existing requirements adequately address primary control center functionality.

18) **Requirement R16**: The PRT recommends moving the requirement for flagging bad data to revisions made in Requirement R14.

19) **Requirement R17**: The PRT recommends that this requirement be written to be specific to the equipment used to determine the frequency component required for Reporting ACE. The PRT also recommends that the SDT move any accuracy requirements applicable to the needs of the Transmission Operator, (which may include MW, MVAR, voltage, potential transformer, current transformer, and remote terminal unit or equivalent) to a TOP or FAC standard. Further study would be needed on the ".25% of full scale" and the "appropriate accuracy" language.

2. BAL-006

The BARC2 PRT has completed its review of BAL-006 and recommends that it be revised. The recommendations below include moving any requirements with implications for real-time operations into BAL-005.

Among other work, the review team considered a FERC directive that recommended the development of a metric to bound the magnitude of inadvertent accumulations, as those accumulations may be indicative of a BA excessively leaning on the resources of others in its Interconnection. The review team

SAR Information

consensus was that an Inadvertent Interchange accumulation value alone cannot yield useful information concerning whether a BA is operating reliably. The PRT document on the consideration of issues and directives more fully covers the PRT recommendations related to the FERC directives. The PRT's recommendations for BAL-006 are fully detailed below.

1) **Purpose**: As the revisions proposed for BAL-006 focus on the minimum requirements for Adjacent Balancing Authorities to agree upon the hourly MW amounts of scheduled and actual Interchange between them, which reinforces that errors in coordination or process will be identified, the PRT recommends that the SDT revise the Purpose statement to be consistent with the Requirements as further developed under the SAR posted with this recommendation.

2) **Requirement R1**: The PRT recommends removing Requirement R1 as written and recommends that the SDT determine if there is merit in developing a reliability metric specific to this standard to measure performance to certain requirements under BAL-006, including the consideration of including the calculation of Inadvertent Interchange. In development of any metric, the PRT recommends that the SDT determine the appropriate time-frame for reliability (as close to real-time as possible). Similar to how BAL-001-2 has CPS1 and BAAL measures dependent upon the BA calculating its Reporting ACE without a stated requirement that "Each BA shall calculate its Reporting ACE", the PRT felt that if the industry supports a measure being developed that uses Inadvertent Interchange in the measure of performance, that the BA would calculate Inadvertent Interchange as needed to comply. Also, similar to the approach taken for defining Reporting ACE in the Glossary with all of the components necessary for the calculation, the PRT is recommending in Requirement R2 below that the definition of Inadvertent Interchange also be updated so that all components necessary for the calculation are identified.

3) **Requirement R2**: The PRT recommends incorporating Requirement R2 into a revised definition of Inadvertent Interchange: The PRT recommends that this definition be modified to capture that the calculation is on an hourly basis and includes the megawatt-hour values for Tie-Lines, Pseudo-Ties, and Dynamic Schedules, along with other scheduled interchange implemented under block scheduling, which does not include the effect of the ramps. The PRT recommends that the definition also include the NERC definitions of On-Peak Accounting and Off-Peak Accounting, which reference the NAESB business practice for inadvertent interchange accounting. The PRT also recommends that the definition clarify the treatment of scheduled and actual interchange associated with asynchronous ties between Interconnections.

4) **Requirement R3**: The PRT recommends incorporating Requirement R3 into BAL-005, as the requirement relates to the agreement on common values used in Real-time and also

SAR Information
recommends developing a guideline to cover the practice of comparing the hourly megawatt-hour values gathered at the end of the hour against the hourly integrated values of the scan-rate data operated to, in order to determine if significant error exists. 5) **Requirement R4**: The SDT should review current practices for confirmation of interchange after-the-fact to determine and justify a shorter duration for agreement on such values for reliability purposes. The PRT also recommends that Requirement R4 be restated to require that the agreement is based upon the aggregate net schedules and net actuals by adjacent BAs as further defined in the new definition of Inadvertent Interchange. In concept, every Tie-Line, Pseudo-Tie, and Interchange Schedule (including Dynamic Schedules) implemented in the Reporting ACE calculation should have an accompanying after-the-fact megawatt-hour value accounted for in the calculation of Inadvertent Interchange. 6) **Requirement R4, Part 4.2**: The SDT should evaluate whether to retire this Requirement, as it is addressed in the new definition of Inadvertent Interchange by the proposed reference to On-Peak Accounting and Off-Peak Accounting. 7) **Requirement R4.3**: The SDT should review this requirement to determine what elements of the requirement are necessary to support reliability. The SDT also should consider including in a guideline document a practice to support providing operations personnel with information on the comparison of monthly revenue class meters to meters used for real-time operation. 8) **Requirement R5**: The SDT should review whether the practice that requires BAs to mutually agree by the 15th calendar day is needed for reliability. The PRT believes there may be merit in requiring BAs to identify the cause of the dispute, and to either correct it within a prescribed number of days, or follow a dispute resolution process. The SDT should ensure that the requirement is clear and distinct, which may require modifying or striking the language regarding dispute resolution.

Reliability Functions	
The Reliability Standards will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☐ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☐ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐ Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐ Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐ Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☐ Transmission Owner	Owns and maintains transmission facilities.
☐ Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☐ Distribution Provider	Delivers electrical energy to the End-use customer.
☐ Generator Owner	Owns and maintains generation facilities.
☐ Generator Operator	Operates generation unit(s) to provide real and reactive power.

Reliability Functions		
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☐	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Reliability Standards.
☒	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Reliability Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A Reliability Standard shall not give any market participant an unfair competitive advantage.	Yes.
2. A Reliability Standard shall neither mandate nor prohibit any specific market structure.	Yes.
3. A Reliability Standard shall not preclude market solutions to achieving compliance with that Reliability Standard.	Yes.

Reliability and Market Interface Principles	
4. A Reliability Standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with Reliability Standards.	Yes.

Related Reliability Standards	
Reliability Standard No.	Explanation
BAL-001-2 and draft BAL-002-2	Some of the proposed revisions to BAL-005 focus on the components used to calculate Reporting ACE, used to measure compliance to CPS1 and BAAL in BAL-001-2, and measure compliance in the draft BAL-002-2 revisions.
EOP-008-1	The purpose of EOP-008-1 is to ensure continued reliable operations of the Bulk Electric System (BES) in the event that a control center becomes inoperable. For certain proposed revisions to BAL-005 in this SAR, the PRT recommends that the SDT consider provisions in EOP-008-1 for the loss of control center functionality.
FAC-001-1	With respect to BAL-005 Requirement R1, the PRT recommends that the SDT consider moving and restating the TOP, LSE, and GOP requirements in an FAC Standard to ensure facilities are within the metered boundaries of a BA prior to transmission operation, resource operation, or load being served. The PRT recommends that the SDT explore whether the role of the TOP would appropriately cover the loads interconnected to that TOP, such that the LSE requirement may not be necessary.
Other	The PRT recommendations include that the ACE and Reporting ACE definitions be reviewed (understanding and identifying as well why there is a difference) to assure that they are comprehensive (including items such as all AC Tie-Lines, Pseudo-ties, and all other necessary Adjacent BA information). As the comprehensive details of the ACE calculation in BAL-001-1 will be retired upon implementation of BAL-001-2, where ACE will only be defined in the NERC Glossary, the PRT suggests that a complete review of all the NERC Standards is necessary to assure where ACE is utilized in a Standard, that any update to the ACE definition would not impact any other Standard.

Related SARs – N/A	
SAR ID	Explanation

Regional Variances – N/A	
Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
RFC	
SERC	
SPP	
WECC	

A. Introduction

1. **Title:** Balancing Authority Control~~Automatic Generation Control~~

2. **Number:** BAL-005-3~~0.2b~~

3. **Purpose:** This standard establishes requirements for acquiring necessary data for the Balancing Authority ~~Automatic Generation Control (AGC) necessary~~ to calculate Reporting ~~Area Control Error (~~ACE~~) and to routinely deploy the Regulating Reserve. The standard also ensures that all facilities and load electrically synchronized to the Interconnection are included within the metered boundary of a Balancing Area~~ so that balancing of resources and demand can be achieved under Tie-Line Bias Control.

4. **Applicability:**

   4.1. Balancing Authorities

   ~~4.2.~~ ~~Generator Operators~~

   ~~4.3.~~ ~~Transmission Operators~~

   ~~4.4.~~ ~~Load Serving Entities~~

5. **Effective Date:** ~~May 13, 2009~~To be determined.

B. Requirements

R1. ~~Only~~Each Balancing Authority shall implement only those Tie-Lines and Pseudo-Ties with A~~a~~djacent Balancing Authorities ~~shall be implemented~~ as Actual Net Interchange ~~Actual~~ in the Reporting ACE. ~~All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.~~

~~R1.1.~~ ~~Each Generator Operator with generation facilities operating in an Interconnection shall ensure that those generation facilities are included within the metered boundaries of a Balancing Authority Area.~~

~~R1.2.~~ ~~Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.~~

~~R1.3.~~ ~~Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.~~

R2. Each Balancing Authority shall implement only those~~Only~~ Interchange Schedules including Dynamic Schedules with A~~a~~djacent Balancing Authorities ~~shall be implemented~~ as Scheduled Net ~~Scheduled~~ Interchange in the Reporting ACE. ~~Each Balancing Authority shall maintain Regulating Reserve that can be controlled by AGC to meet the Control Performance Standard. (Retirement approved by NERC BOT pending applicable regulatory approval.)~~

~~R3.~~ ~~A Balancing Authority providing Regulation Service shall ensure that adequate metering, communications, and control equipment are employed to prevent such service from becoming a Burden on the Interconnection or other Balancing Authority Areas.~~

R3. ~~Adjacent~~ Each Balancing Authorit~~i~~yes shall ensure that ~~adequate metering, communications, and control equipment are employed between them to ensure that~~ common and agreed-upon values are communicated to each~~both~~ applicable adjacent Balancing Authority~~ies~~ for all Tie-Lines, Pseudo-Ties, and ~~Interchange Schedules including~~ Dynamic Schedules~~, even when primary source data is not available~~.

R3.1. A Balancing Authority with a high voltage direct current (HVDC) Tie-Line to another Balancing Authority connected asynchronously to the Interconnection may choose to omit the scheduled and actual Interchange related to the HVDC Tie-Line from the ACE equation if the HVDC Tie-Line is modeled as internal generation or load by both BAs at either end of the Tie-Line.

~~Each Balancing Authority shall perform hourly error checks using Tie-Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment.~~

R3.2. The Balancing Authority shall maintain an I_{ME} equal to zero in its Reporting ACE except during times needed to compensate for any data or equipment error affecting a component of the Reporting ACE calculation (Interchange or frequency). ~~The Balancing Authority shall correct for any component (e.g., Interchange or frequency) of Reporting ACE that is in error or use the interchange meter error (IME) term of the Reporting ACE equation to compensate for any equipment error until repairs can be made~~[HD1].

R3.3. Adjacent Balancing Authorities shall ensure that each Tie-Line, Pseudo-Tie, and Dynamic Schedule between them is equipped with an agreed-upon common source to determine hourly megawatt-hour values. These values shall be provided hourly to each of the Adjacent Balancing Authorities.

R3.4. The Balancing Authority shall ensure that data acquisition for Reporting ACE occur at least every six seconds.

R3.4~~5~~.1. The Balancing Authority shall calculate Reporting ACE at least every six seconds.

R3.4~~5~~.2. ~~Each Balancing Authority shall perform hourly error checks of NA_E using clock-hour accumulations or integrations of Tie-Line megawatt-hour meter readings.~~ The time synchronization of the tie-line MWH meters shall use a common and agreed upon source (e.g., Coordinated Universal Time (UTC[HD2]))

~~**R4.** A Balancing Authority providing Regulation Service shall notify the Host Balancing Authority for whom it is controlling if it is unable to provide the service, as well as any Intermediate Balancing Authorities.~~

~~**R5.** A Balancing Authority receiving Regulation Service shall ensure that backup plans are in place to provide replacement Regulation Service should the supplying Balancing Authority no longer be able to provide this service.~~

~~**R6.**~~**R4.** ~~The Balancing Authority's AGC shall compare total Net Actual Interchange to total Net Scheduled Interchange plus Frequency Bias obligation to determine the Balancing Authority's ACE. Single Balancing Authorities operating asynchronously may employ alternative ACE calculations such as (but not limited to) flat frequency control.~~ If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator.

~~**R7.** The Balancing Authority shall operate AGC continuously unless such operation adversely impacts the reliability of the Interconnection. If AGC has become inoperative, the Balancing Authority shall use manual control to adjust generation to maintain the Net Scheduled Interchange.~~

~~**R7.1.** The Balancing Authority shall ensure that data acquisition for and calculation of ACE occur at least every six seconds.~~

~~**R8.**~~**R5.** Each Balancing Authority shall provide redundant and independent frequency metering equipment that shall automatically activate upon detection of failure of the primary metering source. This overall installation shall provide a minimum availability of 99.95%.

~~**R6.** The Balancing Authority shall include all Interchange Schedules with Adjacent Balancing Authorities in the calculation of Net Scheduled Interchange for the ACE equation.~~

~~**R6.5.** Balancing Authorities with a high voltage direct current (HVDC) link to another Balancing Authority connected asynchronously to their Interconnection may choose to omit the Interchange Schedule related to the HVDC link from the ACE equation if it is modeled as internal generation or load.~~

~~**R7.** The Balancing Authority shall include all Dynamic Schedules in the calculation of Net Scheduled Interchange for the ACE equation.~~

~~**R8.** Balancing Authorities shall include the effect of ramp rates, which shall be identical and agreed to between affected Balancing Authorities, in the Scheduled Interchange values to calculate ACE.~~

~~**R9.** Each Balancing Authority shall include all Tie Line flows with Adjacent Balancing Authority Areas in the ACE calculation.~~

~~**R9.5.** Balancing Authorities that share a tie shall ensure Tie Line MW metering is telemetered to both control centers, and emanates from a common, agreed upon source using common primary metering equipment. Balancing Authorities shall ensure that megawatt-hour data is telemetered or reported at the end of each hour.~~

~~**R9.6.** Balancing Authorities shall ensure the power flow and ACE signals that are utilized for calculating Balancing Authority performance or that are transmitted for Regulation Service are not filtered prior to transmission, except for the Anti-aliasing Filters of Tie Lines.~~

~~**R9.7.** Balancing Authorities shall install common metering equipment where Dynamic Schedules or Pseudo-Ties are implemented between two or more Balancing Authorities to deliver the output of Jointly Owned Units or to serve remote load.~~

~~**R10.** Each Balancing Authority shall perform hourly error checks using Tie Line megawatt-hour meters with common time synchronization to determine the accuracy of its control equipment. The Balancing Authority shall adjust the component (e.g., Tie Line meter) of ACE that is in error (if known) or use the interchange meter error (I_{ME}) term of the ACE equation to compensate for any equipment error until repairs can be made.~~

~~**R11.**~~**R6.** ~~The Balancing Authority shall provide its operating personnel with sufficient instrumentation and data recording equipment to facilitate monitoring of control performance, generation response, and after-the-fact analysis of area performance.~~ As a minimum, the Balancing Authority shall provide its operating personnel with real-time values for ACE, Interconnection frequency and Net Actual Interchange with each Adjacent Balancing Authority Area. The Balancing Authority shall flag missing or bad data for operator display and archival purposes.

~~**R12.**~~**R7.** The Balancing Authority shall provide adequate and reliable backup power supplies and shall periodically test these supplies at the Balancing Authority's control center and other critical locations to ensure continuous operation of AGC and vital data recording equipment during loss of the normal power supply.

~~**R13.** The Balancing Authority shall sample data at least at the same periodicity with which ACE is calculated. The Balancing Authority shall flag missing or bad data for operator display and~~

archival purposes. The Balancing Authority shall collect coincident data to the greatest practical extent, i.e., ACE, Interconnection frequency, Net Actual Interchange, and other data shall all be sampled at the same time.

R14. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25 % of full scale
Remote terminal unit	≤ 0.25 % of full scale
Potential transformer	≤ 0.30 % of full scale
Current transformer	≤ 0.50 % of full scale

The PRT recommends that R17 be written to be specific to the equipment used to determine the frequency component required for Reporting ACE. The PRT also recommends that the SDT recommend moving any accuracy requirements applicable to the needs of the Transmission Operator, which may include MW, MVAR, voltage, potential transformer, current transformer, and remote terminal unit or equivalent to a TOP or FAC standard. Further study would be needed on the ".25% of full scale" and the "appropriate accuracy" language.

C. Measures

Not specified.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Balancing Authorities shall be prepared to supply data to NERC in the format defined below:

1.1.1. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization CPS source data in daily CSV files with time stamped one minute averages of: 1) ACE and 2) Frequency Error.

1.1.2. Within one week upon request, Balancing Authorities shall provide NERC or the Regional Reliability Organization DCS source data in CSV files with time stamped scan rate values for: 1) ACE and 2) Frequency Error for a time period of two minutes prior to thirty minutes after the identified Disturbance.

1.2. Compliance Monitoring Period and Reset Timeframe

Not specified.

1.3. Data Retention

1.3.1. Each Balancing Authority shall retain its ACE, actual frequency, Scheduled Frequency, Net Actual Interchange, Net Scheduled Interchange, Tie Line meter error correction and Frequency Bias Setting data in digital format at the same scan rate at which the data is collected for at least one year.

1.3.2. Each Balancing Authority or Reserve Sharing Group shall retain documentation of the magnitude of each Reportable Disturbance as well as

the ACE charts and/or samples used to calculate Balancing Authority or Reserve Sharing Group disturbance recovery values. The data shall be retained for one year following the reporting quarter for which the data was recorded.

1.4. Additional Compliance Information

Not specified.

2. Levels of Non-Compliance

Not specified.

E. Regional Differences

None identified.

F. Associated Documents

1. Appendix 1 — Interpretation of Requirement R17 (February 12, 2008).

Version History

Version	Date	Action	Change Tracking
0	February 8, 2005	Adopted by NERC Board of Trustees	New
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
0a	December 19, 2007	Added Appendix 1 – Interpretation of R17 approved by BOT on May 2, 2007	Addition
0a	January 16, 2008	Section F: added "1."; changed hyphen to "en dash." Changed font style for "Appendix 1" to Arial	Errata
0b	February 12, 2008	Replaced Appendix 1 – Interpretation of R17 approved by BOT on February 12, 2008 (BOT approved retirement of Interpretation included in BAL-005-0a)	Replacement
0.1b	October 29, 2008	BOT approved errata changes; updated version number to "0.1b"	Errata
0.1b	May 13, 2009	FERC approved – Updated Effective Date	Addition
0.2b	March 8, 2012	Errata adopted by Standards Committee; (replaced Appendix 1 with the FERC-approved revised interpretation of R17 and corrected standard version referenced in Interpretation by changing from "BAL-005-1" to "BAL-005-0)	Errata
0.2b	September 13, 2012	FERC approved – Updated Effective Date	Addition
0.2b	February 7, 2013	R2 and associated elements approved by NERC Board of Trustees for retirement as part of the Paragraph 81 project (Project 2013-02) pending applicable regulatory approval.	

Appendix 1

Effective Date: August 27, 2008 (U.S.)

Interpretation of BAL-005-0 Automatic Generation Control, R17

Request for Clarification received from PGE on July 31, 2007

PGE requests clarification regarding the measuring devices for which the requirement applies, specifically clarification if the requirement applies to the following measuring devices:

- *Only equipment within the operations control room*
- *Only equipment that provides values used to calculate AGC ACE*
- *Only equipment that provides values to its SCADA system*
- *Only equipment owned or operated by the BA*
- *Only to new or replacement equipment*
- *To all equipment that a BA owns or operates*

BAL-005-0

R17. Each Balancing Authority shall at least annually check and calibrate its time error and frequency devices against a common reference. The Balancing Authority shall adhere to the minimum values for measuring devices as listed below:

Device	Accuracy
Digital frequency transducer	≤ 0.001 Hz
MW, MVAR, and voltage transducer	≤ 0.25% of full scale
Remote terminal unit	≤ 0.25% of full scale
Potential transformer	≤ 0.30% of full scale
Current transformer	≤ 0.50% of full scale

Existing Interpretation Approved by Board of Trustees May 2, 2007

BAL-005-0, Requirement 17 requires that the Balancing Authority check and calibrate its control room time error and frequency devices against a common reference at least annually. The requirement to "annually check and calibrate" does not address any devices outside of the operations control room.

The table represents the design accuracy of the listed devices. There is no requirement within the standard to "annually check and calibrate" the devices listed in the table, unless they are included in the control center time error and frequency devices.

Interpretation provided by NERC Frequency Task Force on September 7, 2007 and Revised on November 16, 2007

As noted in the existing interpretation, BAL-005-0 Requirement 17 applies only to the time error and frequency devices that provide, or in the case of back-up equipment may provide, input into the reporting or compliance ACE equation or provide real-time time error or frequency information to the system operator. Frequency inputs from other sources that are for reference only are excluded. The time error and frequency measurement devices may not necessarily be located in the system operations control room or owned by the Balancing Authority; however the Balancing Authority has the responsibility for the

accuracy of the frequency and time error measurement devices. No other devices are included in R 17. The other devices listed in the table at the end of R17 are for reference only and do not have any mandatory calibration or accuracy requirements.

New or replacement equipment that provides the same functions noted above requires the same calibrations. Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy.

A. Introduction

1. **Title:** **Inadvertent Interchange**

2. **Number:** BAL-006-2

3. **Purpose:**

   This standard defines a process for monitoring Balancing Authorities to ensure that, over the long term, Balancing Authority Areas do not excessively depend on other Balancing Authority Areas in the Interconnection for meeting their demand or Interchange obligations.

4. **Applicability:**

   4.1. Balancing Authorities.

5. **Effective Date:** First day of first calendar quarter after applicable regulatory approval, or in those jurisdictions where no regulatory approval is required, first day of first calendar quarter after Board of Trustees adoption.

Note that as the revisions proposed for BAL-006 focus on the minimum requirements for Adjacent Balancing Authorities to agree upon the hourly MW amounts of scheduled and actual Interchange between them, which reinforces that errors in coordination or process will be identified, the PRT recommends that the SDT revise the Purpose statement to be consistent with the Requirements as further developed under the SAR posted with this proposed redline.

B. Requirements

~~**R1.** Each Balancing Authority shall calculate and record hourly Inadvertent Interchange. (*Violation Risk Factor: Lower*)~~

~~**R2.** Each Balancing Authority shall include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. The Balancing Authority shall take into account interchange served by jointly owned generators. (*Violation Risk Factor: Lower*)~~

~~**R3.** Each Balancing Authority shall ensure all of its Balancing Authority Area interconnection points are equipped with common megawatt-hour meters, with readings provided hourly to the control centers of Adjacent Balancing Authorities. (*Violation Risk Factor: Lower*)~~

~~**R4.** Adjacent Balancing Authority Areas shall operate to a common Net Interchange Schedule and Actual Net Interchange value and shall record these hourly quantities, with like values but opposite sign. Each Balancing Authority shall compute its Inadvertent Interchange based on the following: (*Violation Risk Factor: Lower*)~~

~~**R5.**~~**R1.** Each Balancing Authority~~, by the end of the next business day,~~ shall agree with its Adjacent Balancing Authorities by the end of the next business day ~~to~~on: (*Violation Risk Factor: Lower*)

~~**R5.1.**~~**R1.1.** The hourly values of Net Interchange Schedule. (*Violation Risk Factor: Lower*)

~~**R5.2.**~~**R1.2.** The hourly integrated megawatt-hour values of Net Actual Interchange. (*Violation Risk Factor: Lower*)

~~**R6.**~~**R2.** Each Balancing Authority shall use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month. (*Violation Risk Factor: Lower*)

~~**R7.**~~**R3.** ~~A~~Each Balancing Authority shall make after-the-fact corrections to the agreed-to daily and monthly accounting data only as needed to reflect actual operating conditions (e.g. a meter being used for control was sending bad data). Changes or corrections based on non-reliability considerations shall not be reflected in the Balancing Authority's Inadvertent Interchange. After-the-fact corrections to scheduled or actual values will not be accepted without agreement of the Adjacent Balancing Authority(ies). (*Violation Risk Factor: Lower*)

R4. Adjacent Balancing Authorities that cannot mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities by the 15th calendar day of the following month shall, for the purposes of dispute resolution, submit a report to their respective Regional Reliability Organization Survey Contact.

~~R7.1.~~R4.1. The report shall describe the nature and the cause of the dispute as well as a process for correcting the discrepancy. (*Violation Risk Factor: Lower*)

C. Measures

None specified.

D. Compliance

1. Compliance Monitoring Process

1.1. Each Balancing Authority shall submit a monthly summary of Inadvertent Interchange. These summaries shall not include any after-the-fact changes that were not agreed to by the Source Balancing Authority, Sink Balancing Authority and all Intermediate Balancing Authority(ies).

1.2. Inadvertent Interchange summaries shall include at least the previous accumulation, net accumulation for the month, and final net accumulation, for both the On-Peak and Off-Peak periods.

1.3. Each Balancing Authority shall submit its monthly summary report to its Regional Reliability Organization Survey Contact by the 15th calendar day of the following month.

1.4. Each Balancing Authority shall perform an Area Interchange Error (AIE) Survey as requested by the NERC Operating Committee to determine the Balancing Authority's Interchange error(s) due to equipment failures or improper scheduling operations, or improper AGC performance.

1.5. Each Regional Reliability Organization shall prepare a monthly Inadvertent Interchange summary to monitor the Balancing Authorities' monthly Inadvertent Interchange and all-time accumulated Inadvertent Interchange. Each Regional Reliability Organization shall submit a monthly accounting to NERC by the 22nd day following the end of the month being summarized.

2. Violation Severity Levels

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	Each Balancing Authority failed to calculate and record hourly Inadvertent Interchange.
R2.	N/A	N/A	The Balancing Authority failed to include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. OR Failed to take into account interchange served by jointly owned generators.	The Balancing Authority failed to include all AC tie lines that connect to its Adjacent Balancing Authority Areas in its Inadvertent Interchange account. AND Failed to take into account interchange served by jointly owned generators.
R3.	N/A	N/A	N/A	The Balancing Authority failed to ensure all of its Balancing Authority Area interconnection points are equipped with common megawatt-hour meters, with readings provided hourly to the control centers of Adjacent Balancing Authorities.
R4.	The Balancing Authority failed to record Actual Net Interchange values that are equal but opposite in sign to its Adjacent Balancing Authorities.	The Balancing Authority failed to compute Inadvertent Interchange.	The Balancing Authority failed to operate to a common Net Interchange Schedule that is equal but opposite to its Adjacent Balancing Authorities.	N/A
R4.1.	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				values of Net Interchanged Schedule. AND The hourly integrated megawatt-hour values of Net Actual Interchange.
R4.1.1.	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly values of Net Interchanged Schedule.
R4.1.2.	N/A	N/A	N/A	The Balancing Authority, by the end of the next business day, failed to agree with its Adjacent Balancing Authorities to the hourly integrated megawatt-hour values of Net Actual Interchange.
R4.2.	N/A	N/A	N/A	The Balancing Authority failed to use the agreed-to daily and monthly accounting data to compile its monthly accumulated Inadvertent Interchange for the On-Peak and Off-Peak hours of the month.
R4.3.	N/A	N/A	N/A	The Balancing Authority failed to make after-the-fact corrections to the agreed-to daily and monthly accounting data to reflect actual operating conditions or changes or corrections based on non-reliability considerations were reflected in the

R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Balancing Authority's Inadvertent Interchange.
R5.	Adjacent Balancing Authorities that could not mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities, submitted a report to their respective Regional Reliability Organizations Survey Contact describing the nature and the cause of the dispute but failed to provide a process for correcting the discrepancy.	Adjacent Balancing Authorities that could not mutually agree upon their respective Net Actual Interchange or Net Scheduled Interchange quantities by the 15th calendar day of the following month, failed to submit a report to their respective Regional Reliability Organizations Survey Contact describing the nature and the cause of the dispute as well as a process for correcting the discrepancy.	N/A	N/A

E. Regional Differences

1. Inadvertent Interchange Accounting Waiver approved by the Operating Committee on March 25, 2004includes SPP effective May 1, 2006.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed "Proposed" from Effective Date	Errata
1	April 6, 2006	Added following to "Effective Date:" This standard will expire for one year beyond the effective date or when replaced by a new version of BAL-006, whichever comes first.	Errata
2	November 5, 2009	Added approved VRFs and VSLs to document. Removed MISO from list of entities with an Inadvertent Interchange Accounting Waiver (Project 2009-18).	Revision
2	November 5, 2009	Approved by the Board of Trustees	
2	January 6, 2011	Approved by FERC	

Team Roster

Project 2010-14.2 BARC Phase 2 Periodic Review Team

	Participant	Entity
Chair	Doug Hils	Duke Energy
Vice Chair	Thomas W. (Tom) Siegrist	Brickfield Burchette Ritts and Stone, PC
Member	Scott Brooks	Manitoba Hydro
Member	Ron Carlsen	Southern Company
Member	Howard F. Illian	Energy Mark, Inc.
Member	Mike Potishnak	Representing NPCC
Member	Jerry Rust	Northwest Power Pool
Member	Robert Staton	Xcel Energy
Member	Glenn Stephens	Santee Cooper
Member	Stephen Swan	MISO
Member	Mark Trumble	Omaha Public Power District
NERC Staff	Sean Cavote (Lead Standards Developer)	NERC
NERC Staff	Laura Anderson (Supporting Standards Developer)	NERC
NERC Staff	Stephen Crutchfield (Supporting Standards Developer)	NERC
NERC Staff	Mallory Huggins (Supporting Standards Developer)	NERC
NERC Staff	Laura Hussey (Director of Standards Development)	NERC

PMOS	Ken Goldsmith	Alliant Energy Corp. Services, Inc.
FERC	Syed Ahmad	Federal Energy Regulatory Commission

Agenda Item 8
Standards Committee
June 10, 2014

Dispersed Generation Resources Project

Action

Authorize the posting of two of three Project 2014-01 Dispersed Generation Resources "high priority" Reliability Standards (PRC-005-2(X), PRC-005-3(X), PRC-005-X(X), VAR-002-2b(X), and VAR-002-4)[1] and Implementation Plans for an initial 45-day formal comment period with ballot pool formation during the first 30 days and initial during the last 10 days of the comment period.

Background

On January 29, 2014, the Standards Committee (SC) seated 11 members to the Project 2014-01 Standard Drafting Team (SDT). The roster is available here. The goal of the NERC Project 2014-01 Standards Applicability for Dispersed Power Producing Resources SDT is to ensure that the Generator Owners (GOs) and Generator Operators (GOPs) of dispersed generation resources are appropriately assigned responsibility for requirements that impact the reliability of the Bulk Power System (BPS), as the characteristics of operating dispersed generation resources can be unique. In light of the revised BES definition approved by the Federal Energy Regulatory Commission (FERC) in 2014, the intent of this effort is generally to maintain the status quo for applicability of the standards as they have been applied over time with respect to dispersed generation resources, where the status quo does not create a reliability gap.

The SDT performed a review of all standards that apply to GOs and/or GOPs and categorized how each standard should be applied to dispersed generation resources to accomplish the reliability purpose of the standard. The SDT developed a draft white paper to explain its approach, and the white paper was posted on April 17, 2014 for an informal comment period. The feedback received on the whitepaper allowed the SDT to refine its approach and finalize revisions to the standards. As explained in the white paper, the team placed standards in the following categories:

- The existing standard language was appropriate when applied to dispersed generating resources and does not need to be addressed;
- The existing standard language was appropriate when applied to dispersed generating resources but additional NERC guidance documentation is needed to clarify how to implement the requirements for dispersed generating resources; and
- The existing standard language needs to be modified in order to account for the unique characteristics of dispersed generation resources. This could be accomplished through the applicability section of the standard in most cases or, if required, through changes to the individual requirements.

[1] The SDT has prepared applicability revisions for relevant versions of PRC-004 – the third high-priority standard – which will be quality reviewed separately and sent to the Standards Committee to authorize posting after the current comment period and ballot of that standard in Project 2010-05.1 ends.

The SDT further categorized revisions to standards as high, medium, or low priority on the basis of how necessary clarifying the applicability to dispersed generation resources was to support timely implementation of the revised definition of Bulk Electric System. The standards included in this authorization are those the team has designated as high priority. Further evaluation is needed of the medium and l.

Because the revisions to the standards are very limited, NERC staff and the PMOS liaison for the project conducted a narrowly focused quality review, focused on consistency and clarity of language that was added or changed to address applicability of the standard to dispersed generation resources. Please also note that no VRFs or VSLs were revised in the standards, so non-binding polls will not be conducted.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment November 20 – December 19, 2013.

Description of Current Draft

This version of PRC-005 contains revisions to thea pplicability of the Standard intended to clarify application of its Requirements to Bulk Electric System dispersed power producing resources. PRC-005-3, a subsequent version of PRC-005, has been adopted by the NERC Board of Trustees and is pending regulatory approval. Depending on the timing of regulatory approval, this interim version, which has been labeled PRC-005-2(X) for balloting purposes, may be filed for regulatory approval. The Protection System Maintenance and Testing Standard Drafting Team (PSMT SDT) is concurrently making technical revisions to PRC-005 in Project 2007-17.3 to address FERC directives. Project 2014-01 does not have in its scope any technical content changes beyond revising the applicability to ensure consistent application of the Requirements of PRC-005 to dispersed power-producing resources.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Initial Ballot	June – July 2014
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	August – September 2014
Final ballot	October 2014
BOT adoption	November 2014

When this standard has received ballot approval, the text boxes within the Applicability section of the Standard will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: **Protection System Maintenance**

2. Number: PRC-005- X

3. Purpose: To document and implement programs for the maintenance of all Protection Systems affecting the reliability of the Bulk Electric System (BES) so that these Protection Systems are kept in working order.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner

4.1.2 Generator Owner

4.1.3 Distribution Provider

4.2. Facilities:

4.2.1 Protection Systems that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)

4.2.2 Protection Systems used for underfrequency load-shedding systems installed per ERO underfrequency load-shedding requirements.

4.2.3 Protection Systems used for undervoltage load-shedding systems installed to prevent system voltage collapse or voltage instability for BES reliability.

4.2.4 Protection Systems installed as a Special Protection System (SPS) for BES reliability.

The only revisions made to this version of PRC-005 are revisions to section 4.2, to clarify applicability of the Requirements of the standard at generator Facilities. These applicability revisions are intended to clarify and provide for consistent application of the Requirements to BES generator Facilities included in the BES through Inclusion I4 – Dispersed Power Producing Resources.

This version is labeled PRC-005-2(X) for balloting purposes. The 'X' indicates that a version number will be applied at a later time, because multiple versions of PRC-005 are in development to reflect the fact that applicability changes need apply for versions of the standard that are approved (PRC-005-2), pending regulatory approval (PRC-005-3), and in development in Project 2007-17.3. Depending on the timing of approvals of other versions, NERC may file this interim version to provide regulatory certainty for entities as the revised BES definition is implemented.

4.2.5 Protection Systems for the following BES generator Facilities for generators not identified through Inclusion I4 of the BES definition:

4.2.5.1 Protection Systems that act to trip the generator either directly or via lockout or auxiliary tripping relays.

4.2.5.2 Protection Systems for generator step-up transformers for generators that are part of the BES.

Rationale for 4.2.5: In order to differentiate between typical BES generator Facilities and BES generators at dispersed power producing facilities, section 4.2.5 was separated into two sections (4.2.5 and 4.2.6). The applicability to non-dispersed power producing Facilities has been maintained and can be found in 4.2.5. The applicability to dispersed power producing Facilities has been modified and relocated from 4.2.5 to 4.2.6.

4.2.5.3 Protection Systems for station service or excitation transformers connected to the generator bus of generators which are part of the BES, that act to trip the generator either directly or via lockout or tripping auxiliary relays.

4.2.6 Protection Systems for the following BES generator Facilities for dispersed power producing resources identified through Inclusion I4 of the BES definition:

4.2.6.1 Protection Systems for Facilities used in aggregating dispersed BES generation from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above.

Rationale for 4.2.6: Applicability of the Requirements of PRC-005-2 to dispersed power producing resources is separated out in section 4.2.6. The intent is that for such resources, the Requirements would applyonly to Protection Systems on equipment used in aggregating the BES dispersed power producing resources from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or higher including the Protection Systems for those transformers used in aggregating generation.

5. Effective Date: See Implementation Plan.

B. Requirements

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a Protection System Maintenance Program (PSMP) for its Protection Systems identified in Section 4.2. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

The PSMP shall:

1.1. Identify which maintenance method (time-based, performance-based per PRC-005 Attachment A, or a combination) is used to address each Protection System Component Type. All batteries associated with the station dc supply Component Type of a Protection System shall be included in a time-based program as described in Table 1-4 and Table 3.

1.2. Include the applicable monitored Component attributes applied to each Protection System Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, and Table 3 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System Components.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals in its PSMP shall follow the procedure established in PRC-005 Attachment A to establish and maintain its performance-based intervals. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall maintain its Protection System Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall implement and follow its PSMP for its Protection System Components that are included within the performance-based program(s). *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R5. Each Transmission Owner, Generator Owner, and Distribution Provider shall demonstrate efforts to correct identified Unresolved Maintenance Issues. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

C. Measures

M1. Each Transmission Owner, Generator Owner and Distribution Provider shall have a documented Protection System Maintenance Program in accordance with Requirement R1.

For each Protection System Component Type, the documentation shall include the type of maintenance method applied (time-based, performance-based, or a combination of these maintenance methods), and shall include all batteries associated with the station dc supply Component Types in a time-based program as described in Table 1-4 and Table 3. (Part 1.1)

For Component Types that use monitoring to extend the maintenance intervals, the responsible entity(s) shall have evidence for each protection Component Type (such as manufacturer's specifications or engineering drawings) of the appropriate monitored Component attributes as specified in Tables 1-1 through 1-5, Table 2, and Table 3. (Part 1.2)

M2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals shall have evidence that its current performance-based maintenance program(s) is in accordance with Requirement R2, which may include but is not limited to Component lists, dated maintenance records, and dated analysis records and results.

M3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System Components included within its time-based program in accordance with Requirement R3. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance intervals in accordance with Requirement R2 shall have evidence that it has implemented the Protection System Maintenance Program for the Protection System Components included in its performance-based program in accordance with Requirement R4. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence that it has undertaken efforts to correct identified Unresolved Maintenance Issues in accordance with Requirement R5. The evidence may include but is not limited to work orders, replacement Component orders, invoices, project schedules with completed milestones, return material authorizations (RMAs) or purchase orders.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards

1.2. Compliance Monitoring and Enforcement Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.3. Evidence Retention

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

The Transmission Owner, Generator Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

For Requirement R1, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep its current dated Protection System Maintenance Program, as well as any superseded versions since the preceding compliance audit, including the documentation that specifies the type of maintenance program applied for each Protection System Component Type.

For Requirement R2, Requirement R3, Requirement R4, and Requirement R5, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the two most recent performances of each distinct maintenance activity for the Protection System Component, or all performances of each distinct maintenance activity for the Protection System Component since the previous scheduled audit date, whichever is longer.

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

1.4. Additional Compliance Information

None.

2. Violation Severity Levels

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The responsible entity's PSMP failed to specify whether one Component Type is being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1) OR The responsible entity's PSMP failed to include applicable station batteries in a time-based program. (Part 1.1)	The responsible entity's PSMP failed to specify whether two Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1)	The responsible entity's PSMP failed to include the applicable monitoring attributes applied to each Protection System Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, and Table 3 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System Components. (Part 1.2).	The responsible entity failed to establish a PSMP. OR The responsible entity failed to specify whether three or more Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1).
R2	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within three years.	NA	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within four years.	The responsible entity uses performance-based maintenance intervals in its PSMP but: 1) Failed to establish the technical justification described within Requirement R2 for the initial use of the performance-based PSMP OR 2) Failed to reduce Countable Events to no more than 4% within five years OR 3) Maintained a Segment with less than 60 Components OR 4) Failed to: • Annually update the list of Components, OR

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Annually perform maintenance on the greater of 5% of the segment population or 3 Components, OR • Annually analyze the program activities and results for each Segment.
R3	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain 5% or less of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.	For Protection System Components included within a time-based maintenance program, the responsible entity failed to maintain more than 15% of the total Components included within a specific Protection System Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, and Table 3.
R4	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain 5% or less of the annual scheduled maintenance for a specific Protection System Component Type in accordance with their performance-based PSMP.	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the annual scheduled maintenance for a specific Protection System Component Type in accordance with their performance-based PSMP.	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the annual scheduled maintenance for a specific Protection System Component Type in accordance with their performance-based PSMP.	For Protection System Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 15% of the annual scheduled maintenance for a specific Protection System Component Type in accordance with their performance-based PSMP.
R5	The responsible entity failed to undertake efforts to correct 5 or	The responsible entity failed to undertake efforts to correct greater than 5, but less than or equal to 10	The responsible entity failed to undertake efforts to correct greater than 10, but less than or equal to 15	The responsible entity failed to undertake efforts to correct greater

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
	fewer identified Unresolved Maintenance Issues.	identified Unresolved Maintenance Issues.	identified Unresolved Maintenance Issues.	than 15 identified Unresolved Maintenance Issues.

E. Regional Variances

None

F. Supplemental Reference Document

The following documents present a detailed discussion about determination of maintenance intervals and other useful information regarding establishment of a maintenance program.

1. PRC-005-2 Protection System Maintenance Supplementary Reference and FAQ — July 2012.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. 3. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/05
1a	February 17, 2011	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers	Project 2009-17 interpretation
1a	February 17, 2011	Adopted by Board of Trustees	
1a	September 26, 2011	FERC Order issued approving interpretation of R1 and R2 (FERC's Order is effective as of September 26, 2011)	
1.1a	February 1, 2012	Errata change: Clarified inclusion of generator interconnection Facility in Generator Owner's responsibility	Revision under Project 2010-07
1b	February 3, 2012	FERC Order issued approving interpretation of R1, R1.1, and R1.2 (FERC's Order dated March 14, 2012). Updated version from 1a to 1b.	Project 2009-10 Interpretation
1.1b	April 23, 2012	Updated standard version to 1.1b to reflect FERC approval of PRC-005-1b.	Revision under Project 2010-07

Version	Date	Action	Change Tracking
1.1b	May 9, 2012	PRC-005-1.1b was adopted by the Board of Trustees as part of Project 2010-07 (GOTO).	
2	November 7, 2012	Adopted by Board of Trustees	Complete revision, absorbing maintenance requirements from PRC-005-1b, PRC-008-0, PRC-011-0, PRC-017-0
2	October 17, 2013	Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase "or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;" to the second sentence under the "Retirement of Existing Standards" section.	
2	December 19, 2013	FERC Order issued approving PRC-005-2. (The enforcement date for PRC-005-2 will be April 1, 2015, which is the first date entities must be compliant with part of the standard. The implementation plan for PRC-005-2 includes specific compliance dates and timeframes for each of the Requirements. The regulatory approval date in the U.S. is February 24, 2014.	
TBD (balloted as 2(X)	TBD	Standard revised in Project 2014-01	Applicability section revised to clarify application of Requirements to BES dispersed power producing resources

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[1]**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 calendar years	For all unmonitored relays: • Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (see Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. • Alarming for power supply failure (see Table 2).	12 calendar years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.

[1] For the tables in this standard, a calendar year starts on the first day of a new year (January 1) after a maintenance activity has been completed. For the tables in this standard, a calendar month starts on the first day of the first month after a maintenance activity has been completed.

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[1]**	**Maintenance Activities**
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2).	12 calendar years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 1-2 Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.	4 calendar months	Verify that the communications system is functional.
	6 calendar years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2).	12 calendar years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with all of the following: • Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation). (See Table 2) • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).	12 calendar years	Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the Protection System

Table 1-3 Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage and current sensing devices not having monitoring attributes of the category below.	12 calendar years	Verify that current and voltage signal values are provided to the protective relays.
Voltage and Current Sensing devices connected to microprocessor relays with AC measurements are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2).	No periodic maintenance specified	None.

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply using **Vented Lead-Acid (VLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack
	18 Calendar Months -or- 6 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(b)

Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3)

Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).

Component Attributes	Maximum Maintenance Interval	Maintenance Activities
Protection System Station dc supply **with Valve Regulated Lead-Acid (VRLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	6 Calendar Months	Inspect: • Condition of all individual units by measuring battery cell/unit internal ohmic values.
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Physical condition of battery rack
	6 Calendar Months -or- 3 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **Nickel-Cadmium (NiCad) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells. • Physical condition of battery rack
	6 Calendar Years	Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(d) Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System station dc supply not using a battery and not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	18 Calendar Months	Inspect: Condition of non-battery based dc supply
	6 Calendar Years	Verify that the dc supply can perform as manufactured when ac power is not present.

Table 1-4(e) Component Type – Protection System Station dc Supply for non-BES Interrupting Devices for SPS, non-distributed UFLS, and non-distributed UVLS systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a SPS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).	When control circuits are verified (See Table 1-5)	Verify Station dc supply voltage.

Table 1-4(f) Exclusions for Protection System Station dc Supply Monitoring Devices and Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2).	No periodic maintenance specified	No periodic verification of station dc supply voltage is required.
Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2).		No periodic inspection of the electrolyte level for each cell is required.
Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2).		No periodic inspection of unintentional dc grounds is required.
Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2).		No periodic verification of float voltage of battery charger is required.
Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2).		No periodic verification of the battery continuity is required.
Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2).		No periodic verification of the intercell and terminal connection resistance is required.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2).		No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2).		No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required.

Table 1-5 Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3) **Note:** Table requirements apply to all Control Circuitry Components of Protection Systems, and SPSs except as noted.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry).	6 calendar years	Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device.
Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 calendar years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with SPS.	12 calendar years	Verify all paths of the control circuits essential for proper operation of the SPS.
Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays.	12 calendar years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with protective functions and/or SPS whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

Table 2 – Alarming Paths and Monitoring In Tables 1-1 through 1-5 and Table 3, alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any alarm path through which alarms in Tables 1-1 through 1-5 and Table 3 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the "Alarm Path with monitoring" category below. Alarms are reported within 24 hours of detection to a location where corrective action can be initiated.	12 Calendar Years	Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated.
Alarm Path with monitoring: The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated.	No periodic maintenance specified	None.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 calendar years	Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self diagnosis and alarming (See Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. Alarming for power supply failure (See Table 2).	12 calendar years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2).	12 calendar years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Voltage and/or current sensing devices associated with UFLS or UVLS systems.	12 calendar years	Verify that current and/or voltage signal values are provided to the protective relays.
Protection System dc supply for tripping non-BES interrupting devices used only for a UFLS or UVLS system.	12 calendar years	Verify Protection System dc supply voltage.
Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-BES interrupting device trip coils).	12 calendar years	Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic).
Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-BES interrupting device trip coils).	12 calendar years	Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices.
Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-BES interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-BES interrupting devices (excludes non-BES interrupting device trip coils).	No periodic maintenance specified	None.
Trip coils of non-BES interrupting devices in UFLS or UVLS systems.	No periodic maintenance specified	None.

PRC-005 — Attachment A

Criteria for a Performance-Based Protection System Maintenance Program

Purpose: To establish a technical basis for initial and continued use of a performance-based Protection System Maintenance Program (PSMP).

To establish the technical justification for the initial use of a performance-based PSMP:

1. Develop a list with a description of Components included in each designated Segment of the Protection System Component population, with a minimum **Segment** population of 60 Components.
2. Maintain the Components in each Segment according to the time-based maximum allowable intervals established in Tables 1-1 through 1-5 and Table 3 until results of maintenance activities for the Segment are available for a minimum of 30 individual Components of the Segment.
3. Document the maintenance program activities and results for each Segment, including maintenance dates and Countable Events for each included Component.
4. Analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment and develop maintenance intervals.
5. Determine the maximum allowable maintenance interval for each Segment such that the Segment experiences **Countable Events** on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

To maintain the technical justification for the ongoing use of a performance-based PSMP:

1. At least annually, update the list of Protection System Components and Segments and/or description if any changes occur within the Segment.
2. Perform maintenance on the greater of 5% of the Components (addressed in the performance based PSMP) in each Segment or 3 individual Components within the Segment in each year.
3. For the prior year, analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment.
4. Using the prior year's data, determine the maximum allowable maintenance interval for each Segment such that the Segment experiences Countable Events on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.
5. If the Components in a Protection System Segment maintained through a performance-based PSMP experience 4% or more Countable Events, develop, document, and implement an action plan to reduce the Countable Events to less than 4% of the Segment population within 3 years.

Implementation Plan

Project 2014-01 Standards Applicability for Dispersed Power Producing Resources
PRC-005-2(X)

The standard numbers currently include an (X) to indicate the version numbering will be updated. Some standards are open in current projects and others are pending with governmental authorities. As a result, NERC will assign the appropriate version number prior to Board of Trustees adoption.

Standards Involved

Approval:

- PRC-005-2(X) – Protection System Maintenance

Retirement:

- PRC-005-2 – Protection System Maintenance

Prerequisite Approvals:

N/A

Background:

In light of the adoption of a revised "Bulk Electric System" definition by the Board of Trustees (Board), changes to the applicability sections of certain Reliability Standards, including PRC-005, are necessary to align with the implementation of the revised "Bulk Electric System" definition. The Standard Drafting Team (SDT) for Project 2014-01 – Standards Applicability for Dispersed Power Producing Resources has modified the applicability section of certain Generator Owner/Generator Operator requirements to recognize the unique technical and reliability aspects of dispersed generation in order to ensure the applicability of the standards is consistent with the reliable operation of the Bulk-Power System.

Reliability Standard PRC-005-2, with its associated Implementation Plan, was adopted by the NERC Board on November 7, 2012. The SDT has revised the applicability section of PRC-005-2 to align with the revised definition of "Bulk Electric System" in the event that this version of PRC-005 is mandatory and enforceable on the effective date of the revised definition of "Bulk Electric System."

General Considerations:

PRC-005-2(X) is proposed for approval to align the applicability section of PRC-005-2 with the revised definition of "Bulk Electric System." PRC-005-2 may already be retired pursuant to an implementation plan of a successor version of PRC-005 by the time the revised definition of "Bulk Electric System" becomes effective. If this occurs, PRC-005-2(X) will not go into effect.

Effective Date

PRC-005-2(X) shall become effective on the later of the effective date of the revised definition of Bulk Electric System or the first day following the effective date of PRC-005-2.

Retirement of Existing Standards:

PRC-005-2 shall be retired at midnight of the day immediately prior to the effective date of PRC-005-2(X) in the particular jurisdiction in which the revised standard is becoming effective.

Implementation Plan

All aspects of the Implementation Plan for PRC-005-2 will remain applicable to PRC-005-2(X) and are incorporated here by reference.

Cross References

The Implementation Plan for the revised definition of "Bulk Electric System" is available here.

The Implementation Plan for PRC-005-2 is available here.

Standard PRC-005-3(X) — Protection System and Automatic Reclosing Maintenance

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment November 20 – December 19, 2013.

Description of Current Draft

~~The Protection System Maintenance and Testing Standard Drafting Team (PSMT SDT) is posting draft 1 of PRC-005-X for a 45-day comment period and ballot in the last ten days of the comment period under the new Standards Process Manual (Effective: June 26, 2013).~~

~~This draft contains the technical content of the standard.~~ ~~A parallel effort in the~~ The Project 2014-01, Standards Applicability for Dispersed Generation Resources Standards Drafting Team (DGR SDT)~~,~~ ~~will~~ is posting proposed ~~an~~ applicability changes to ~~PRC-005-2 and~~ PRC-005-3 for comment and ballot. This draft contains the DGR SDT's recommended changes within ~~technical content of~~ the standard. Project 2014-01 does not have in its scope any technical content changes beyond revising the applicability to ensure consistent application of the Requirements of PRC-005 to dispersed power-producing resources.

In a parallel effort, the Protection System Maintenance and Testing Standard Drafting Team (PSMT SDT) has posted draft 1 of PRC-005-X for a 45-day comment period, and ballot in the last ten days of the comment period under the new Standards Process Manual (Effective: June 26, 2013).

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Initial Ballot	June – July 2014
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	August – September 2014
Final ballot	October 2014
BOT adoption	November 2014

When this standard has received ballot approval, the text boxes within the Applicability section of the Standard will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: **Protection System and Automatic Reclosing Maintenance**

2. Number: PRC-005-3(X)

3. Purpose: To document and implement programs for the maintenance of all Protection Systems and Automatic Reclosing affecting the reliability of the Bulk Electric System (BES) so that they are kept in working order.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner

4.1.2 Generator Owner

4.1.3 Distribution Provider

4.2. Facilities:

4.2.1 Protection Systems that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)

4.2.2 Protection Systems used for underfrequency load-shedding systems installed per ERO underfrequency load-shedding requirements.

4.2.3 Protection Systems used for undervoltage load-shedding systems installed to prevent system voltage collapse or voltage instability for BES reliability.

4.2.4 Protection Systems installed as a Special Protection System (SPS) for BES reliability.

The only revisions made to this version of PRC-005 are revisions to section 4.2, to clarify applicability of the Requirements of the standard at generator Facilities. These applicability revisions are intended to clarify and provide for consistent application of the Requirements to BES generator Facilities included in the BES through Inclusion I4 – Dispersed Power Producing Resources.

This version is labeled PRC-005-3(X) for balloting purposes. The 'X' indicates that a version number will be applied at a later time, because multiple versions of PRC-005 are in development to reflect the fact that applicability changes need apply for versions of the standard that are approved (PRC-005-2), pending regulatory approval (PRC-005-3), and in development in Project 2007-17.3.

4.2.5 Protection Systems for the following BES generator Facilities ~~that are part of the BES, including~~ for generators not identified through Inclusion I4 of the BES definition:

4.2.5.1 Protection Systems that act to trip the generator either directly or via lockout or auxiliary tripping relays.

4.2.5.2 Protection Systems for generator step-up transformers for generators that are part of the BES.

~~**4.2.5.3** Protection Systems for transformers connecting aggregated generation, where the aggregated generation is part of the BES (e.g., transformers connecting facilities such as wind farms to the BES).~~

~~**4.2.5.4**~~**4.2.5.3** Protection Systems for station service or excitation transformers connected to the generator bus of generators which are part of the BES, that act to trip the generator either directly or via lockout or tripping auxiliary relays.

Rationale for 4.2.5: In order to differentiate between typical BES generator Facilities and BES generators at dispersed power producing facilities, section 4.2.5 was separated into two sections (4.2.5 and 4.2.6). The applicability to non-dispersed power producing Facilities has been maintained and can be found in 4.2.5. The applicability to dispersed power producing Facilities has been modified and relocated from 4.2.5 to 4.2.6.

4.2.6 Protection Systems for the following BES generator Facilities for dispersed power producing resources identified through Inclusion I4 of the BES definition:

4.2.6.1 Protection Systems for ~~electrical equipment~~Facilities used in aggregating dispersed BES generation from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above.

Rationale for 4.2.6: Applicability of the Requirements of PRC-005-2 to dispersed power producing resources is separated out in section 4.2.6. The intent is that for such resources, the Requirements would apply ~~-~~only to Protection Systems on equipment used in aggregating the BES dispersed power producing resources from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or higher including the Protection Systems for those transformers used in aggregating generation.

~~4.2.6~~4.2.7 Automatic Reclosing[1], including:

~~4.2.6.1~~4.2.7.1 Automatic Reclosing applied on the terminals of Elements connected to the BES bus located at generating plant substations where the total installed gross generating plant capacity is greater than the gross capacity of the largest BES generating unit within the Balancing Authority Area.

~~4.2.6.2~~4.2.7.2 Automatic Reclosing applied on the terminals of all BES Elements at substations one bus away from generating plants specified in Section 4.2.6.1 when the substation is less than 10 circuit-miles from the generating plant substation.

~~4.2.6.3~~4.2.7.3 Automatic Reclosing applied as an integral part of an SPS specified in Section 4.2.4.

5. Effective Date: See Implementation Plan.

6. Definitions Used in this Standard: The following terms are defined for use only within PRC-005-3, and should remain with the standard upon approval rather than being moved to the Glossary of Terms.

Automatic Reclosing – Includes the following Components:

- Reclosing relay
- Control circuitry associated with the reclosing relay.

Unresolved Maintenance Issue – A deficiency identified during a maintenance activity that causes the component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up corrective action.

Segment – Components of a consistent design standard, or a particular model or type from a single manufacturer that typically share other common elements. Consistent performance is expected across the entire population of a Segment. A Segment must contain at least sixty (60) individual Components.

Component Type – Either any one of the five specific elements of the Protection System definition or any one of the two specific elements of the Automatic Reclosing definition.

Component – A Component is any individual discrete piece of equipment included in a Protection System or in Automatic Reclosing, including but not limited to a protective relay, reclosing relay, or current sensing device. The designation of what constitutes a control circuit

[1] Automatic Reclosing addressed in Section 4.2.6.1 and 4.2.6.2 may be excluded if the equipment owner can demonstrate that a close-in three-phase fault present for twice the normal clearing time (capturing a minimum trip-close-trip time delay) does not result in a total loss of gross generation in the Interconnection exceeding the gross capacity of the largest BES generating unit within the Balancing Authority Area where the Automatic Reclosing is applied.

Component is dependent upon how an entity performs and tracks the testing of the control circuitry. Some entities test their control circuits on a breaker basis whereas others test their circuitry on a local zone of protection basis. Thus, entities are allowed the latitude to designate their own definitions of control circuit Components. Another example of where the entity has some discretion on determining what constitutes a single Component is the voltage and current sensing devices, where the entity may choose either to designate a full three-phase set of such devices or a single device as a single Component.

Countable Event – A failure of a Component requiring repair or replacement, any condition discovered during the maintenance activities in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 which requires corrective action or a Protection System Misoperation attributed to hardware failure or calibration failure. Misoperations due to product design errors, software errors, relay settings different from specified settings, Protection System Component or Automatic Reclosing configuration or application errors are not included in Countable Events.

B. Requirements

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a Protection System Maintenance Program (PSMP) for its Protection Systems and Automatic Reclosing identified in Facilities Section 4.2. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

The PSMP shall:

1.1. Identify which maintenance method (time-based, performance-based per PRC-005 Attachment A, or a combination) is used to address each Protection System and Automatic Reclosing Component Type. All batteries associated with the station dc supply Component Type of a Protection System shall be included in a time-based program as described in Table 1-4 and Table 3.

1.2. Include the applicable monitored Component attributes applied to each Protection System and Automatic Reclosing Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System and Automatic Reclosing Components.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals in its PSMP shall follow the procedure established in PRC-005 Attachment A to establish and maintain its performance-based intervals. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall maintain its Protection System and Automatic Reclosing Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall implement and follow its PSMP for its Protection System and Automatic Reclosing Components that are included within the performance-based program(s). *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

R5. Each Transmission Owner, Generator Owner, and Distribution Provider shall demonstrate efforts to correct identified Unresolved Maintenance Issues. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

C. Measures

M1. Each Transmission Owner, Generator Owner and Distribution Provider shall have a documented Protection System Maintenance Program in accordance with Requirement R1.

For each Protection System and Automatic Reclosing Component Type, the documentation shall include the type of maintenance method applied (time-based, performance-based, or a combination of these maintenance methods), and shall include all batteries associated with the station dc supply Component Types in a time-based program as described in Table 1-4 and Table 3. (Part 1.1)

For Component Types that use monitoring to extend the maintenance intervals, the responsible entity(s) shall have evidence for each Protection System and Automatic Reclosing Component Type (such as manufacturer's specifications or engineering drawings) of the appropriate

monitored Component attributes as specified in Tables 1-1 through 1-5, Table 2, Table 3, and Table 4-1 through 4-2. (Part 1.2)

M2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals shall have evidence that its current performance-based maintenance program(s) is in accordance with Requirement R2, which may include but is not limited to Component lists, dated maintenance records, and dated analysis records and results.

M3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System and Automatic Reclosing Components included within its time-based program in accordance with Requirement R3. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance intervals in accordance with Requirement R2 shall have evidence that it has implemented the Protection System Maintenance Program for the Protection System and Automatic Reclosing Components included in its performance-based program in accordance with Requirement R4. The evidence may include but is not limited to dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence that it has undertaken efforts to correct identified Unresolved Maintenance Issues in accordance with Requirement R5. The evidence may include but is not limited to work orders, replacement Component orders, invoices, project schedules with completed milestones, return material authorizations (RMAs) or purchase orders.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Compliance Monitoring and Enforcement Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.3. Evidence Retention

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

The Transmission Owner, Generator Owner, and Distribution Provider shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

For Requirement R1, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep its current dated Protection System Maintenance Program, as well as any superseded versions since the preceding compliance audit, including the documentation that specifies the type of maintenance program applied for each Protection System Component Type.

For Requirement R2, Requirement R3, Requirement R4, and Requirement R5, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the two most recent performances of each distinct maintenance activity for the Protection System or Automatic Reclosing Component, or all performances of each distinct maintenance activity for the Protection System or Automatic Reclosing Component since the previous scheduled audit date, whichever is longer.

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

1.4. Additional Compliance Information

None.

2. Violation Severity Levels

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The responsible entity's PSMP failed to specify whether one Component Type is being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1) OR The responsible entity's PSMP failed to include applicable station batteries in a time-based program. (Part 1.1)	The responsible entity's PSMP failed to specify whether two Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1)	The responsible entity's PSMP failed to specify whether three Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1). OR The responsible entity's PSMP failed to include the applicable monitoring attributes applied to each Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Components. (Part 1.2).	The responsible entity failed to establish a PSMP. OR The responsible entity's PSMP failed to specify whether four or more Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (Part 1.1).
R2	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within three years.	NA	The responsible entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within four years.	The responsible entity uses performance-based maintenance intervals in its PSMP but: 1) Failed to establish the technical justification described within Requirement R2 for the initial use of the performance-based PSMP OR 2) Failed to reduce Countable Events to no more than 4% within five years OR

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
				3) Maintained a Segment with less than 60 Components OR 4) Failed to: • Annually update the list of Components, OR • Annually perform maintenance on the greater of 5% of the Segment population or 3 Components, OR • Annually analyze the program activities and results for each Segment.
R3	For Components included within a time-based maintenance program, the responsible entity failed to maintain 5% or less of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.	For Components included within a time-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.	For Components included within a time-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.	For Components included within a time-based maintenance program, the responsible entity failed to maintain more than 15% of the total Components included within a specific Component Type, in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, and Tables 4-1 through 4-2.
R4	For Components included within a performance-based maintenance program, the responsible entity failed to maintain 5% or less of the annual scheduled maintenance for a specific	For Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 5% but 10% or less of the annual scheduled	For Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 10% but 15% or less of the annual	For Components included within a performance-based maintenance program, the responsible entity failed to maintain more than 15% of the annual scheduled

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Component Type in accordance with their performance-based PSMP.	maintenance for a specific Component Type in accordance with their performance-based PSMP.	scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP.	maintenance for a specific Component Type in accordance with their performance-based PSMP.
R5	The responsible entity failed to undertake efforts to correct 5 or fewer identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 5, but less than or equal to 10 identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 10, but less than or equal to 15 identified Unresolved Maintenance Issues.	The responsible entity failed to undertake efforts to correct greater than 15 identified Unresolved Maintenance Issues.

E. Regional Variances

None

F. Supplemental Reference Document

The following documents present a detailed discussion about determination of maintenance intervals and other useful information regarding establishment of a maintenance program.

1. PRC-005-2 Protection System Maintenance Supplementary Reference and FAQ — March 2013.
2. Considerations for Maintenance and Testing of Autoreclosing Schemes — November 2012.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. 3. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/05
1a	February 17, 2011	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers	Project 2009-17 interpretation
1a	February 17, 2011	Adopted by Board of Trustees	
1a	September 26, 2011	FERC Order issued approving interpretation of R1 and R2 (FERC's Order is effective as of September 26, 2011)	
1.1a	February 1, 2012	Errata change: Clarified inclusion of generator interconnection Facility in Generator Owner's responsibility	Revision under Project 2010-07
1b	February 3, 2012	FERC Order issued approving interpretation of R1, R1.1, and R1.2 (FERC's Order dated March 14, 2012). Updated version from 1a to 1b.	Project 2009-10 Interpretation
1.1b	April 23, 2012	Updated standard version to 1.1b to reflect FERC approval of PRC-005-1b.	Revision under Project 2010-07

Version	Date	Action	Change Tracking
1.1b	May 9, 2012	PRC-005-1.1b was adopted by the Board of Trustees as part of Project 2010-07 (GOTO).	
2	November 7, 2012	Adopted by Board of Trustees	Project 2007-17 - Complete revision, absorbing maintenance requirements from PRC-005-1.1b, PRC-008-0, PRC-011-0, PRC-017-0
2	October 17, 2013	Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase "or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;" to the second sentence under the "Retirement of Existing	
3	November 7, 2013	Adopted by the NERC Board of Trustees	Revised to address the FERC directive in Order No.758 to include Automatic Reclosing in maintenance programs.
TBD (balloted as 2(X)	TBD	Standard revised in Project 2014-01	Applicability section revised to clarify application of Requirements to BES dispersed power producing resources

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[2]**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	For all unmonitored relays: • Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (see Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. • Alarming for power supply failure (see Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.

[2] For the tables in this standard, a calendar year starts on the first day of a new year (January 1) after a maintenance activity has been completed. For the tables in this standard, a calendar month starts on the first day of the first month after a maintenance activity has been completed.

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[2]**	**Maintenance Activities**
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 1-2 Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.	4 Calendar Months	Verify that the communications system is functional.
	6 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2).	12 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with all of the following: • Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation). (See Table 2) • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).	12 Calendar Years	Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the Protection System

Table 1-3 Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage and current sensing devices not having monitoring attributes of the category below.	12 Calendar Years	Verify that current and voltage signal values are provided to the protective relays.
Voltage and Current Sensing devices connected to microprocessor relays with AC measurements are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2).	No periodic maintenance specified	None.

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply using **Vented Lead-Acid (VLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	18 Calendar Months -or- 6 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **with Valve Regulated Lead-Acid (VRLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	6 Calendar Months	Inspect: • Condition of all individual units by measuring battery cell/unit internal ohmic values.
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Physical condition of battery rack

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	6 Calendar Months -or- 3 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **Nickel-Cadmium (NiCad) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells. • Physical condition of battery rack
	6 Calendar Years	Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(d) Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System station dc supply not using a battery and not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	18 Calendar Months	Inspect: Condition of non-battery based dc supply
	6 Calendar Years	Verify that the dc supply can perform as manufactured when ac power is not present.

Table 1-4(e) Component Type – Protection System Station dc Supply for non-BES Interrupting Devices for SPS, non-distributed UFLS, and non-distributed UVLS systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a SPS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).	When control circuits are verified (See Table 1-5)	Verify Station dc supply voltage.

Table 1-4(f) Exclusions for Protection System Station dc Supply Monitoring Devices and Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2).	No periodic maintenance specified	No periodic verification of station dc supply voltage is required.
Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2).		No periodic inspection of the electrolyte level for each cell is required.
Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2).		No periodic inspection of unintentional dc grounds is required.
Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2).		No periodic verification of float voltage of battery charger is required.
Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2).		No periodic verification of the battery continuity is required.
Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2).		No periodic verification of the intercell and terminal connection resistance is required.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2).		No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2).		No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required.

Table 1-5 Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3) Note: Table requirements apply to all Control Circuitry Components of Protection Systems, and SPSs except as noted.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device.
Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with SPS. (See Table 4-2(b) for SPS which include Automatic Reclosing.)	12 Calendar Years	Verify all paths of the control circuits essential for proper operation of the SPS.
Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays.	12 Calendar Years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with protective functions and/or SPSs whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

Table 2 – Alarming Paths and Monitoring In Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2, alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any alarm path through which alarms in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the "Alarm Path with monitoring" category below. Alarms are reported within 24 hours of detection to a location where corrective action can be initiated.	12 Calendar Years	Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated.
Alarm Path with monitoring: The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated.	No periodic maintenance specified	None.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate. For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self diagnosis and alarming (See Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Voltage and/or current sensing devices associated with UFLS or UVLS systems.	12 Calendar Years	Verify that current and/or voltage signal values are provided to the protective relays.
Protection System dc supply for tripping non-BES interrupting devices used only for a UFLS or UVLS system.	12 Calendar Years	Verify Protection System dc supply voltage.
Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic).
Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices.
Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-BES interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-BES interrupting devices (excludes non-BES interrupting device trip coils).	No periodic maintenance specified	None.
Trip coils of non-BES interrupting devices in UFLS or UVLS systems.	No periodic maintenance specified	None.

Table 4-1 Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Reclosing Relay		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored reclosing relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.
Monitored microprocessor reclosing relay with the following: • Internal self diagnosis and alarming (See Table 2). • Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.

Table 4-2(a) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing Relays that are NOT an Integral Part of an SPS		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Unmonitored Control circuitry associated with Automatic Reclosing that is not an integral part of an SPS.	12 Calendar Years	Verify that Automatic Reclosing, upon initiation, does not issue a premature closing command to the close circuitry.
Control circuitry associated with Automatic Reclosing that is not part of an SPS and is monitored and alarmed for conditions that would result in a premature closing command. (See Table 2)	No periodic maintenance specified	None.

Table 4-2(b) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing Relays that ARE an Integral Part of an SPS		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Close coils or actuators of circuit breakers or similar devices that are used in conjunction with Automatic Reclosing as part of an SPS (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each close coil or actuator is able to operate the circuit breaker or mitigating device.
Unmonitored close control circuitry associated with Automatic Reclosing used as an integral part of an SPS.	12 Calendar Years	Verify all paths of the control circuits associated with Automatic Reclosing that are essential for proper operation of the SPS.
Control circuitry associated with Automatic Reclosing that is an integral part of an SPS whose integrity is monitored and alarmed. (See Table 2)	No periodic maintenance specified	None.

PRC-005 — Attachment A

Criteria for a Performance-Based Protection System Maintenance Program

Purpose: To establish a technical basis for initial and continued use of a performance-based Protection System Maintenance Program (PSMP).

To establish the technical justification for the initial use of a performance-based PSMP:

1. Develop a list with a description of Components included in each designated Segment, with a minimum **Segment** population of 60 Components.
2. Maintain the Components in each Segment according to the time-based maximum allowable intervals established in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 until results of maintenance activities for the Segment are available for a minimum of 30 individual Components of the Segment.
3. Document the maintenance program activities and results for each Segment, including maintenance dates and Countable Events for each included Component.
4. Analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment and develop maintenance intervals.
5. Determine the maximum allowable maintenance interval for each Segment such that the Segment experiences **Countable Events** on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

To maintain the technical justification for the ongoing use of a performance-based PSMP:

1. At least annually, update the list of Components and Segments and/or description if any changes occur within the Segment.
2. Perform maintenance on the greater of 5% of the Components (addressed in the performance based PSMP) in each Segment or 3 individual Components within the Segment in each year.
3. For the prior year, analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment.
4. Using the prior year's data, determine the maximum allowable maintenance interval for each Segment such that the Segment experiences Countable Events on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.
5. If the Components in a Segment maintained through a performance-based PSMP experience 4% or more Countable Events, develop, document, and implement an action plan to reduce the Countable Events to less than 4% of the Segment population within 3 years.

Implementation Plan

Project 2014-01 Standards Applicability for Dispersed Power Producing Resources
PRC-005-3(X)

The standard numbers currently include an (X) to indicate the version numbering will be updated. Some standards are open in current projects and others are pending with governmental authorities. As a result, NERC will assign the appropriate version number prior to Board of Trustees adoption.

Standards Involved

Approval:

- PRC-005-3(X) – Protection System and Automatic Reclosing Maintenance

Retirement:

- PRC-005-2(X) – Protection System Maintenance
- PRC-005-3 – Protection System and Automatic Reclosing Maintenance

Prerequisite Approvals

N/A

Background

In light of the adoption of a revised "Bulk Electric System" definition by the Board of Trustees (Board), changes to the applicability sections of certain Reliability Standards, including PRC-005, are necessary to align with the implementation of the revised "Bulk Electric System" definition. The Standard Drafting Team (SDT) for Project 2014-01 – Standards Applicability for Dispersed Power Producing Resources has modified the applicability section of certain Generator Owner/Generator Operator requirements to recognize the unique technical and reliability aspects of dispersed generation in order to ensure the applicability of the standards is consistent with the reliable operation of the Bulk-Power System.

Reliability Standard PRC-005-3, with its associated Implementation Plan, was adopted by the NERC Board on November 7, 2013. The SDT has revised the applicability section of PRC-005-3 to align with the revised definition of "Bulk Electric System" in the event that this version of PRC-005 is mandatory and enforceable on the effective date of the revised definition of "Bulk Electric System."

General Considerations

PRC-005-3(X) is proposed for approval to align the applicability section of PRC-005-3 with the revised definition of "Bulk Electric System." PRC-005-3 may already be retired pursuant to an Implementation Plan of a successor version of PRC-005 by the time the revised definition of "Bulk Electric System" becomes effective. If this occurs, PRC-005-3(X) will not go into effect.

Effective Date

PRC-005-3(X) shall become effective on the later of the effective date of the revised definition of Bulk Electric System or the first day following the effective date of PRC-005-3.

Retirement of Existing Standards

PRC-005-3 shall be retired at midnight of the day immediately prior to the effective date of PRC-005-3(X) in the particular jurisdiction in which the revised standard is becoming effective.

Implementation Plan

PRC-005-3(X) only modifies the applicability for PRC-005-3. All aspects of the Implementation Plan for PRC-005-3 will remain applicable to PRC-005-3(X) and are incorporated here by reference.

Cross References

The Implementation Plan for the revised definition of "Bulk Electric System" is available here.

The Implementation Plan for PRC-005-3 is available here.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment November 20 – December 19, 2013.

Description of Current Draft

The Project 2014-01, Standards Applicability for Dispersed Generation Resources Standards Drafting Team (DGR SDT) is posting proposed applicability changes to PRC-005-3 for comment and ballot. This draft contains the DGR SDT's recommended changes within the standard, which are intended to clarify application of the Requirements to Bulk Electric System (BES) dispersed power producing resources. Project 2014-01 does not have in its scope any technical content changes beyond revising the applicability to ensure consistent application of the Requirements of PRC-005 to dispersed power-producing resources.

In a parallel effort, the Protection System Maintenance and Testing Standard Drafting Team (PSMT SDT) has posted draft 1 of PRC-005-X for a 45-day comment period, and ballot in the last ten days of the comment period under the new Standards Process Manual (Effective: June 26, 2013).

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Initial Ballot	June – July 2014
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	August – September 2014
Final ballot	October 2014
BOT adoption	November 2014

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms (Glossary) are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, this defined term will be removed from the individual standard and added to the Glossary.

Protection System Maintenance Program (PSMP) — An ongoing program by which Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components are kept in working order and proper operation of malfunctioning components is restored. A maintenance program for a specific Component includes one or more of the following activities:

- Verify — Determine that the Component is functioning correctly.
- Monitor — Observe the routine in-service operation of the Component.
- Test — Apply signals to a Component to observe functional performance or output behavior, or to diagnose problems.
- Inspect — Examine for signs of Component failure, reduced performance or degradation.
- Calibrate — Adjust the operating threshold or measurement accuracy of a measuring element to meet the intended performance requirement.

See Section A.6, Definitions Used in this Standard, for additional definitions that are new or modified for use within this standard.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** **Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance**
2. **Number:** **PRC-005-X**
3. **Purpose:** To document and implement programs for the maintenance of all Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying affecting the reliability of the Bulk Electric System (BES) so that they are kept in working order.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1** Transmission Owner
     - **4.1.2** Generator Owner
     - **4.1.3** Distribution Provider
     - **4.1.4** Balancing Authority
   - **4.2. Facilities:**
     - **4.2.1** Protection Systems and Sudden Pressure Relaying that are installed for the purpose of detecting Faults on BES Elements (lines, buses, transformers, etc.)
     - **4.2.2** Protection Systems used for underfrequency load-shedding systems installed per ERO underfrequency load-shedding requirements.
     - **4.2.3** Protection Systems used for undervoltage load-shedding systems installed to prevent system voltage collapse or voltage instability for BES reliability.
     - **4.2.4** Protection Systems installed as a Special Protection System (SPS) for BES reliability.
     - **4.2.5** Protection Systems for the following BES generator Facilities ~~that are part of the BES, including~~ for generators not identified through Inclusion I4 of the BES definition:

The only revisions made to this version of PRC-005 are revisions to section 4.2, to clarify applicability of the Requirements of the standard at generator Facilities. These applicability revisions are intended to clarify and provide for consistent application of the Requirements to BES generator Facilities included in the BES through Inclusion I4 – Dispersed Power Producing Resources.

This version is labeled PRC-005-~~2(~~X~~)~~ for balloting purposes. The 'X' indicates that a version number will be applied at a later time, because multiple versions of PRC-005 are in development to reflect the fact that applicability changes need applied~~y~~ for versions of the standard that are approved (PRC-005-2), pending regulatory approval (PRC-005-3), and in development in Project 2007-17.3. ~~-~~Depending on the timing of approvals of other versions, NERC may file this interim version to provide regulatory certainty for entities as the revised BES definition is implemented.

4.2.5.1 Protection Systems that act to trip the generator either directly or via lockout or auxiliary tripping relays.

4.2.5.2 Protection Systems and Sudden Pressure Relaying for generator step-up transformers for generators that are part of the BES.

~~**4.2.5.3** Protection Systems for transformers connecting aggregated generation, where the aggregated generation is part of the BES (e.g., transformers connecting facilities such as wind farms to the BES).~~

4.2.5.3 Protection Systems and Sudden Pressure Relaying for station service or excitation transformers connected to the generator bus of generators which are part of the BES, that act to trip the generator either directly or via lockout or tripping auxiliary relays.

Rationale for 4.2.5: In order to differentiate between typical BES generator Facilities and BES generators at dispersed power producing facilities, section 4.2.5 was separated into two sections (4.2.5 and 4.2.6). The applicability to non-dispersed power producing facilities has been maintained and can be found in 4.2.5. The applicability to dispersed power producing Facilities has been modified and relocated from 4.2.5 to 4.2.6.

4.2.6 Protection Systems for the following BES generator Facilities for dispersed power producing resources identified through Inclusion I4 of the BES definition:

4.2.6.1 Protection Systems for ~~electrical equipment~~Facilities~~-~~ used in aggregating dispersed BES generation from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above.

Rationale for 4.2.6: The Facilities listed that are applicable to dispersed power producing facilities are covered within 4.2.6. The intent is to NOT include the individual generating resources in the Protection System Maintenance Program, and as such the Protection Systems within the individual generating resources would not be within the scope of PRC-005. Only Protection Systems on equipment used in aggregating the dispersed BES generation from the point where those resources aggregate to greater than 75MVA to a common point of connection at 100kV would be included in the Protection System Maintenance Program, including the Protection Systems for those transformers used in aggregating generation.

~~4.2.6~~4.2.7 Automatic Reclosing[1], including:

~~4.2.6.1~~4.2.7.1 Automatic Reclosing applied on the terminals of Elements connected to the BES bus located at generating plant substations where the total installed gross generating plant capacity is greater than the gross capacity of the largest BES generating unit within the Balancing Authority Area.

~~4.2.6.2~~4.2.7.2 Automatic Reclosing applied on the terminals of all BES Elements at substations one bus away from generating plants specified in Section 4.2.6.1 when the substation is less than 10 circuit-miles from the generating plant substation.

4.2.6.3. Automatic Reclosing applied as an integral part of an SPS specified in Section 4.2.4.

[1] Automatic Reclosing addressed in Section 4.2.7.1 and 4.2.7.2 may be excluded if the equipment owner can demonstrate that a close-in three-phase fault present for twice the normal clearing time (capturing a minimum trip-close-trip time delay) does not result in a total loss of gross generation in the Interconnection exceeding the gross capacity of the largest BES generating unit within the Balancing Authority Area where the Automatic Reclosing is applied.

5. **Effective Date:** See Implementation Plan.

6. **Definitions Used in this Standard:**

Automatic Reclosing – Includes the following Components:

- Reclosing relay
- Control circuitry associated with the reclosing relay.

Sudden Pressure Relaying – A system that trips an interrupting device(s) to isolate the equipment it is monitoring and includes the following Components:

- Fault pressure relay – a mechanical relay or device that detects rapid changes in gas pressure, oil pressure, or oil flow that are indicative of Faults within liquid-filled, wire-wound equipment
- Control circuitry associated with a fault pressure relay

Unresolved Maintenance Issue – A deficiency identified during a maintenance activity that causes the Component to not meet the intended performance, cannot be corrected during the maintenance interval, and requires follow-up corrective action.

Segment – Components of a consistent design standard, or a particular model or type from a single manufacturer that typically share other common elements. Consistent performance is expected across the entire population of a Segment. A Segment must contain at least sixty (60) individual Components.

Component Type –

- Any one of the five specific elements of a Protection System.
- Any one of the two specific elements of Automatic Reclosing.
- Any one of the two specific elements of Sudden Pressure Relaying.

Rationale for the deletion of part of the definition of Component: The SDT determined that it was explanatory in nature and adequately addressed in the Supplementary Reference and FAQ Document.

Component – Any individual discrete piece of equipment included in a Protection System, Automatic Reclosing, or Sudden Pressure Relaying.

Countable Event – A failure of a Component requiring repair or replacement, any condition discovered during the maintenance activities in Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-2, and Table 5, which requires corrective action or a Protection System Misoperation attributed to hardware failure or calibration failure. Misoperations due to product design errors, software errors, relay settings different from specified settings, Protection System Component, Automatic Reclosing, or Sudden

Pressure Relaying configuration or application errors are not included in Countable Events.

B. Requirements and Measures

R1. Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a Protection System Maintenance Program (PSMP) for its Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying identified in Section 4.2, Facilities. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning*]

The PSMP shall:

1.1. Identify which maintenance method (time-based, performance-based per PRC-005 Attachment A, or a combination) is used to address each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type. All batteries associated with the station dc supply Component Type of a Protection System shall be included in a time-based program as described in Table 1-4 and Table 3.

1.2. Include the applicable monitored Component attributes applied to each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, Table 4-1 through 4-2, and Table 5 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components.

M1. Each Transmission Owner, Generator Owner and Distribution Provider shall have a documented Protection System Maintenance Program in accordance with Requirement R1.

For each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type, the documentation shall include the type of maintenance method applied (time-based, performance-based, or a combination of these maintenance methods), and shall include all batteries associated with the station dc supply Component Types in a time-based program as described in Table 1-4 and Table 3. (Part 1.1)

For Component Types that use monitoring to extend the maintenance intervals, the responsible entity(s) shall have evidence for each Protection System, Automatic Reclosing, and Sudden Pressure Relaying Component Type (such as manufacturer's specifications or engineering drawings) of the appropriate monitored Component attributes as specified in Tables 1-1 through 1-5, Table 2, Table 3, Table 4-1 through 4-2, and Table 5. (Part 1.2)

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals in its PSMP shall follow the procedure

established in PRC-005 Attachment A to establish and maintain its performance-based intervals. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Each Transmission Owner, Generator Owner, and Distribution Provider that uses performance-based maintenance intervals shall have evidence that its current performance-based maintenance program(s) is in accordance with Requirement R2, which may include, but is not limited to, Component lists, dated maintenance records, and dated analysis records and results.

Rationale for R3 part 3.1 and 3.1.1.: The SDT, upon further reflection, determined that the PRC-005-3 Implementation Plan actually included a requirement that entities with newly-identified Automatic Reclosing Components implement its PSMP for those Components, and therefore determined that it was more appropriate to include this information in the standard rather than the implementation plan.

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall, except as provided in part 3.1, maintain its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components that are included within the time-based maintenance program in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Table 4-1 through 4-2, and Table 5. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

3.1. For each newly-identified Automatic Reclosing Component following a notification under Requirement R6, each Transmission Owner, Generator Owner, and Distribution Provider shall perform maintenance activities or provide documentation of prior maintenance activities according to either 3.1.1 or 3.1.2.

3.1.1. Complete the maintenance activities prescribed within Tables 4-1, 4-2(a), and 4-2(b) for the newly-identified Automatic Reclosing Component prior to the end of the third calendar year following the notification under Requirement R6; or

3.1.2. Provide documentation that the Automatic Reclosing Component was last maintained in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 4-1, 4-2(a), and 4-2(b).

M3. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes time-based maintenance program(s) shall have evidence that it has maintained its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components included within its time-based program in accordance with Requirement R3. The evidence may include, but is not limited to, dated maintenance records, dated

maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

Rationale for R4 part 4.1 and 4.1.1.: The SDT, upon further reflection, determined that the PRC-005-3 Implementation Plan actually included a requirement that entities with newly-identified Automatic Reclosing Components implement its PSMP for those Components, and therefore determined that it was more appropriate to include this information in the standard rather than the implementation plan.

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance program(s) in accordance with Requirement R2 shall, except as provided in part 4.1, implement and follow its PSMP for its Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components that are included within the performance-based program(s). *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

4.1. For each newly-identified Automatic Reclosing Component following a notification under Requirement R6, each Transmission Owner, Generator Owner, and Distribution Provider shall perform maintenance activities or provide documentation of prior maintenance activities according to either 4.1.1 or 4.1.2.

4.1.1. Complete the maintenance activities prescribed within Tables 4-1, 4-2(a), and 4-2(b) for the newly-identified Automatic Reclosing Component prior to the end of the third calendar year following the notification under Requirement R6; or

4.1.2. Provide documentation that the Automatic Reclosing Component was last maintained in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 4-1, 4-2(a), and 4-2(b).

M4. Each Transmission Owner, Generator Owner, and Distribution Provider that utilizes performance-based maintenance intervals in accordance with Requirement R2 shall have evidence that it has implemented the Protection System Maintenance Program for the Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components included in its performance-based program in accordance with Requirement R4. The evidence may include, but is not limited to, dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

R5. Each Transmission Owner, Generator Owner, and Distribution Provider shall demonstrate efforts to correct identified Unresolved Maintenance Issues. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence that it has undertaken efforts to correct identified Unresolved Maintenance

Issues in accordance with Requirement R5. The evidence may include, but is not limited to, work orders, replacement Component orders, invoices, project schedules with completed milestones, return material authorizations (RMAs) or purchase orders.

Rationale for R6: The information addressed in Requirement R6 is necessary for Transmission Owners, Generator Owners, and Distribution Provides to accurately apply Section 4.2.7, Applicability. The Balancing Authority is the entity that maintains the information and should have the responsibility to provide this information to the applicable entities. The drafting team reconsidered the inclusion of the Balancing Authority and determined it is appropriate to include the requirement the standard. This requirement may be relocated to another standard during future reviews of standards for quality and content.

The periodicity was chosen to balance the needs of the Transmission Owner, Generator Owner, and Distribution Provider to obtain the information with the needs of the Balancing Authority to provide an accurate gross capacity (considering retirement or installation of generating units and/or changes in its Balancing Authority Area) in order to properly include Automatic Reclosing in a PSMP.

R6. Each Balancing Authority shall, at least once every calendar year with not more than 15 calendar months between notifications, notify each Transmission Owner, Generator Owner, and Distribution Provider within its Balancing Authority Area of the gross capacity, in MW or MVA, of the largest BES generating unit within the Balancing Authority Area. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M6. Each Balancing Authority shall have dated documentation that it notified each Transmission Owner, Generator Owner, and Distribution Provider in accordance with Requirement R6. Examples of evidence may include, but are not limited to, copies of correspondence, such as e-mails or memoranda.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time

since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Transmission Owner, Generator Owner, Distribution Provider, and Balancing Authority shall each keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

For Requirement R1, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep its current dated Protection System Maintenance Program, as well as any superseded versions since the preceding compliance audit, including the documentation that specifies the type of maintenance program applied for each Protection System Component Type.

For Requirement R2, Requirement R3, Requirement R4, and Requirement R5, the Transmission Owner, Generator Owner, and Distribution Provider shall each keep documentation of the most recent performance of each distinct maintenance activity for the Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component, or all performances of each distinct maintenance activity for the Protection System, Automatic Reclosing, or Sudden Pressure Relaying Component since the previous scheduled audit date, whichever is longer.

For Requirement R6, the Balancing Authority shall keep documentation for three calendar years that it provided information identifying the largest BES generating unit to the Transmission Owners, Generator Owners, and Distribution Providers in its Balancing Authority Area.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information

None

Table of Compliance Elements

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The entity's PSMP failed to specify whether one Component Type is being addressed by time-based or performance-based maintenance, or a combination of both (part 1.1).	The entity's PSMP failed to specify whether two Component Types are being addressed by time-based or performance-based maintenance, or a combination of both (part 1.1).	The entity's PSMP failed to specify whether three Component Types are being addressed by time-based or performance-based maintenance, or a combination of both. (part 1.1). OR The entity's PSMP failed to include the applicable monitoring attributes applied to each Component Type consistent with the maintenance intervals specified in Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-2, and Table 5 where monitoring is used to extend the maintenance intervals beyond those specified for unmonitored Components (part 1.2).	The entity failed to establish a PSMP. OR The entity's PSMP failed to specify whether four or more Component Types are being addressed by time-based or performance-based maintenance, or a combination of both (part 1.1). OR The entity's PSMP failed to include applicable station batteries in a time-based program (part 1.1).
R2	The entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within three years.	NA	The entity uses performance-based maintenance intervals in its PSMP but failed to reduce Countable Events to no more than 4% within four years.	The entity uses performance-based maintenance intervals in its PSMP but: 1) Failed to establish the technical justification described within Requirement R2 for the initial use of the performance-based PSMP OR 2) Failed to reduce Countable Events to no more than 4% within five years OR

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
				3) Maintained a Segment with less than 60 Components OR 4) Failed to: • Annually update the list of Components, OR • Annually perform maintenance on the greater of 5% of the Segment population or 3 Components, OR • Annually analyze the program activities and results for each Segment.
R3	For Components included within a time-based maintenance program, the entity failed to maintain 5% or less of the total Components included within a specific Component Type in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-2, and Table 5. For Automatic Reclosing Components added to a time-based maintenance program per information from the Balancing	For Components included within a time-based maintenance program, the entity failed to maintain more than 5% but 10% or less of the total Components included within a specific Component Type in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-2, and Table 5. For Automatic Reclosing Components added to a time-based maintenance program per	For Components included within a time-based maintenance program, the entity failed to maintain more than 10% but 15% or less of the total Components included within a specific Component Type in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-2, and Table 5. For Automatic Reclosing Components added to a time-based maintenance program per	For Components included within a time-based maintenance program, the entity failed to maintain more than 15% of the total Components included within a specific Component Type in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 1-1 through 1-5, Table 2, Table 3, Tables 4-1 through 4-2, and Table 5. For Automatic Reclosing Components added to a time-

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Authority, the entity failed to maintain 5% or less of the total Components in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 4-1 through 4-2.	information from the Balancing Authority, the entity failed to maintain more than 5% but 10% or less of the total Components in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 4-1 through 4-2.	information from the Balancing Authority, the entity failed to maintain more than 10% but 15% or less of the total Components in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 4-1 through 4-2.	based maintenance program per information from the Balancing Authority, the entity failed to maintain more than 15% of the total Components in accordance with the minimum maintenance activities and maximum maintenance intervals prescribed within Tables 4-1 through 4-2.
R4	For Components included within a performance-based maintenance program, the entity failed to maintain 5% or less of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP. For Automatic Reclosing Components added to a performance-based maintenance program per information from the Balancing Authority, the entity failed to maintain 5% or less of the total Components in accordance with their performance-based PSMP.	For Components included within a performance-based maintenance program, the entity failed to maintain more than 5% but 10% or less of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP. For Automatic Reclosing Components added to a performance-based maintenance program per information from the Balancing Authority, the entity failed to maintain more than 5% but 10% or less of the total Components in accordance with their performance-based PSMP.	For Components included within a performance-based maintenance program, the entity failed to maintain more than 10% but 15% or less of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP. For Automatic Reclosing Components added to a performance-based maintenance program per information from the Balancing Authority, the entity failed to maintain more than 10% but 15% or less of the total Components in accordance with their performance-based PSMP.	For Components included within a performance-based maintenance program, the entity failed to maintain more than 15% of the annual scheduled maintenance for a specific Component Type in accordance with their performance-based PSMP. For Automatic Reclosing Components added to a performance-based maintenance program per information from the Balancing Authority, the entity failed to maintain more than 15% of the total Components in accordance with their performance-based PSMP.

Requirement Number	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The entity failed to undertake efforts to correct 5 or fewer identified Unresolved Maintenance Issues.	The entity failed to undertake efforts to correct greater than 5 but less than or equal to 10 identified Unresolved Maintenance Issues.	The entity failed to undertake efforts to correct greater than 10 but less than or equal to 15 identified Unresolved Maintenance Issues.	The entity failed to undertake efforts to correct greater than 15 identified Unresolved Maintenance Issues.
R6				The entity failed to notify each Transmission Owner, Generator Owner, and Distribution Provider within its Balancing Authority Area at least once every calendar year of the gross capacity, in MW or MVA, of the largest BES generating unit within the Balancing Authority Area. OR The entity had more than 15 calendar months between notifications to each Transmission Owner, Generator Owner, and Distribution Provider of the gross capacity, in MW or MVA, of the largest BES generating unit within the Balancing Authority Area.

D. Regional Variances

None.

E. Interpretations

None.

F. Supplemental Reference Documents

The following documents present a detailed discussion about determination of maintenance intervals and other useful information regarding establishment of a maintenance program.

1. *Supplementary Reference and FAQ - PRC-005-X Protection System Maintenance,* Protection System Maintenance and Testing Standard Drafting Team (April 2014)
2. *Considerations for Maintenance and Testing of Auto-reclosing Schemes*, NERC System Analysis and Modeling Subcommittee, and NERC System Protection and Control Subcommittee (November 2012)

Sudden Pressure Relays and Other Devices that Respond to Non-Electrical Quantities – SPCS Input for Standard Development in Response to FERC Order No. 758, NERC System Protection and Control Subcommittee (December 2013)

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. 3. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/05
1a	February 17, 2011	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers	Project 2009-17 interpretation
1a	February 17, 2011	Adopted by Board of Trustees	

Version	Date	Action	Change Tracking
1a	September 26, 2011	FERC Order issued approving interpretation of R1 and R2 (FERC's Order is effective as of September 26, 2011)	
1.1b	May 9, 2012	PRC-005-1.1b was adopted by the Board of Trustees as part of Project 2010-07 (Generator Requirements at the Transmission Interface).	
2	November 7, 2012	Adopted by Board of Trustees	Project 2007-17 - Complete revision, absorbing maintenance requirements from PRC-005-1.1b, PRC-008-0, PRC-011-0, PRC-017-0
2	October 17, 2013	Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase "or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;" to the second sentence under the "Retirement of Existing…"	
TBD (balloted as 4(X)	TBD	Standard revised in Project 2014-01	Applicability section revised to clarify application of Requirements to BES dispersed power producing resources
~~1a~~	~~September 26, 2011~~	~~FERC Order issued approving interpretation of R1 and R2 (FERC's Order is effective as of September 26, 2011)~~	
~~1.1a~~	~~February 1, 2012~~	~~Errata change: Clarified inclusion of generator interconnection Facility in Generator Owner's responsibility~~	~~Revision under Project 2010-07~~

Version	Date	Action	Change Tracking
~~1b~~	~~February 3, 2012~~	~~FERC Order issued approving interpretation of R1, R1.1, and R1.2 (FERC's Order dated March 14, 2012). Updated version from 1a to 1b.~~	~~Project 2009-10 Interpretation~~
~~1.1b~~	~~April 23, 2012~~	~~Updated standard version to 1.1b to reflect FERC approval of PRC-005-1b.~~	~~Revision under Project 2010-07~~

Version	Date	Action	Change Tracking
~~1.1b~~	~~May 9, 2012~~	~~PRC-005-1.1b was adopted by the Board of Trustees as part of Project 2010-07 (Generator Requirements at the Transmission Interface).~~	
~~2~~	~~November 7, 2012~~	~~Adopted by Board of Trustees~~	~~Project 2007-17 - Complete revision, absorbing maintenance requirements from PRC-005-1.1b, PRC-008-0, PRC-011-0, PRC-017-0~~
~~2~~	~~October 17, 2013~~	~~Errata Change: The Standards Committee approved an errata change to the implementation plan for PRC-005-2 to add the phrase "or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities;" to the second sentence under the "Retirement of Existing~~	
3	November 7, 2013	Adopted by the NERC Board of Trustees	Revised to address the FERC directive in Order No.758 to include Automatic Reclosing in maintenance programs.
3.1	February 12, 2014	Approved by the Standards Committee	Errata changes to correct capitalization of defined terms

Version	Date	Action	Change Tracking
4			Project 2007-17.3 – Revised to address the FERC directive in Order No. 758 to include sudden pressure relays in maintenance programs.
TBD (balloted as 2(X)	TBD	.Standard revised in Project 2014-01.	Applicability section revised to clarify application of Requirements to BES dispersed power producing resources

(X) – Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval[2]**	**Maintenance Activities**
tive relay not having all the monitoring attributes	6 Calendar Years	For all unmonitored relays: • Verify that settings are as specified For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
or protective relay with the following: is and alarming (see Table 2). ent waveform sampling three or more times per nversion of samples to numeric values for ations by microprocessor electronics. supply failure (see Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values.

dard, a calendar year starts on the first day of a new year (January 1) after a maintenance activity has been completed

Table 1-1 Component Type - Protective Relay Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**[2]	**Maintenance Activities**
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2). • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). • Alarming for change of settings (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 1-2 Component Type - Communications Systems Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.	4 Calendar Months	Verify that the communications system is functional.
	6 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with continuous monitoring or periodic automated testing for the presence of the channel function, and alarming for loss of function (See Table 2).	12 Calendar Years	Verify that the communications system meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.
Any communications system with all of the following: • Continuous monitoring or periodic automated testing for the performance of the channel using criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate, and alarming for excessive performance degradation). (See Table 2) • Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2).	12 Calendar Years	Verify only the unmonitored communications system inputs and outputs that are essential to proper functioning of the Protection System

Table 1-3 Component Type - Voltage and Current Sensing Devices Providing Inputs to Protective Relays Excluding distributed UFLS and distributed UVLS (see Table 3)		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any voltage and current sensing devices not having monitoring attributes of the category below.	12 Calendar Years	Verify that current and voltage signal values are provided to the protective relays.
Voltage and Current Sensing devices connected to microprocessor relays with AC measurements are continuously verified by comparison of sensing input value, as measured by the microprocessor relay, to an independent ac measurement source, with alarming for unacceptable error or failure (see Table 2).	No periodic maintenance specified	None.

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply using **Vented Lead-Acid (VLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells where cells are visible – or measure battery cell/unit internal ohmic values where the cells are not visible • Physical condition of battery rack

Table 1-4(a) Component Type – Protection System Station dc Supply Using Vented Lead-Acid (VLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	18 Calendar Months -or- 6 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **with Valve Regulated Lead-Acid (VRLA) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	6 Calendar Months	Inspect: • Condition of all individual units by measuring battery cell/unit internal ohmic values.
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Physical condition of battery rack

Table 1-4(b) Component Type – Protection System Station dc Supply Using Valve-Regulated Lead-Acid (VRLA) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS systems, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	6 Calendar Months -or- 3 Calendar Years	Verify that the station battery can perform as manufactured by evaluating cell/unit measurements indicative of battery performance (e.g. internal ohmic values or float current) against the station battery baseline. -or- Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Protection System Station dc supply **Nickel-Cadmium (NiCad) batteries** not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • Electrolyte level • For unintentional grounds
	18 Calendar Months	Verify: • Float voltage of battery charger • Battery continuity • Battery terminal connection resistance • Battery intercell or unit-to-unit connection resistance Inspect: • Cell condition of all individual battery cells. • Physical condition of battery rack

Table 1-4(c) Component Type – Protection System Station dc Supply Using Nickel-Cadmium (NiCad) Batteries Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
	6 Calendar Years	Verify that the station battery can perform as manufactured by conducting a performance or modified performance capacity test of the entire battery bank.

Table 1-4(d) Component Type – Protection System Station dc Supply Using Non Battery Based Energy Storage Excluding distributed UFLS and distributed UVLS (see Table 3) Protection System Station dc supply used only for non-BES interrupting devices for SPS, non-distributed UFLS system, or non-distributed UVLS systems is excluded (see Table 1-4(e)).		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System station dc supply not using a battery and not having monitoring attributes of Table 1-4(f).	4 Calendar Months	Verify: • Station dc supply voltage Inspect: • For unintentional grounds
	18 Calendar Months	Inspect: Condition of non-battery based dc supply
	6 Calendar Years	Verify that the dc supply can perform as manufactured when ac power is not present.

Table 1-4(e) Component Type – Protection System Station dc Supply for non-BES Interrupting Devices for SPS, non-distributed UFLS, and non-distributed UVLS systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any Protection System dc supply used for tripping only non-BES interrupting devices as part of a SPS, non-distributed UFLS, or non-distributed UVLS system and not having monitoring attributes of Table 1-4(f).	When control circuits are verified (See Table 1-5)	Verify Station dc supply voltage.

Table 1-4(f) Exclusions for Protection System Station dc Supply Monitoring Devices and Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any station dc supply with high and low voltage monitoring and alarming of the battery charger voltage to detect charger overvoltage and charger failure (See Table 2).	No periodic maintenance specified	No periodic verification of station dc supply voltage is required.
Any battery based station dc supply with electrolyte level monitoring and alarming in every cell (See Table 2).		No periodic inspection of the electrolyte level for each cell is required.
Any station dc supply with unintentional dc ground monitoring and alarming (See Table 2).		No periodic inspection of unintentional dc grounds is required.
Any station dc supply with charger float voltage monitoring and alarming to ensure correct float voltage is being applied on the station dc supply (See Table 2).		No periodic verification of float voltage of battery charger is required.
Any battery based station dc supply with monitoring and alarming of battery string continuity (See Table 2).		No periodic verification of the battery continuity is required.
Any battery based station dc supply with monitoring and alarming of the intercell and/or terminal connection detail resistance of the entire battery (See Table 2).		No periodic verification of the intercell and terminal connection resistance is required.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with internal ohmic value or float current monitoring and alarming, and evaluating present values relative to baseline internal ohmic values for every cell/unit (See Table 2).		No periodic evaluation relative to baseline of battery cell/unit measurements indicative of battery performance is required to verify the station battery can perform as manufactured.
Any Valve Regulated Lead-Acid (VRLA) or Vented Lead-Acid (VLA) station battery with monitoring and alarming of each cell/unit internal ohmic value (See Table 2).		No periodic inspection of the condition of all individual units by measuring battery cell/unit internal ohmic values of a station VRLA or Vented Lead-Acid (VLA) battery is required.

Table 1-5 Component Type - Control Circuitry Associated With Protective Functions Excluding distributed UFLS and distributed UVLS (see Table 3) Note: Table requirements apply to all Control Circuitry Components of Protection Systems, and SPSs except as noted.		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Trip coils or actuators of circuit breakers, interrupting devices, or mitigating devices (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each trip coil is able to operate the circuit breaker, interrupting device, or mitigating device.
Electromechanical lockout devices which are directly in a trip path from the protective relay to the interrupting device trip coil (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify electrical operation of electromechanical lockout devices.
Unmonitored control circuitry associated with SPS. (See Table 4-2(b) for SPS which include Automatic Reclosing.)	12 Calendar Years	Verify all paths of the control circuits essential for proper operation of the SPS.
Unmonitored control circuitry associated with protective functions inclusive of all auxiliary relays.	12 Calendar Years	Verify all paths of the trip circuits inclusive of all auxiliary relays through the trip coil(s) of the circuit breakers or other interrupting devices.
Control circuitry associated with protective functions and/or SPSs whose integrity is monitored and alarmed (See Table 2).	No periodic maintenance specified	None.

Table 2 – Alarming Paths and Monitoring In Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2, alarm attributes used to justify extended maximum maintenance intervals and/or reduced maintenance activities are subject to the following maintenance requirements		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any alarm path through which alarms in Tables 1-1 through 1-5, Table 3, and Tables 4-1 through 4-2 are conveyed from the alarm origin to the location where corrective action can be initiated, and not having all the attributes of the "Alarm Path with monitoring" category below. Alarms are reported within 24 hours of detection to a location where corrective action can be initiated.	12 Calendar Years	Verify that the alarm path conveys alarm signals to a location where corrective action can be initiated.
Alarm Path with monitoring: The location where corrective action is taken receives an alarm within 24 hours for failure of any portion of the alarming path from the alarm origin to the location where corrective action can be initiated.	No periodic maintenance specified	None.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored protective relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate. For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Verify acceptable measurement of power system input values.
Monitored microprocessor protective relay with the following: • Internal self-diagnosis and alarming (See Table 2). • Voltage and/or current waveform sampling three or more times per power cycle, and conversion of samples to numeric values for measurement calculations by microprocessor electronics. Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Protection System. • Acceptable measurement of power system input values
Monitored microprocessor protective relay with preceding row attributes and the following: • Ac measurements are continuously verified by comparison to an independent ac measurement source, with alarming for excessive error (See Table 2).	12 Calendar Years	Verify only the unmonitored relay inputs and outputs that are essential to proper functioning of the Protection System.

Table 3 Maintenance Activities and Intervals for distributed UFLS and distributed UVLS Systems		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
• Some or all binary or status inputs and control outputs are monitored by a process that continuously demonstrates ability to perform as designed, with alarming for failure (See Table 2). Alarming for change of settings (See Table 2).		
Voltage and/or current sensing devices associated with UFLS or UVLS systems.	12 Calendar Years	Verify that current and/or voltage signal values are provided to the protective relays.
Protection System dc supply for tripping non-BES interrupting devices used only for a UFLS or UVLS system.	12 Calendar Years	Verify Protection System dc supply voltage.
Control circuitry between the UFLS or UVLS relays and electromechanical lockout and/or tripping auxiliary devices (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify the path from the relay to the lockout and/or tripping auxiliary relay (including essential supervisory logic).
Electromechanical lockout and/or tripping auxiliary devices associated only with UFLS or UVLS systems (excludes non-BES interrupting device trip coils).	12 Calendar Years	Verify electrical operation of electromechanical lockout and/or tripping auxiliary devices.
Control circuitry between the electromechanical lockout and/or tripping auxiliary devices and the non-BES interrupting devices in UFLS or UVLS systems, or between UFLS or UVLS relays (with no interposing electromechanical lockout or auxiliary device) and the non-BES interrupting devices (excludes non-BES interrupting device trip coils).	No periodic maintenance specified	None.
Trip coils of non-BES interrupting devices in UFLS or UVLS systems.	No periodic maintenance specified	None.

Table 4-1 Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Reclosing Relay		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any unmonitored reclosing relay not having all the monitoring attributes of a category below.	6 Calendar Years	Verify that settings are as specified. For non-microprocessor relays: • Test and, if necessary calibrate For microprocessor relays: • Verify operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.
Monitored microprocessor reclosing relay with the following: • Internal self-diagnosis and alarming (See Table 2). • Alarming for power supply failure (See Table 2).	12 Calendar Years	Verify: • Settings are as specified. • Operation of the relay inputs and outputs that are essential to proper functioning of the Automatic Reclosing.

Table 4-2(a) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing Relays that are NOT an Integral Part of an SPS		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Unmonitored Control circuitry associated with Automatic Reclosing that is not an integral part of an SPS.	12 Calendar Years	Verify that Automatic Reclosing, upon initiation, does not issue a premature closing command to the close circuitry.
Control circuitry associated with Automatic Reclosing that is not part of an SPS and is monitored and alarmed for conditions that would result in a premature closing command. (See Table 2)	No periodic maintenance specified	None.

Table 4-2(b) Maintenance Activities and Intervals for Automatic Reclosing Components Component Type – Control Circuitry Associated with Reclosing Relays that ARE an Integral Part of an SPS		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Close coils or actuators of circuit breakers or similar devices that are used in conjunction with Automatic Reclosing as part of an SPS (regardless of any monitoring of the control circuitry).	6 Calendar Years	Verify that each close coil or actuator is able to operate the circuit breaker or mitigating device.
Unmonitored close control circuitry associated with Automatic Reclosing used as an integral part of an SPS.	12 Calendar Years	Verify all paths of the control circuits associated with Automatic Reclosing that are essential for proper operation of the SPS.
Control circuitry associated with Automatic Reclosing that is an integral part of an SPS whose integrity is monitored and alarmed. (See Table 2)	No periodic maintenance specified	None.

Table 5 Maintenance Activities and Intervals for Sudden Pressure Relaying		
Component Attributes	**Maximum Maintenance Interval**	**Maintenance Activities**
Any fault pressure relay.	6 Calendar Years	Verify the pressure or flow sensing mechanism is operable.
Control circuitry associated with Sudden Pressure Relaying from the fault pressure relay to the interrupting device trip coil(s).	12 Calendar Years	Verify all paths of the control circuits that are essential for proper operation of the Sudden Pressure Relaying.

PRC-005 — Attachment A

Criteria for a Performance-Based Protection System Maintenance Program

Purpose: To establish a technical basis for initial and continued use of a performance-based Protection System Maintenance Program (PSMP).

To establish the technical justification for the initial use of a performance-based PSMP:

1. Develop a list with a description of Components included in each designated Segment, with a minimum **Segment** population of 60 Components.
2. Maintain the Components in each Segment according to the time-based maximum allowable intervals established in Tables 1-1 through 1-5, Table 3, Tables 4-1 through 4-2, and Table 5 until results of maintenance activities for the Segment are available for a minimum of 30 individual Components of the Segment.
3. Document the maintenance program activities and results for each Segment, including maintenance dates and Countable Events for each included Component.
4. Analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment and develop maintenance intervals.
5. Determine the maximum allowable maintenance interval for each Segment such that the Segment experiences **Countable Events** on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

To maintain the technical justification for the ongoing use of a performance-based PSMP:

1. At least annually, update the list of Components and Segments and/or description if any changes occur within the Segment.
2. Perform maintenance on the greater of 5% of the Components (addressed in the performance based PSMP) in each Segment or 3 individual Components within the Segment in each year.
3. For the prior year, analyze the maintenance program activities and results for each Segment to determine the overall performance of the Segment.
4. Using the prior year's data, determine the maximum allowable maintenance interval for each Segment such that the Segment experiences Countable Events on no more than 4% of the Components within the Segment, for the greater of either the last 30 Components maintained or all Components maintained in the previous year.

If the Components in a Segment maintained through a performance-based PSMP experience 4% or more Countable Events, develop, document, and implement an action plan to reduce the Countable Events to less than 4% of the Segment population within 3 years.

Implementation Plan

Project 2014-01 Standards Applicability for Dispersed Power Producing Resources
PRC-005-X(X)

The standard numbers currently include an (X) to indicate the version numbering will be updated. Some standards are open in current projects and others are pending with governmental authorities. As a result, NERC will assign the appropriate version number prior to BOT adoption.

Standards Involved
Approval:

- PRC-005-X(X) – Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance

Retirement:

- PRC-005-3(X) – Protection System and Automatic Reclosing Maintenance
- PRC-005-X – Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance

Prerequisite Approvals:
N/A

Background:
In light of the adoption of a revised "Bulk Electric System" definition by the Board of Trustees, changes to the applicability sections of certain Reliability Standards, including PRC-005, are necessary to align with the implementation of the revised "Bulk Electric System" definition. The Standard Drafting Team (SDT) for Project 2014-01 – Standards Applicability for Dispersed Power Producing Resources has modified the applicability section of certain Generator Owner/Generator Operator requirements to recognize the unique technical and reliability aspects of dispersed generation in order to ensure the applicability of the standards is consistent with the reliable operation of the Bulk-Power System.

Reliability Standard PRC-005-X has concluded a 45-day comment and ballot period to address sudden pressure relays. The SDT has revised the applicability section of PRC-005-X to align with the revised definition of "Bulk Electric System" in the event that this version of PRC-005 is mandatory and enforceable on the effective date of the revised definition of "Bulk Electric System."

General Considerations:
PRC-005-X(X) is proposed for approval to align the applicability section of PRC-005-X with the revised definition of "Bulk Electric System." PRC-005-X may already be retired pursuant to an Implementation

Plan of a successor version of PRC-005 by the time the revised definition of "Bulk Electric System" becomes effective. If this occurs, PRC-005-X(X) will not go into effect.

Effective Date

PRC-005-X(X) shall become effective on the later of the effective date of the revised definition of Bulk Electric System or the first day following the effective date of PRC-005-X.

Retirement of Existing Standards

PRC-005-X shall be retired at midnight of the day immediately prior to the effective date of PRC-005-X(X) in the particular jurisdiction in which the revised standard is becoming effective.

Implementation Plan

PRC-005-X(X) only modifies the applicability for PRC-005-X. All aspects of the Implementation Plan for PRC-005-X will remain applicable to PRC-005-X(X) and are incorporated here by reference.

Cross References

The Implementation Plan for the revised definition of "Bulk Electric System" is available here.

The Implementation Plan for PRC-005-X is available here.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment November 20 – December 19, 2013.

Description of Current Draft

The Project 2014-01 Dispersed Power Producing Resources drafting team is posting minor applicability revisions to VAR-002-2b. The standard previously was adopted by the NERC Board of Trustees on August 16, 2012, and approved by FERC on April 16, 2013. The intent of the revisions is to clarify application of Requirements R4 and R5 to BES Bulk Electric Systems (BES) dispersed power producing resources included in the BES though Inclusion I4 of the BES definition.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Initial Ballot	June – July 2014
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	August – September 2014
Final ballot	October 2014
BOT adoption	November 2014

DRAFT

When this standard has received ballot approval, the text boxes within the Applicability section of the Standard will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: **Generator Operation for Maintaining Network Voltage Schedules**

2. Number: VAR-002-2b(X)

3. Purpose: To ensure generators provide reactive and voltage control necessary to ensure voltage levels, reactive flows, and reactive resources are maintained within applicable Facility Ratings to protect equipment and the reliable operation of the Interconnection.

4. Applicability

4.1. Generator Operator.

4.2. Generator Owner.

5. Effective Date: The standard shall become effective on the date the standard is approved by an applicable government authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction~~In those jurisdictions where regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter after applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter after Board of Trustees approval~~.

The only revisions made to this version of VAR-002 are revisions to Requirements R3 and R4, to clarify applicability of the Requirements of the standard at generator Facilities. These applicability revisions are intended to clarify and provide for consistent application of the Requirements to BES generator Facilities included in the BES through Inclusion I4 – Dispersed Power Producing Resources.

The revisions to the two Requirements were made to VAR-002-2b, which is the currently enforceable version of VAR-002. VAR-002-3 is pending regulatory approval, and depending on the timing of the approval of VAR-002-3, NERC may request approval of this interim version of the standard in order to provide regulatory certainty for entities as the revised definition of BES is being implemented. This interim version is labeled VAR-002-2b(X) for balloting purposes.

B. Requirements

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (automatic voltage regulator in service and controlling voltage) unless the Generator Operator has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- That the generator is being operated in start-up[1] or shutdown[2] mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in the automatic voltage control mode for a reason other than start-up or shutdown.

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within applicable Facility Ratings[4]) as directed by the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

2.1. When a generator's automatic voltage regulator is out of service, the Generator Operator shall use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator.

2.2. When directed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

R3. Each Generator Operator shall notify its associated Transmission Operator as soon as practical, but within 30 minutes of any of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

3.1. A status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.

- Reporting of status or capability changes is not applicable to the individual dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition.

3.2. A status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.

Rationale for R3 Exclusion:

VAR-002 addresses control and management of reactive resources and provides voltage control where it has an impact on the BES. For dispersed power producing resources as identified in Inclusion I4, Requirement R3.1 should not apply at the individual generator level due to the unique characteristics and small scale of individual dispersed power producing resources. In addition, other standards such as proposed TOP-003 require the Generator Operator to provide real time data as directed by the TOP.

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.

[2] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

[3] The voltage or Reactive Power schedule is a target value communicated by the Transmission Operator to the Generator Operator establishing a tolerance band within which the target value is to be maintained during a specified period.

[4] When a Generator is operating in manual control, reactive power capability may change based on stability considerations and this may lead to a change in the associated Facility Ratings.

R4. The Generator Owner shall provide the following to its associated Transmission Operator and Transmission Planner within 30 calendar days of a request. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

4.1. For generator step-up transformers and auxiliary transformers[5] with primary voltages equal to or greater than the generator terminal voltage:

4.1.1. Tap settings.

4.1.2. Available fixed tap ranges.

4.1.3. Impedance data.

4.1.4. The +/- voltage range with step-change in % for load-tap changing transformers.

Rationale for Footnote 5 in Requirement R4, Part 4.1:

The Transmission Operator / Transmission Provider needs to review tap settings on the main transformers that connect the generation to the high voltage system. The Transmission Operator / Transmission Provider must assure that the collector system (typically 34.5 kV) voltage coordinates with the voltage set-points and tolerance bands established by the Transmission Operator / Transmission. The portion of the collector system that aggregates 75 MVA or less of resources is excluded under I4 and the individual unit step-up transformers primarily affect the collector system, so it should also be excluded and left to the Generator Owner to design and manage based on the secondary voltages expected on the collector system.

R5. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

5.1. If the Generator Operator can't comply with the Transmission Operator's specifications, the Generator Operator shall notify the Transmission Operator and shall provide the technical justification.

C. Measures

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode as specified in Requirement 1. If a generator is being started up or shut down with the automatic voltage control off and no notification of the automatic voltage regulator status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode. Such evidence must include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached.

M2. The Generator Operator shall have evidence to show that it controlled its generator voltage and reactive output to meet the voltage or Reactive Power schedule provided by its associated Transmission Operator as specified in Requirement 2.

[5] For dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition, this requirement applies only to those transformers that have at least one winding at a voltage of 100 kV or above.

M3. The Generator Operator shall have evidence to show that it responded to the Transmission Operator's direction as identified in Requirement 2.1 and Requirement 2.2.

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any of the changes identified in Requirement 3.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirements 4.1.1 through 4.1.4

M6. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation as identified in Requirement 5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

~~For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.~~

~~For functional entities that work for their Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority~~.

1.2. Data Retention

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

The Generator Operator shall maintain evidence needed for Measure 1 through Measure 4 and Measure 7 for the current and previous calendar year.

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. (Measures 5 and 6)

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Enforcement Processes:

The following processes may be used:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

DRAFT

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The responsible entity did not operate each generator in the automatic voltage control mode and failed to notify the Transmission Operator as identified in R1.
R2.	When directed by the Transmission Operator to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for up to and including 45 minutes.	When directed by the Transmission Operator to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for more than 45 minutes up to and including 60 minutes. OR When a generator's automatic voltage regulator is out of service, the Generator Operator failed to use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator. OR The Generator Operator failed to provide an explanation of why the voltage schedule could not be met.	When directed by the Transmission Operator to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for more than 60 minutes up to and including 75 minutes.	When directed by the Transmission Operator to maintain the generator voltage or reactive power schedule the Generator Operator failed to meet the directed values for more than 75 minutes. OR When a generator's automatic voltage regulator is out of service, the Generator Operator failed to use an alternative method to control the generator voltage and reactive output to meet the voltage or Reactive Power schedule directed by the Transmission Operator and the Generator Operator failed to provide an explanation of why the voltage schedule could not be met.
R3.	N/A	N/A	The Generator Operator failed to notify the Transmission Operator within 30 minutes of the information as specified in either R3.1 or R3.2	The Generator Operator failed to notify the Transmission Operator within 30 minutes of the information as specified in both R3.1 and R3.2

DRAFT

R4.	The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner one of the types of data as specified in R4.1.1 or R 4.1.2 or 4.1.3 or 4.1.4 OR The information was provided in more than 30, but less than or equal to 35 calendar days of the request.	The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner two of the types of data as specified in R4.1.1 or R 4.1.2 or 4.1.3 or 4.1.4 OR The information was provided in more than 35, but less than or equal to 40 calendar days of the request.	The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner three of the types of data as specified in R4.1.1 or R 4.1.2 or 4.1.3 or 4.1.4 OR The information was provided in more than 40, but less than or equal to 45 calendar days of the request.	The Responsible entity failed to provide to its associated Transmission Operator and Transmission Planner any of the types of data as specified in R4.1.1 and R 4.1.2 and 4.1.3 and 4.1.4 OR The information was provided in more than 45 calendar days of the request.
R5.	N/A	N/A	N/A	The responsible entity failed to ensure that transformer tap positions were changed according to the specifications provided by the Transmission Operator when said actions would not have violated safety, an equipment rating, a regulatory requirement, or a statutory requirement.
R5.1.	N/A	N/A	N/A	The responsible entity failed to notify the Transmission Operator and to provide technical justification.

DRAFT

E. Regional Differences

None identified.

F. Associated Documents

1. Appendix 1 — Interpretation of Requirements R1 and R2 (August 1, 2007).

Version History

Version	Date	Action	Change Tracking
1	May 15, 2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and 2.4.3.	July 5, 2006
1a	December 19, 2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	January 16, 2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	Errata
1.1a	October 29, 2008	BOT adopted errata changes; updated version number to "1.1a"	Errata
1.1b	March 3, 2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	Revised
2b	TBD	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4.	Revised
2b	August 16, 2012	Adopted by Board of Trustees	
2b	April 16, 2013	FERC Order issued approving VAR-002-2b	
2b(X)	TBD	Interim version to clarify applicability of two Requirements to BES dispersed power producing resources. Revised in Project 2014-01.	Revised

DRAFT

Appendix 1

Interpretation of Requirements R1 and R2

Request:

Requirement R1 of Standard VAR-002-1 states that Generation Operators shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (***automatic voltage regulator in service and controlling voltage***) unless the Generator Operator has notified the Transmission Operator.

Requirement R2 goes on to state that each Generation Operator shall maintain the generator voltage ***or Reactive Power output*** as directed by the Transmission Operator.

The two underlined phrases are the reasons for this interpretation request.

Most generation excitation controls include a device known as the Automatic Voltage Regulator, or AVR. This is the device which is referred to by the R1 requirement above. Most AVR's have the option of being set in various operating modes, such as constant voltage, constant power factor, and constant Mvar.

In the course of helping members of the WECC insure that they are in full compliance with NERC Reliability Standards, I have discovered both Transmission Operators and Generation Operators who have interpreted this standard to mean that AVR operation in the constant power factor or constant Mvar modes complies with the R1 and R2 requirements cited above. Their rational is as follows:

- The AVR is clearly in service because it is operating in one of its operating modes
- The AVR is clearly controlling voltage because to maintain constant PF or constant Mvar, it controls the generator terminal voltage
- R2 clearly gives the Transmission Operator the option of directing the Generation Operator to maintain a constant reactive power output rather than a constant voltage.

Other parties have interpreted this standard to require operation in the constant voltage mode only. Their rational stems from the belief that the purpose of the VAR-002-1 standard is to insure the automatic delivery of additional reactive to the system whenever a voltage decline begins to occur.

The material impact of misinterpretation of these standards is twofold.

- First, misinterpretation may result in reduced reactive response during system disturbances, which in turn may contribute to voltage collapse.
- Second, misinterpretation may result in substantial financial penalties imposed on generation operators and transmission operators who believe that they are in full compliance with the standard.

In accordance with the NERC Reliability Standards Development Procedure, I am requesting that a formal interpretation of the VAR-002-1 standard be provided. Two specific questions need to be answered.

- First, does AVR operation in the constant PF or constant Mvar modes comply with R1?
- Second, does R2 give the Transmission Operator the option of directing the Generation Owner to operate the AVR in the constant Pf or constant Mvar modes rather than the constant voltage mode?

Interpretation:

1. First, does AVR operation in the constant PF or constant Mvar modes comply with R1?

   Interpretation: No, only operation in constant voltage mode meets this requirement. This answer is predicated on the assumption that the generator has the physical equipment that will allow such operation and that the Transmission Operator has not directed the generator to run in a mode other than constant voltage.

2. Second, does R2 give the Transmission Operator the option of directing the Generation Owner (sic) to operate the AVR in the constant Pf or constant Mvar modes rather than the constant voltage mode?

   Interpretation: Yes, if the Transmission Operator specifically directs a Generator Operator to operate the AVR in a mode other than constant voltage mode, then that directed mode of AVR operation is allowed.

DRAFT

Appendix 2

Interpretation of VAR-002-1a

Request:

VAR-002 — Generator Operation for Maintaining Network Voltage Schedules, addresses the generator's provision of voltage and VAR control. Confusion exists in the industry and regions as to which requirements in this standard apply to Generator Operators that operate generators that do not have automatic voltage regulation capability.

The Standard's requirements do not identify the subset of generator operators that need to comply – forcing some generator operators that do not have any automatic voltage regulation capability to demonstrate how they complied with the requirements, even when they aren't physically able to comply with the requirements. Generator owners want clarification to verify that they are not expected to acquire AVR devices to comply with the requirements in this standard.

Many generators do not have automatic voltage regulators and do not receive voltage schedules. These entities are at a loss as to how to comply with these requirements and are expending resources attempting to demonstrate compliance with these requirements. A clarification will avoid challenges and potential litigation stemming from sanctions and penalties applied to entities that are being audited for compliance with this standard, but who do not fall within the scope or intent of the standard itself.

Please identify which requirements apply to generators that do not operate generators equipped with AVRs.

Response: All the requirements and associated subrequirements in VAR-002-1a apply to Generator Owners and Generator Operators that own or operate generators whether equipped with an automatic voltage regulator or not. The standard is predicated on the assumption that the generator has the physical equipment (automatic voltage regulator) that is capable of automatic operation. A generator that is not equipped with an automatic voltage regulator results in a functionally equivalent condition to a generator equipped with an automatic voltage regulator that is out of service due to maintenance or failure.

There are no requirements in the standard that require a generator to have an automatic voltage regulator, nor are there any requirements for a Generator Owner to modify its generator to add an automatic voltage regulator. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power output (within applicable Facility Ratings) as directed by the Transmission Operator.

DRAFT

Implementation Plan

Dispersed Generation Resources
VAR-002-2b(X)

Standards Involved

Approval:

- VAR-002-2b(X) – Generator Operation for Maintaining Network Voltage Schedules

Retirement or Supersede:

- VAR-002-2b – Generator Operation for Maintaining Network Voltage Schedules

Prerequisite Approvals:

N/A

Background

In light of the adoption of a revised "Bulk Electric System" definition by the Board of Trustees (Board), changes to the applicability sections of certain Reliability Standards, including VAR-002, are necessary to align with the implementation of the revised "Bulk Electric System" definition. The Standard Drafting Team (SDT) for Project 2014-01 – Standards Applicability for Dispersed Power Producing Resources has modified the applicability section of certain Generator Owner/Generator Operator requirements to recognize the unique technical and reliability aspects of dispersed generation in order to ensure the applicability of the standards is consistent with the reliable operation of the Bulk-Power System.

Effective Date

VAR-002-2b(X) shall become effective on the date the standard is approved by an applicable government authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board or as otherwise provided for in that jurisdiction.

Retirement of Existing Standards:

The existing standard VAR-002-2b shall be retired at midnight of the day immediately prior to the effective date of VAR-002-2b(X).

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment November 20 – December 19~~,~~ 2013.

Description of Current Draft

The Project 2014-01 Dispersed Power Producing Resources drafting team is posting minor applicability revisions to VAR-002-3. The standard previously ~~, which~~ was adopted by the NERC Board of Trustees in May 2014 and is pending regulatory approval. The intent of the revisions is to clarify application of Requirements R4 and R5 to ~~BES~~ Bulk Electric Systems (BES) dispersed power producing resources included in the BES though Inclusion I4 of the BES definition.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Initial Ballot	June – July 2014
45-day Additional Formal Comment Period with Additional Ballot (if necessary)	August – September 2014
Final ballot	October 2014
BOT adoption	November 2014

DRAFT

Version History

Version	Date	Action	Change Tracking
1	5/1/2006	Added "(R2)" to the end of levels on non-compliance 2.1.2, 2.2.2, 2.3.2, and 2.4.3.	July 5, 2006
1a	12/19/2007	Added Appendix 1 – Interpretation of R1 and R2 approved by BOT on August 1, 2007	Revised
1a	1/16/2007	In Section A.2., Added "a" to end of standard number. Section F: added "1."; and added date.	Errata
1.1a	10/29/2008	BOT adopted errata changes; updated version number to "1.1a"	Errata
1.1b	3/3/2009	Added Appendix 2 – Interpretation of VAR-002-1.1a approved by BOT on February 10, 2009	Revised
2b	4/16/2013	Revised R1 to address an Interpretation Request. Also added previously approved VRFs, Time Horizons and VSLs. Revised R2 to address consistency issue with VAR-001-2, R4. FERC Order issued approving VAR-002-2b.	Revised
3	5/5/2014	Revised under Project 2013-04 to address outstanding Order 693 directives.	Revised
3	5/7/2014	Adopted by NERC Board of Trustees	
4	TBD	Revised under Project 2014-01 to clarify applicability of Requirements to BES dispersed power producing resources.	Revised

DRAFT

Definitions of Terms Used in the Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the NERC Glossary of Terms used in Reliability Standards (Glossary) are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None.

DRAFT

When this standard has received ballot approval, the text boxes within the Standard will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** **Generator Operation for Maintaining Network Voltage Schedules**

2. **Number:** VAR-002-4

3. **Purpose:** To ensure generators provide reactive support and voltage control, within generating Facility capabilities, in order to protect equipment and maintain reliable operation of the Interconnection.

4. **Applicability:**

   4.1. Generator Operator

   4.2. Generator Owner

5. **Effective Dates**

   The standard shall become effective on the later of the effective date of VAR-002-3, or the date the standard VAR-002-4 is approved by an applicable government authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction~~on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction~~.

The only revisions made to this version of VAR-002 are revisions to Requirements R4 and R5, to clarify applicability of the Requirements of the standard at generator Facilities. These applicability revisions are intended to clarify and provide for consistent application of the Requirements to BES generator Facilities included in the BES through Inclusion I4 – Dispersed Power Producing Resources.

The revisions to the two Requirements were made to VAR-002-3, which was approved by its ballot pool and adopted by the NERC Board in May 2014, VAR-002-3 is currently pending regulatory approval.

DRAFT

B. Requirements and Measures

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode as instructed by the Transmission Operator unless: 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following: *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- That the generator is being operated in start-up,[1] shutdown,[2] or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator; or
- That the generator is not being operated in automatic voltage control mode or in the control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing.

M1. The Generator Operator shall have evidence to show that it notified its associated Transmission Operator any time it failed to operate a generator in the automatic voltage control mode or in a different control mode as specified in Requirement R1. If a generator is being started up or shut down with the automatic voltage control off, or is being tested, and no notification of the AVR status is made to the Transmission Operator, the Generator Operator will have evidence that it notified the Transmission Operator of its procedure for placing the unit into automatic voltage control mode as required in Requirement R1. Such evidence may include, but is not limited to, dated evidence of transmittal of the procedure such as an electronic message or a transmittal letter with the procedure included or attached. If a generator is exempted, the Generator Operator shall also have evidence that the generator is exempted from being in automatic voltage control mode (with its AVR in service and controlling voltage).

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule[3] (within each generating Facility's capabilities[4]) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

2.1. When a generator's AVR is out of service or the generator does not have an AVR, the Generator Operator shall use an alternative method to control the generator reactive

[1] Start-up is deemed to have ended when the generator is ramped up to its minimum continuously sustainable load and the generator is prepared for continuous operation.

[2] Shutdown is deemed to begin when the generator is ramped down to its minimum continuously sustainable load and the generator is prepared to go offline.

[3] The voltage or Reactive Power schedule is a target value with a tolerance band or a voltage or Reactive Power range communicated by the Transmission Operator to the Generator Operator.

[4] Generating Facility capability may be established by test or other means, and may not be sufficient at times to pull the system voltage within the schedule tolerance band. Also, when a generator is operating in manual control, reactive power capability may change based on stability considerations.

output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

2.2. When instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

2.3. Generator Operators that do not monitor the voltage at the location specified in their voltage schedule shall have a methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

M2. In order to identify when a generator is deviating from its schedule, the Generator Operator will monitor voltage based on existing equipment at its Facility. The Generator Operator shall have evidence to show that the generator maintained the voltage or Reactive Power schedule provided by the Transmission Operator, or shall have evidence of meeting the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator. Evidence may include, but is not limited to, operator logs, SCADA data, phone logs, and any other notifications that would alert the Transmission Operator or otherwise demonstrate that the Generator Operator complied with the Transmission Operator's instructions for addressing deviations from the voltage or Reactive Power schedule.

For Part 2.1, when a generator's AVR is out of service or the generator does not have an AVR, a Generator Operator shall have evidence to show an alternative method was used to control the generator reactive output to meet the voltage or Reactive Power schedule provided by the Transmission Operator.

For Part 2.2, the Generator Operator shall have evidence that it complied with the Transmission Operator's instructions to modify its voltage or provided an explanation to the Transmission Operator of why the Generator Operator was unable to comply with the instruction. Evidence may include, but is not limited to, operator logs, SCADA data, and phone logs.

For Part 2.3, for Generator Operators that do not monitor the voltage at the location specified on the voltage schedule, the Generator Operator shall demonstrate the methodology for converting the scheduled voltage specified by the Transmission Operator to the voltage point being monitored by the Generator Operator.

~~**R7.**~~

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within 30 minutes of such change, then the Generator Operator is not required to notify the Transmission Operator of the status change *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

M3. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of any status change identified in Requirement R3. If the status has been restored within the first 30 minutes, no notification is necessary.

R4. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within 30 minutes of the Generator Operator becoming aware of such change, then the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

- Reporting of reactive capability changes is not applicable to the individual for dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition.

Rationale for Exclusion in R4:

VAR-002 addresses control and management of reactive resources and provides voltage control where it has an impact on the BES. For dispersed power producing resources as identified in Inclusion I4, Requirement R4 should not apply at the individual generator level due to the unique characteristics and small scale of individual dispersed power producing resources. In addition, other standards such as proposed TOP-003 require the Generator Operator to provide real time data as directed by the TOP.

M4. The Generator Operator shall have evidence it notified its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability in accordance with Requirement R4. If the capability has been restored within the first 30 minutes, no notification is necessary.

~~R4.~~R5. Each Generator Operator shall notify its associated Transmission Operator within 30 minutes of becoming aware of a change in reactive capability due to factors other than a status change described in Requirement R3. If the capability has been restored within 30 minutes of the Generator Operator becoming aware of such change, then the Generator Operator is not required to notify the Transmission Operator of the change in reactive capability. *[Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]*

~~4.1.~~5.1. For generator step-up transformers and auxiliary transformers[5] with primary

Rationale for Footnote 5 in Requirement R5, Part 5.1: The Transmission Operator / Transmission Provider needs to review tap settings on the main transformers that connect the generation to the high voltage system. The Transmission Operator / Transmission Provider must assure that the collector system (typically 34.5 kV) voltage coordinates with the voltage set-points and tolerance bands established by the Transmission Operator / Transmission. The portion of the collector system that aggregates 75 MVA or less of resources is excluded under I4 and the individual unit step-up transformers primarily affect the collector system, so it should also be excluded and left to the Generator Owner to design and manage based on the secondary voltages expected on the collector system.

[5] For dispersed power producing resources identified through Inclusion I4 of the Bulk Electric System definition, this requirement applies only to those transformers that have at least one winding at a voltage of 100 kV or above.

voltages equal to or greater than the generator terminal voltage:

~~4.1.1.~~5.1.1. Tap settings.

~~4.1.2.~~5.1.2. Available fixed tap ranges.

~~4.1.3.~~5.1.3. Impedance data.

M5. The Generator Owner shall have evidence it provided its associated Transmission Operator and Transmission Planner with information on its step-up transformers and auxiliary transformers as required in Requirement R5, Part 5.1.1 through Part 5.1.3 within 30 calendar days.

~~R5.~~R6. After consultation with the Transmission Operator regarding necessary step-up transformer tap changes, the Generator Owner shall ensure that transformer tap positions are changed according to the specifications provided by the Transmission Operator, unless such action would violate safety, an equipment rating, a regulatory requirement, or a statutory requirement. *[Violation Risk Factor: Lower] [Time Horizon: Real-time Operations]*

~~5.1.~~6.1. If the Generator Owner cannot comply with the Transmission Operator's specifications, the Generator Owner shall notify the Transmission Operator and shall provide the technical justification.

~~R8.~~R7. The Generator Owner shall have evidence that its step-up transformer taps were modified per the Transmission Operator's documentation in accordance with Requirement R6. The Generator Owner shall have evidence that it notified its associated Transmission Operator when it could not comply with the Transmission Operator's step-up transformer tap specifications in accordance with Requirement R6, Part 6.1.

DRAFT

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" refers to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

The Generator Owner shall keep its latest version of documentation on its step-up and auxiliary transformers. The Generator Operator shall maintain all other evidence for the current and previous calendar year.

The Compliance Monitor shall retain any audit data for three years.

1.3. Compliance Monitoring and Assessment Processes:

"Compliance Monitoring and Assessment Processes" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated reliability standard.

1.4. Additional Compliance Information:

None.

DRAFT

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Real-time Operations**	**Medium**	N/A	N/A	N/A	Unless exempted, the Generator Operator did not operate each generator connected to the interconnected transmission system in the automatic voltage control mode or in a different control mode as instructed by the Transmission Operator, and failed to provide the required notifications to Transmission Operator as identified in Requirement R1.
R2	**Real-time Operations**	**Medium**	N/A	N/A	The Generator Operator did not have a conversion methodology when it monitors voltage at a location different from the schedule provided by the Transmission Operator.	The Generator Operator did not maintain the voltage or Reactive Power schedule as instructed by the Transmission Operator and did not make the necessary notifications required by the Transmission Operator. OR The Generator Operator did not have an operating AVR, and the responsible entity did not use an alternative method for controlling voltage. OR The Generator Operator did not modify voltage when directed, and the

DRAFT

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						responsible entity did not provide any explanation.
R3	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of the status change.
R4	**Real-time Operations**	**Medium**	N/A	N/A	N/A	The Generator Operator did not make the required notification within 30 minutes of becoming aware of the capability change.
R5	**Real-time Operations**	**Lower**	N/A	N/A	The Generator Owner failed to provide its associated Transmission Operator and Transmission Planner one of the types of data specified in Requirement R5 Parts 5.1.1, 5.1.2, and 5.1.3.	The Generator Owner failed to provide to its associated Transmission Operator and Transmission Planner two or more of the types of data specified in Requirement R5 Parts 5.1.1, 5.1.2, and 5.1.3.
R6	**Real-time Operations**	**Lower**	N/A	N/A	N/A	The Generator Owner did not ensure the tap changes were made according the Transmission Operator's specifications.

DRAFT

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Generator Owner failed to perform the tap changes, and the Generator Owner did not provide technical justification for why it could not comply with the Transmission Operator specifications.

DRAFT

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

DRAFT

Guidelines and Technical Basis

For technical basis for each requirement, please review the rationale provided for each requirement.

Implementation Plan

Dispersed Generation Resources
VAR-002-4

Standards Involved
Approval:

- VAR-002-4 – Generator Operation for Maintaining Network Voltage Schedules

Retirement or Supersede:

- VAR-002-3 – Generator Operation for Maintaining Network Voltage Schedules

Prerequisite Approvals:
N/A

Background:
In light of the adoption of a revised "Bulk Electric System" definition by the Board of Trustees (Board), changes to the applicability sections of certain Reliability Standards, including VAR-002, are necessary to align with the implementation of the revised "Bulk Electric System" definition. The Standard Drafting Team (SDT) for Project 2014-01 – Standards Applicability for Dispersed Power Producing Resources has modified the applicability section of certain Generator Owner/Generator Operator requirements to recognize the unique technical and reliability aspects of dispersed generation in order to ensure the applicability of the standards is consistent with the reliable operation of the Bulk-Power System.

Effective Date
VAR-002-4 shall become effective on the later of the effective date of VAR-002-3, or the date the VAR-002-4 is approved by an applicable government authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board or as otherwise provided for in that jurisdiction.

Retirement of Existing Standards:
Proposed VAR-002-3, shall be retired at midnight of the day immediately prior to the effective date of VAR-002-4.

Standards Committee Project Management Oversight Subcommittee (PMOS) Update

Action

None requested. Update Only.

Background

The PMOS met in person on June 10, 2014. A verbal update of the items discussed will be provided at the SC meeting.

Agenda Item 9b
Standards Committee
June 10-11, 2014

Standards Committee Process Subcommittee Update

Action

Information only

Background

The Standards Committee Process Subcommittee (SCPS) continues to work on several projects. Detailed scope documents for the Consensus Building and SAR Development initiative and the Review of Standards Processes and Procedures task will be presented for endorsement. A report has been prepared as part of the Ballot Pool Management initiative. The SCPS and NERC Standards Information staff will present a resource package containing the active Standards resource documents on a common template to accompany the Drafting Team Guidelines at the July Standards Committee call. The SCPS also continues to work on the Cost Effective Analysis Process with NERC staff.

Addressing Failure to Achieve Quorum in Balloting Standards

Action

Informational update only

Background

Development or modification of a Reliability Standard requires industry balloting of the new Standard or modification. Per the current Standards Process Manual ballot pool approval requires a quorum, which is established by at least 75% of the members of a ballot pool submitting a response in addition to a two-thirds majority of the weighted Segments votes being affirmative. Several ballots have recently experienced failure to achieve the required quorum by the end of the specified voting window, necessitating extension of the voting window. In light of the recent challenges in reaching quorum at the end of the announced voting window, the Standards Committee Process Subcommittee (SCPS) and NERC staff have been "exploring options to create and maintain an effective ballot pool and strategies to address situations where a quorum is not reached by the time a ballot period is scheduled to close." November 2013 SC Agenda item 13 (a) iii. This effort has coincided with development and implementation of the new Standards Balloting System (SBS). This update contains steps taken to date to facilitate reaching quorum in a timely manner, actions being taken on ballots using the original (current) balloting system, enhancements and features of the new Standards Balloting System that are anticipated to improve the reaching quorum, and future plans for analysis and action.

Steps Taken to Date

NERC Standards Information staff has taken the following actions in 2012 and 2013 to address identified challenges to gaining quorum for ballots.

1. The Registered Ballot Body (RBB) was reviewed for members with no activity on their voting records for one year or longer. Members were sent a letter, emailed and/or called. Non-responsive members were removed from the RBB. 41 members were contacted, with seven RBB members removed and nine proxy pool members removed. This review will be performed annually.
2. Segment 8 of the RBB (Small Electricity Users) was reviewed to ensure members were accurately registered.
3. A review of the RBB's Segment representation, as directed in the Appendix 3D Registered Ballot Body Criteria of the NERC Rules of Procedure was performed. Based on the registration responses, the RBB was reviewed and updated.
4. Members of ballot pools who are no longer able to vote due to company mergers were removed from ballot pools and from the RBB.
5. A comparison between RBB and ballot pools to remove members in older ballot pools that are no longer voting members was initiated.

Actions Currently Being Taken

Several actions are being taken with the current ballot pools to encourage reaching a quorum before the voting window closes. Some of these are interim measures necessary at least until projects are transitioned to the new SBS, at which time longer term management can be evaluated.

1. The cleanup of ballot pools mentioned above is continuing prior to the ballot start date. This includes consideration of the effects of company mergers and the comparison of ballot pool membership to the RBB.
2. A contractor has been working with Standards Information staff to perform queries on ballot pools from September 2013 to March 2014 for further analysis. A preliminary query was performed on Segment 10 (Regional Entities) and is being used to refine the specifications for future queries. NERC is developing the capability to perform the queries and will be using the results along with the SCPS members to inform future strategies.
3. Analysis of ballot pools that have been extended is being performed by NERC Standards Information staff. A table containing the balloted projects in 2014 is included.
4. NERC Standards Information staff is communicating to industry voters the importance of abstaining when ballot pools are joined and they do not intend to vote in a particular ballot. These communications included a "Balloting 101" email and reminders at the Standards and Compliance Workshop.
5. An annual review of the RBB's Segment representation will be performed.
6. Reminders are being sent to individuals who have not voted and/or others in their company near the end of a voting window if quorum has not been achieved. Standards Committee leadership has also been assisting with contacting ballot pool members and the Trades to encourage voting.

Potential Improvements in new Software Balloting System (SBS)

Certain enhancements and features that have been built into the new SBS are anticipated to generate improvement in reaching quorum, both during initialization of the system and on an ongoing basis. Examples include:

1. New registration will be required for accessing voting in the new system, improving the cleanup of the RBB.
2. Proxies can be designated until the close of the ballot voting window making voting more accessible. Currently proxy designation can only be accomplished during ballot pool formation.
3. The "My Ballot Activity" section provides a single page view to join, vote and designate proxies, making managing voting activities easier.
4. The Replacement Voter feature allows a voter representing a segment to exit the RBB and be replaced by a new voter who can assume voting activities in the ballot pools.

Future Plans for Analysis and Action

The SCPS and NERC Standards Information staff will monitor the results of both the management strategies being implemented and the enhancements contained in the new SBS. NERC Standards Information staff will also continue the analysis already initiated into the causes of difficulties in achieving quorum in ballot pools. Based on the information gathered, the SCPS and NERC Standards Information staff will evaluate whether additional measures are necessary. An initial list of strategies for consideration has been developed to serve as a starting point if the problem persists. This list is for consideration only and has not been evaluated for practicality or effectiveness.

Suggestions/Ideas

Consider changes to proxy process – allow for multiple proxies, associate proxies with RBB Registered Entity rather than each individual standard.

Ballot pool (or ballot body) members who demonstrate poor voting performance should be replaced if they miss a defined number of votes.

Put an expiration date on a ballot pool – if the pool expires it will have to be "reinitialized", or ballot pool members could be asked to confirm their intent to remain in the pool.

Look at lowering the quorum % to address lack of quorum due to "poor performance".

Allow multiple individuals from a Registered Entity to join the RBB according to their specialty and then only allow one to join the ballot pool (for example an operations person or a CIP person).

Draft agreement for RBB Members defining responsibilities.

Have voters voluntarily notify NERC when they join the ballot pool that in the event they fail to vote by the voting deadline that their vote should be recorded as an abstention.

Analysis of Issues Achieving a Quorum (Jan 1-May 22, 2014)

Project Name and Number	Standard	Ballot Type	Ballot Start Date	Ballot End Date	# of Days Extended
Project 2007-02 - Operating Personnel Communications Protocols	COM-002-4	Additional Ballot	01/22/14	02/04/14	2
Project 2008-12 - Coordinate Interchange Standards	Definitions	Additional Ballot	01/16/14	01/29/14	2
Project 2008-12 - Coordinate Interchange Standards	INT-004-3 and INT-010-2	Additional Ballot	01/10/14	01/22/14	0
Project 2010-01 - Training	PER-005-2	Additional Ballot	01/08/14	01/21/14	1
Project 2010-02 - Connecting Facilities to the Grid	FAC-001-2 and FAC-002-2	Initial Ballot	05/06/14	05/16/14	1
Project 2010-03 - Modeling Data (MOD B)	MOD-033-1	Additional Ballot	01/10/14	01/22/14	1
Project 2010-04 - Demand Data (MOD C)	MOD-031-1	Additional Ballot	04/01/14	04/14/14	2
Project 2010-05.1 - Protection System: Phase 1 (Misoperations)	PRC-004-3	Additional Ballot	02/21/14	03/11/14	6
Project 2012-13 - NUC - Nuclear Plant Interface Coordination	NUC-001-3	Initial Ballot	05/13/14	05/22/14	0
Project 2013-04 - Voltage and Reactive Control	VAR-002-3	Additional Ballot	04/04/14	04/16/14	2
Project 2014-04 - Physical Security	CIP-014-1	Initial Ballot	04/20/14	04/24/14	0

Agenda Item 9b ii
Standards Committee
June 10-11, 2014

Consensus Building and SAR Development

Action

Discuss and endorse the attached proposed scope for the development of a holistic process on consensus building and SAR development associated with proposed standard development projects.

Background

In early 2013, the Standards Committee Process Subcommittee (SCPS) proposed a concept and drafted a process document to improve SAR development with a focus on obtaining sufficient technical information to support SAR posting. The Standards Committee supported the concept, and directed the SCSP to provide further details on the proposed process. By September 2013, the SCPS developed a final draft process document but decided to withhold presenting it to the SC for approval pending the completion of a parallel effort to develop the concept and process to improve consensus building for standard projects through informal outreach.

At the December 2013 meeting, the SC adopted a preferred option (Option C) to enhance consensus building. In view of the interrelationship between consensus building and SAR development, the SC, SCPS and PMOS leadership proposed that a combined task be undertaken to develop a holistic process that will improve the effectiveness and efficiency of consensus building for standard projects starting at or before the initial project proposal stage and continuing to the acceptance/approval of the SAR by the Standards Committee. The SCPS volunteered to take the lead for this task.

The attached scope document on consensus building and SAR development has been reviewed and commented by the SC leadership, the SCPS and PMOS, and NERC staff. The SCPS is seeking the SC's approval of the proposed scope document, and to add this task to the SCPS work plan.

Date: May 22, 2014

Scope of NERC SCPS Project
Consensus Building for Standard Authorization Request (SAR) Development

Need for Project:

To develop a process which will facilitate the effective and efficient development of technical information and building of industry consensus leading to the Standards Committee's acceptance/approval of the SAR for proposed standard projects.

Project Scope Statement:

The objective of this task is to develop a new or revised process which will improve the effectiveness and efficiency of consensus building tasks for standard projects starting at or before the initial project proposal stage and continuing to the acceptance/approval of the SAR by the Standards Committee.

A standard project can be initiated by any one of the following means:

a. Recommendation by the Reliability Issues Steering Committee (RISC) to address an emerging reliability risk/issue;

b. Compliance with, or a response to, directives by regulatory authorities or the NERC Board of Trustees;

c. A review/revision or need identified in the Standards Committee's Reliability Standards Development Plan (RSDP);

d. A request by industry participants through the submission of a SAR;

e. Input by a stakeholder into the Single Portal for a potential reliability related issue.

This project will require a comprehensive review of the existing SAR and Informal development processes and proposing changes- , where appropriate, to improve effectiveness and efficiency in consensus building activities leading to the posting and acceptance/approval of the SAR. The project also will have to be fully coordinated with the RISC, PMOS and other SC activities and SCPS projects. The project is to be conducted in 2 stages.

<u>Stage 1</u> (March 2014 to September 2014)

Develop a revised process that covers the following key activities:

- Collection of technical information needed to support the proposal for a standard project;
- Informal outreach and consensus building on the need and scope of the project;
- Drafting/revising the SAR to achieve clarity with sufficient technical information that supports the proposed purpose and scope of project;

- Posting of SAR and responding to public comments, and revising SAR to address industry comments;
- Consider conducting a Cost Impact Analysis (CIA) as outlined in the NERC Cost Effective Analysis Process Phase 1 to determine potential cost impacts of potential proposed solutions;
- Recommending acceptance/approval/rejection of the SAR to the SC with due consideration given to industry input.

The role of the RISC throughout these activities should be considered and clearly stated as appropriate.

Stage 2 (Latter Part of 2014 to Early 2015)

Revise the Standard Processes Manual to incorporate pertinent elements of the revised process.

Resources:
A small team comprising of 4-5 SCPS members, 1-2 PMOS members and 1-2 NERC Standards and NERC Legal staff.

Stage 1 is expected to start in March 2014 ending September 2014; Stage 2 is expected to start in the latter part of 2014 in conjunction with other SPM changes following the completion of another SCPS task to improve the effectiveness and efficiency of standards development, including balloting.

Standards Committee Strategic Work Plan 2013-2015, Task No. 2: Review of the Standards Processes and Procedures

Action
Endorse.

Background
Task No. 2: Review of the Standards Processes and Procedures:
Implement revisions needed to NERC's Rules of Procedure/SPM and SC processes and procedures to enhance SC and SDT accountability to timely deliver high quality Reliability Standards and execute the Strategic Plan, including the completion of Standards Process Input Group (SPIG) recommendations. All revisions, creation or elimination of processes and procedures provisions shall be presented to the SC for adoption, prior to presenting to the NERC Board of Trustees (BOT) for approval.

Steps Taken to Date:
Two questionnaires were sent seeking feedback in the early part of 2013. The first questionnaire was sent to standards drafting teams to determine areas for improvement in the standard development process. Although a few suggestions were made regarding legal representation on the standard drafting teams, there were no substantive improvements identified for process improvement.

A second questionnaire was sent to a broader audience which focused on asking for a "single biggest issue" with all aspects of the standard development process. This also concluded with no centralized issue to be identified.

Future Plans for Action:
The Task #2 Team noted a limited number of NERC Projects that have been through the revision of the current Standard Process Manual; those that were completed under the new manual were either informal development or were expedited due to FERC directives (MODs, VARs, PER-005, GMD, and CIP-014). The task team felt that evaluating additional projects which undergo formal development with the current Process Manual would allow a more comprehensive review. Additionally, it was noted that polling industry at this time would be deemed problematic due to the number of Project postings.

The recommendation of the task group was unanimous; "keep the scoping document but postpone any actions". The group noted that an outreach plan other than a survey should be considered. The task team also makes the following suggestions: 1) standing committees be solicited for outreach options, and 2) include outreach for this task as an agenda topic during compliance workshops.

A proposed starting time for Task #2 is second quarter of 2015.

Agenda Item 10
Standards Committee
June 10-11, 2014

Standards Committee Communications Updates and Activities

Action
Information only.

Background
Mallory Huggins of NERC Staff and Scott Miller will provide an update on NERC and Standards Committee communication activities in the last month.

May 2014

NERC Legal and Regulatory Filings - Standards

RECENT FILINGS

DATE	PROJECT/DESCRIPTION
March 7, 2014	Petition of NERC for Approval of Proposed Reliability Standard PER-005-2 and Retirement of Reliability Standard PER-005-1. Docket No. RD14-7
March 10, 2014	Doc-Less Motion to Intervene in Docket No. RD14-6-000
March 12, 2014	Petition of NERC for Approval of Interpretation of Regional Reliability Standard TOP-007-WECC-1. Docket Nos. RM09-14 and RD14-8
March 18, 2014	Request of NERC for Extension of Time to File Revisions to the Violation Risk Factors Assigned to Reliability Standards CIP-006-5, Requirement R3 and CIP-004-5, Requirement R4. Docket No. RM13-5
March 24, 2014	Comments of NERC in Response to Notice of Proposed Rulemaking EOP-010-1 (Geomagnetic Disturbance Operations). Docket No. RM14-1
March 31, 2014	NERC Standards Report, Status and Timetable for Processing Regulatory Directives. Docket No. RR09-6
April 1, 2014	TOP/IRO Quarterly Status Report. Docket No. RM13-12, RM13-14, RM3-15
April 2, 2014	Petition of NERC for Approval of Reliability Standard BAL-001-2 (Real Power Balancing Control Performance). Docket No. RM14-10
April 21, 2014	Comments of NERC in Response to Notice of Proposed Rulemaking PRC-025-1 and PRC-023-3 (Generator Relay Loadability and Revised Transmission Relay Loadability). Docket No. RM13-19 and RM14-3
May 9, 2014	Supplemental Information to Petition of NERC for Approval of Reliability Standard BAL-001-2 (Real Power Balancing Control Performance). Docket No. RM14-10.
May 13, 2014	Petition of NERC for Approval of Proposed Reliability Standard MOD-031-1 and Retirement of Reliability Standards MOD-016-1.1, MOD-017-0.1, MOD-018-0, MOD-019-0.1, and MOD-021-1. Docket No. RM14-12.
May 14, 2014	Petition of NERC for Approval of Proposed Reliability Standards COM-001-2 and COM-002-4. Docket No. RM14-13.
May 15, 2014	NERC Revisions to the Violation Risk Factors and Violation Severity Levels Assigned to Certain Critical Infrastructure Protection Reliability Standards. Docket No. RM13-5.
May 15, 2015	Errata to Petition of NERC for Approval of Proposed Reliability Standards COM-001-2 and COM-002-4. Docket No. RM14-13.
May 20, 2014	Quarterly Nova Scotia filing
May 23, 2014	Petition of NERC for Approval of Proposed Reliability Standard CIP-014-1. Docket No. RM14-15.

UPCOMING FILING DATES

DATE	PROJECT/DESCRIPTION
May 31, 2014	Quarterly filing regarding timeframe to restore power to the auxiliary systems of nuclear power plants

PROJECTED FILINGS

STATUS	PROJECT/DESCRIPTION
Scheduled for BOT, May 2014 Projected Filing Date: June 6, 2014	Petition for Approval of Proposed Reliability Standards VAR-001-4 and VAR-002-3

Project 2013-03 Geomagnetic Disturbance Mitigation

Action

Authorize posting draft TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance (GMD) Events, Violation Risk Factors/Violation Severity Levels, and associated implementation plan for 45-day comment and initial ballot (and a non-binding poll for VRFs and VSLs), with ballot pool formation during the first 30 days and initial ballot and non-binding poll during the last 10 days of the 45-day period.

Background

On May 16, 2013, FERC issued Order No. 779 directing NERC to develop Reliability Standards addressing the potential impact of GMDs in two stages:

- Stage 1 Standard requiring applicable entities to implement Operating Procedures. EOP-010-1 – GMD Operations was adopted by the Board of Trustees and filed at FERC in November 2013.
- Stage 2 Standard(s) requiring applicable entities to conduct assessments of the impacts of benchmark GMD events on their systems and requiring the development and implementation of a plan to mitigate the risk of instability, uncontrolled separation, or cascading, if impacts are identified. FERC established a filing deadline of January 21, 2015 for Stage 2.

The Standard Drafting Team (SDT) developed proposed standard TPL-007-1, the Benchmark GMD Event Description white paper, and the Transformer Thermal Impact Assessment white paper to meet the stage 2 directives. The proposed standard is applicable to Planning Coordinators, Transmission Planners, Transmission Owners, and Generator Owners with areas or transformers connected at 200 kV or higher. It includes requirements for planning entities to assess GMD impacts from a 1-in-100 year benchmark GMD event and develop mitigation plans to address identified issues. The standard also includes requirements for owners to assess the thermal impact of a benchmark event on applicable transformers.

The benchmark GMD event was developed through statistical analysis and can be tailored to the specific location of the system being studied as described in the white paper.

After obtaining initial feedback from the GMD Task Force (GMDTF) during the GMDTF meeting in February 2014, drafts were posted for informal comment from April 22 – May 21, 2014. During the informal comment period, the SDT conducted a webinar, technical conference, and participated in several calls with various stakeholder groups.

The draft standard includes revisions to address concerns raised by stakeholders, including clarifying responsibilities within the standard as well as clarifying the sequence of required performance to address interdependent Requirements. On June 2, 2014, NERC staff from Standards, Legal, and Compliance conducted a quality review (QR) of the draft standard and Implementation Plan. Following the QR, the SDT made numerous revisions responsive to the QR feedback.

Given the newness of tools and analysis capabilities for assessing GMD impacts and the timeframe in which NERC has been provided to develop the Stage 2 GMD Standard, the SDT has a proactive communication plan underway to inform and educate stakeholders. This plan

includes additional webinars, a technical conference during the comment period, and communication with NERC, region, and trade group committees.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. The Standards Committee accepted the Standard Authorization Request (SAR) submitted by the Geomagnetic Disturbance Task Force (GMD TF) and approved Project 2013-03 (Geomagnetic Disturbance Mitigation) on June 5, 2013.
2. The SAR was posted for informal comment from June 26, 2013 through August 12, 2013.

Description of Current Draft

This is the first draft of the proposed Reliability Standard. It is posted for 45-day comment and initial ballot.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Initial Ballot	June 2014
45-day Formal Comment Period with Additional Ballot	August 2014
Final ballot	October 2014
BOT adoption	November 2014

Effective Dates

The definition shall become effective on the first day of the first calendar quarter after the date that this standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the definition shall become effective on the first day of the first calendar quarter after the date this standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

The Requirements shall become effective as described in the Implementation Plan beginning on the first day of the first calendar quarter that is 12 months after the date that this standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the Requirements shall become effective as described in the Implementation Plan beginning on the first day of the first calendar quarter that is 12 months after the date this standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Compliance shall be implemented over a 4-year period as described in the Implementation Plan.

Version History

Version	Date	Action	Change Tracking
1	TBD	Project 2013-03 (Phase 2)	N/A

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Geomagnetic Disturbance Vulnerability Assessment or GMD Vulnerability Assessment: Documented evaluation of potential susceptibility to voltage collapse, Cascading, or localized damage of equipment due to geomagnetic disturbances.

A. Introduction

1. **Title: Transmission System Planned Performance for Geomagnetic Disturbance Events**

2. **Number:** TPL-007-1

3. **Purpose:** Establish requirements for Transmission system planned performance during geomagnetic disturbance (GMD) events.

4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Planning Coordinator with a planning area that includes a Facility or Facilities specified in 4.2;
   4.1.2 Transmission Planner with a planning area that includes a Facility or Facilities specified in 4.2;
   4.1.3 Transmission Owner who owns a Facility or Facilities specified in 4.2;
   4.1.4 Generator Owner who owns a Facility or Facilities specified in 4.2.

   4.2. Facilities:

   4.2.1 Facilities that include power transformer(s) with high side, wye-grounded winding with terminal voltage greater than 200 kV.

Rationale: Instrumentation transformers and station service transformers do not have significant impact on GIC flows; therefore, they are not included in the applicability for this standard.

5. **Background:**

During a GMD event, geomagnetically-induced currents (GIC) may cause transformer hot-spot heating or damage, loss of Reactive Power sources, increased Reactive Power demand, and Misoperation, the combination of which may result in voltage collapse and blackout.

B. Requirements and Measures

R1. Each Planning Coordinator, in conjunction with each of its Transmission Planners, shall identify the individual and joint responsibilities of the Planning Coordinator and each of the Transmission Planners in the Planning Coordinator's planning area for maintaining models and performing the studies needed to complete GMD Vulnerability Assessment(s). *[Violation Risk Factor: Low] [Time Horizon: Long-term Planning]*

M1. Each Planning Coordinator, in conjunction with each of its Transmission Planners, shall provide documentation on roles and responsibilities, such as meeting minutes,

agreements, and email correspondence that identifies that agreement has been reached on individual and joint responsibilities for maintaining models and performing the studies needed to complete GMD Vulnerability Assessment(s) in accordance with Requirement R1.

R2. Responsible entities, as determined in Requirement R1, shall maintain System models and geomagnetically-induced current (GIC) System models of the responsible entity's planning area for performing the studies needed to complete GMD Vulnerability Assessment(s). *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M2. A responsible entity, as determined in Requirement R1, shall have evidence in either electronic or hard copy format that it is maintaining System models and GIC System models of the responsible entity's planning area for performing the studies needed to complete GMD Vulnerability Assessment(s).

Rationale for Requirement R2:

A GMD Vulnerability Assessment requires a GIC System model to calculate GIC flow which is used to determine transformer Reactive Power absorption and transformer thermal response. Guidance for developing the GIC System model are provided in the GIC Application Guide developed by the NERC GMD Task Force and available at: http://www.nerc.com/comm/PC/Geomagnetic%20Disturbance%20Task%20Force%20GMDTF%202013/GIC%20Application%20Guide%202013_approved.pdf

The System model specified in Requirement R2 is used in conducting steady state power flow analysis that accounts for the Reactive Power absorption of transformers due to GIC in the System.

The projected System condition for GMD planning may include adjustments to the System that are executable in response to space weather information. These adjustments could include recalling or postponing maintenance outages, for example.

R3. Responsible entities, as determined in Requirement R1, shall complete a GMD Vulnerability Assessment of the Near-Term Transmission Planning Horizon once every 60 calendar months. This GMD Vulnerability Assessment shall use studies based on models identified in Requirement R2, document assumptions, and document summarized results of the steady state analysis. *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

3.1. Studies shall include the following conditions:

3.1.1. System peak Load for at least one year within the Near-Term Transmission Planning Horizon; and

3.1.2. System Off-Peak Load for at least one year within the Near-Term Transmission Planning Horizon.

3.2. Studies shall be conducted based on the benchmark GMD event described in Attachment 1 to determine whether the system meets the performance requirements in Table 1.

3.3. The GMD Vulnerability Assessment shall be provided within 90 days of completion to the responsible entity's Reliability Coordinator, adjacent Planning Coordinators, adjacent Transmission Planners, and to any functional entity that submits a written request and has a reliability related need.

3.3.1 If a recipient of the GMD Vulnerability Assessment provides documented comments on the results, the responsible entity shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.

M3. A responsible entity, as determined in Requirement R1, shall have dated evidence such as electronic or hard copies of its GMD Vulnerability Assessment that meet all of the requirements in Requirement R3. A Responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date that it has distributed its GMD Vulnerability Assessment within 90 calendar days of completion to its Reliability Coordinator, adjacent Planning Coordinators, adjacent Transmission Planners, and to any functional entity who has submitted a written request indicating a reliability related need as specified in Requirement R3. A responsible entities, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date that it has provided a documented response to comments received on its GMD Vulnerability Assessment within 90 calendar days of receipt of those comments in accordance with Requirement R3.

Rationale for Requirement R3:

The GMD Vulnerability Assessment includes steady state power flow analysis and supporting studies using the models specified in Requirement R2 that account for the effects of GIC. Performance criteria are specified in Table 1.

System peak Load and Off-peak Load must be examined in the analysis.

Distribution of GMD Vulnerability Assessment results provides a means for sharing relevant information with other entities responsible for planning reliability. Results of GIC studies may affect neighboring systems and should be taken into account by planners.

The GMD Planning Guide developed by the NERC GMD Task Force provides technical information on GMD-specific considerations for planning studies. It is available at:

http://www.nerc.com/comm/PC/Geomagnetic%20Disturbance%20Task%20Force%20GMDTF%202013/GMD%20Planning%20Guide_approved.pdf

R4. Responsible entities, as determined in Requirement R1, shall have criteria for acceptable System steady state voltage limits for its System during the benchmark GMD event described in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

M4. A responsible entity, as determined in Requirement R1, shall have evidence such as electronic or hard copies of the criteria for acceptable System steady state voltage limits for its System in accordance with Requirement R4.

Rationale for Requirement R4:

System steady state voltage limits for GMD Vulnerability Assessment may by different from the limits used in the TPL-001 Planning Assessment. The planner must adhere to established limits that ensure the planned System achieves the performance requirements in Table 1.

R5. Responsible entities, as determined in Requirement R1, shall provide geomagnetically-induced current (GIC) flow information to be used for the transformer thermal impact assessment specified in Requirement R6 to each Transmission Owner and Generator Owner in the planning area that owns an applicable power transformer. The GIC flow information shall include for each applicable power transformer: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

5.1 Maximum effective GIC value for the worst case geoelectric field orientation for the benchmark GMD event described in Attachment 1; and

5.2 Effective GIC time series, GIC(t), calculated using the benchmark GMD event described in Attachment 1 for each applicable power transformer where the Maximum effective GIC value for the worst case geoelectric field orientation exceeds 15 Amperes per phase.

M5. A Responsible entity, as determined in Requirement R1, shall provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date that it has provided GIC flow information to each Transmission Owner and Generator Owner that owns an applicable power transformer as specified in Requirement R5.

Rationale for Requirement R5:

This GIC information is necessary for determining the thermal impact of GIC on transformers in the planning area and must be provided to entities responsible for performing the thermal impact assessment so that they can accurately perform the assessment.

The GIC flows provided in part 5.1 are used to screen the transformer fleet such that only those transformers that experience an effective GIC flow of 15A or greater are evaluated.

The GIC flows provided by part 5.2 and 5.3 are used to convert the steady-state GIC flows to time-series GIC data used for transformer thermal impact assessment. Additional guidance is available in the Thermal Impact Assessment white paper:

http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx

R6. Each Transmission Owner and Generator Owner shall conduct a thermal impact assessment for each of its solely and jointly owned applicable power transformers where

the maximum effective geomagnetically-induced current (GIC) value provided in Requirement R5 part 5.1 is 15 Amperes or greater per phase. The thermal impact assessment shall: *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

6.1. Be based on the effective GIC flow information provided in Requirement R5;
6.2. Document assumptions used in the analysis;
6.3. Describe suggested actions and supporting analysis to mitigate the impact of GICs, if any; and
6.4. Be performed and provided to the responsible entities, as determined in Requirement R1, within 12 calendar months of receiving GIC flow information specified in Requirement R5.

M6. Each Transmission Owner and Generator Owner shall have evidence such as electronic or hard copies of thermal impact assessment for all of its applicable solely and jointly owned power transformers where maximum effective GIC value provided in Requirement R5 part 5.1 is 15 Amperes or greater per phase as specified in Requirement R6.

Rationale for Requirement R6:

The thermal impact assessment may be based on manufacturer-provided GIC capability curves, thermal response simulation, or other technically justified means. A process for conducting the assessment is presented in the Transformer Thermal Impact Assessment white paper posted on the project page.

http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx

R7. Responsible entities, as determined in Requirement R1, that conclude through the GMD Vulnerability Assessment conducted in Requirement R3 that their System does not meet the performance requirements of Table 1 shall develop a Corrective Action Plan addressing how the performance requirements will be met. The Corrective Action Plan shall: *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

7.1. List System deficiencies and the associated actions needed to achieve required System performance. Examples of such actions include:

- Installation, modification, retirement, or removal of Transmission and generation Facilities and any associated equipment.
- Installation, modification, or removal of Protection Systems or Special Protection Systems.
- Use of Operating Procedures specifying how long they will be needed as part of the Corrective Action Plan.
- Use of Demand-Side Management, new technologies, or other initiatives.

7.2. Be reviewed in subsequent GMD Vulnerability Assessments until it is determined that the System meets the performance requirements contained in Table 1; and

7.3. Be provided within 90 days of completion to the responsible entity's Reliability Coordinator, adjacent Planning Coordinators, adjacent Transmission Planners,

and to any functional entity that submits a written request and has a reliability related need.

7.3.1. If a recipient of the Corrective Action Plan provides documented comments on the results, the responsible entity shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.

M7. A Responsible entity, as determined in Requirement R1, that concludes through the GMD Vulnerability Assessment conducted in Requirement R3 that the responsible entity's System does not meet the performance requirements of Table 1 shall have evidence, such as electronic or hard copies of its Corrective Action Plan as specified in Requirement R7. A responsible entity, as determined in Requirement R1, shall also provide evidence, such as email records, web postings with an electronic notice of posting, or postal receipts showing recipient and date that it has distributed any developed Corrective Action Plan within 90 calendar days of its completion to its Reliability Coordinator, adjacent Planning Coordinators, adjacent Transmission Planners, and to any functional entity who has indicated a reliability related need as specified in Requirement R7. A responsible entity, as determined in Requirement R1, shall also provide evidence, such as email notices or postal receipts showing recipient and date that it has provided a documented response to comments received on its Corrective Action Plan within 90 calendar days of receipt of those comments in accordance with Requirement R7.

Table 1 –Steady State Planning Events

Steady State:

a. The System shall remain stable. Cascading and uncontrolled islanding shall not occur.

b. Load loss as well as generation loss is acceptable as a consequence of the planning event.

c. Planned System adjustments such as Transmission configuration changes and re-dispatch of generation are allowed if such adjustments are executable within the time duration applicable to the Facility Ratings.

d. System steady state voltages shall be within acceptable limits as established by the Planning Coordinator and the Transmission Planner in accordance with Requirement R4.

Category	Initial Condition	Event	Interruption of Firm Transmission Service Allowed	Load Loss Allowed
GMD GMD Event with Outages	1. System as may be postured in response to space weather information[1], and then 2. GMD event[2]	Reactive Power compensation devices and other Transmission Facilities removed as a result of Protection System operation during the GMD event[3]	Yes[4]	Yes[4]

Table 1 – Steady State Performance Footnotes

1. The System condition for GMD planning may include adjustments to posture the System that are executable in response to space weather information.
2. The GMD conditions for the planning event are described in Attachment 1 (Benchmark GMD Event).
3. Protection Systems may trip due to the effects of harmonics. GMD planning analysis shall consider removal of equipment that the planner determines may be susceptible.
4. The objective of the GMD Vulnerability Assessment is to prevent instability, uncontrolled separation, Cascading and uncontrolled islanding of the System during a GMD event. Load loss and/or curtailment of Firm Transmission Service may be needed to meet BES performance requirements during studied GMD conditions but should not be used as the primary method of achieving required performance. GMD Operating Procedures should be based on predetermined triggers from studied GMD conditions so that the likelihood and magnitude of Load loss or curtailment of Firm Transmission Service is minimized during a GMD event.

Attachment 1

Calculating Geoelectric Fields for the Benchmark GMD Event

The benchmark GMD event[1] defines the geoelectric field values used to compute geomagnetically-induced current (GIC) flows that are needed to conduct a GMD Vulnerability Assessment. It is composed of the following elements: (1) a reference peak geoelectric field amplitude of 8 V/km derived from statistical analysis of historical magnetometer data; (2) scaling factors to account for local geomagnetic latitude; (3) scaling factors to account for local earth conductivity; and (4) a reference geomagnetic field time series or waveshape to facilitate time-domain analysis of GMD impact on equipment.

The regional geoelectric field peak amplitude to be used in GMD Vulnerability Assessment, E_{peak}, can be obtained from the reference geoelectric field value of 8 V/km using the following relationship

$$E_{peak} = 8 \times \alpha \times \beta \text{ (V/km)}$$

where α is the scaling factor to account for local geomagnetic latitude, and β is a scaling factor to account for the local earth conductivity structure.

Scaling the Geomagnetic Field

The benchmark GMD event is defined for geomagnetic latitude of 60° and it must be scaled to account for regional differences based on geomagnetic latitude. Table 2 provides a scaling factor correlating peak geoelectric field to geomagnetic latitude. Alternatively, the scaling factor α can be computed with the empirical expression

$$\alpha = 0.001 \cdot e^{(0.115 \cdot L)}$$

where L is the geomagnetic latitude in degrees and $0.1 \leq \alpha \leq 1$

For large planning areas that cover more than one scaling factor from Table 2, the most conservative (largest) value for α should be used in scaling the geomagnetic field. Alternatively, a planner could use a tool that is capable of performing analysis using a non-uniform or piecewise uniform geomagnetic field.

[1] The benchmark GMD event description is available on the Project 2013-03 Geomagnetic Disturbance Mitigation project page:http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx

Table 2: Geomagnetic Field Scaling Factors	
Geomagnetic Latitude (Degrees)	**Scaling Factor1 (α)**
≤ 40	0.10
45	0.2
50	0.3
54	0.5
56	0.6
57	0.7
58	0.8
59	0.9
≥ 60	1.0

Scaling the Geoelectric Field

The benchmark GMD event is defined for the reference Quebec earth model described in Table 4. The peak geoelectric field, E_{peak}, to be used in a GMD Vulnerability Assessment may be obtained by either

- Calculating the geoelectric field for the ground conductivity in the planning area and the reference geomagnetic field time series scaled according to geomagnetic latitude, using a procedure such as the plane wave method described in the NERC GMD Task Force GIC Application Guide[2]; or
- Using the earth conductivity scaling factor β from Table 3 that correlates to the ground conductivity map in Figure 1 or Figure 2. Along with the scaling factor α, β is applied to the reference geolectric field using the following equation to obtain the regional geoelectric field peak amplitude E_{peak} to be used in GMD Vulnerability Assessment. When a ground conductivity model is not available the planning entity should use a β factor of 1 or a technically-justified value.

$$E_{peak} = 8 \times \alpha \times \beta \text{ (V/km)}$$

The earth models used to calculate Table 3 for the United States were obtained from publicly available magnetotelluric data that is published on the U. S. Geological Survey website[3]. The models used to calculate Table 3 for Canada were obtained from Natural Resources Canada (NRCan) and reflect the average structure for large regions. NRCan also has developed some models for sub-regions which should be used when available. Because all models in Table 3 are approximations, a planner can substitute a technically justified earth model for its planning area when available.

[2] Available at the NERC GMD Task Force project page: http://www.nerc.com/comm/PC/Pages/Geomagnetic-Disturbance-Task-Force-(GMDTF)-2013.aspx

[3] Available at http://geomag.usgs.gov/conductivity/

For large planning areas that cover more than one scaling factor from Table 3, the most conservative (largest) value for β should be used in scaling the geoelectric field. Alternatively, a planner could use a tool that is capable of performing analysis using a non-uniform or piecewise uniform geoelectric field.

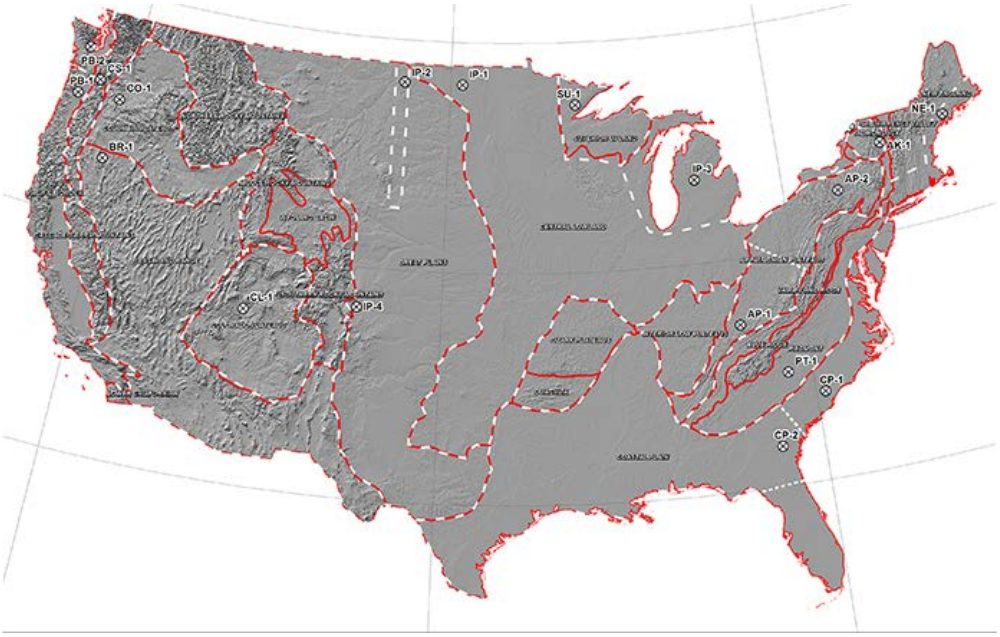


Figure 1: Physiographic Regions of the Continental United States[4]

Figure 2: Physiographic Regions of Canada

[4] Additional map detail is available at the U.S. Geological Survey (http://geomag.usgs.gov/)

Table 3 Geoelectric Field Scaling Factors	
USGS Earth model	Scaling Factor (β)
AK1A	0.56
AK1B	.0.56
AP1	0.33
AP2	0.82
BR1	0.22
CL1	0.76
CO1	0.27
CP1	0.81
CP2	0.95
CS1	0.41
IP1	0.94
IP2	0.28
IP3	0.93
IP4	0.41
NE1	0.81
PB1	0.62
PB2	0.46
PT1	1.17
SL1	0.53
SU1	0.93
BOU	0.28
FBK	0.56
PRU	0.21
BC	0.67
PRAIRIES	0.96
SHIELD	1.0
ATLANTIC	0.79

Table 4: Reference Earth Model (Quebec)	
Layer Thickness (km)	Resistivity (Ω-m)
15	20,000
10	200
125	1,000
200	100
∞	3

Reference Geomagnetic Field Time Series or Waveshape[5]

The geomagnetic field measurement record of the March 13-14 1989 GMD event, measured at NRCan's Ottawa geomagnetic observatory is the basis for the reference geomagnetic field waveshape to be used to calculate the GIC time series, GIC(t), required for transformer thermal impact assessment.

The geomagnetic latitude of the Ottawa geomagnetic observatory is 55°; therefore, the amplitude of the geomagnetic field measurement data were scaled up to the 60° reference geomagnetic latitude (see Figure 3) such that the resulting peak geoelectric field amplitude computed using the reference earth model was 8 V/km (see Figs. 4 and 5). Sampling rate for the geomagnetic field waveshape is 10 seconds.[6] To use this geoelectric field time series where a different earth model is applicable, it should be scaled with the appropriate conductivity scaling factor β.

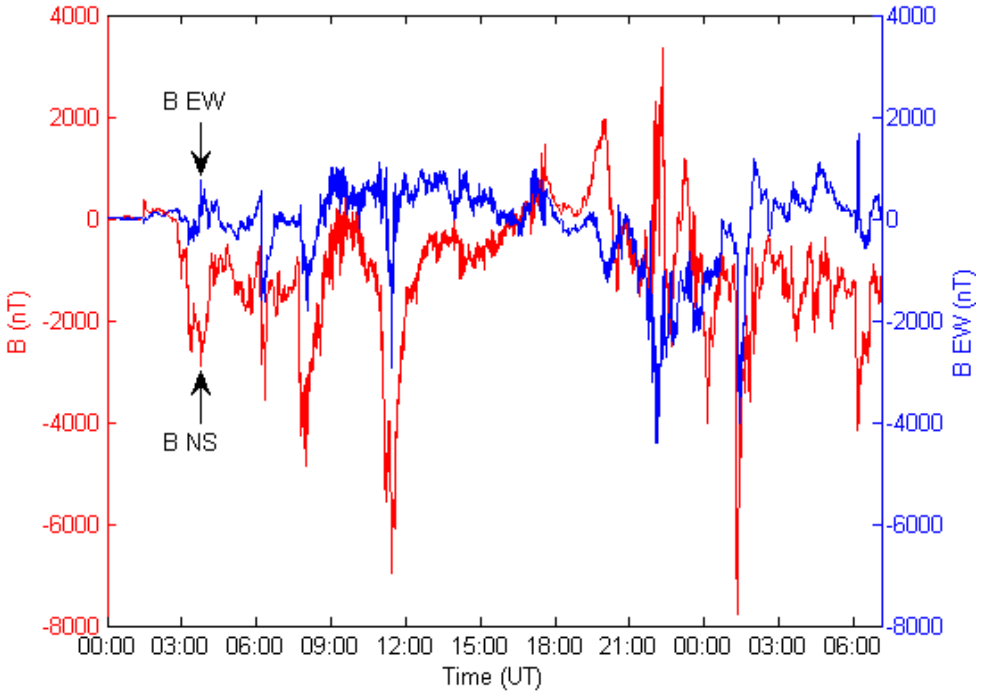


Figure 3: Benchmark Geomagnetic Field Waveshape. Red B_n (Northward), Blue B_e (Eastward)

[5] Refer to the Benchmark GMD Event Description for details on the determination of the reference geomagnetic field waveshape: http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx

[6] The data file of the benchmark geomagnetic field waveshape is available on the NERC GMD Task Force project page: http://www.nerc.com/comm/PC/Pages/Geomagnetic-Disturbance-Task-Force-(GMDTF)-2013.aspx

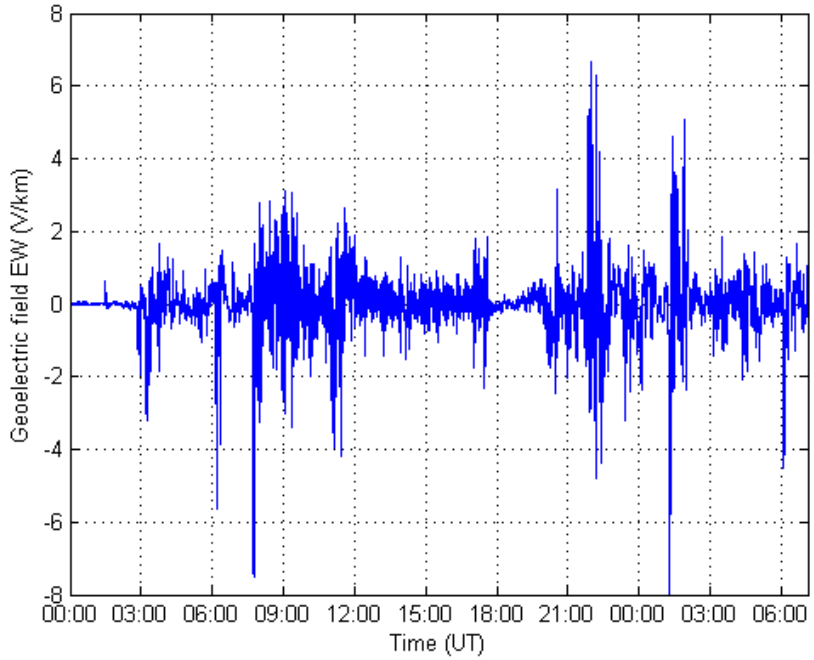


Figure 4: Benchmark Geoelectric Field Waveshape - E_E (Eastward)

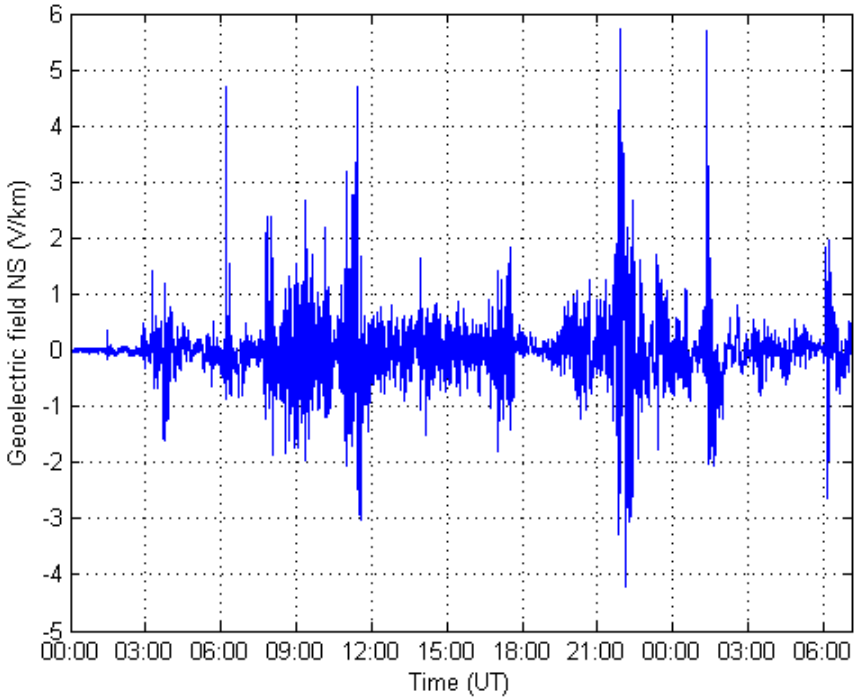


Figure 5: Benchmark Geoelectric Field Waveshape – E_N (Northward)

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards

1.2. Evidence Retention

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

The Planning Coordinator, Transmission Planner, Transmission Owner, and Generator Owner shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The responsible entities shall retain documentation as evidence for five years.

If a Planning Coordinator, Transmission Planner, Transmission Owner, or Generator Owner is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Low	N/A	N/A	N/A	The Planning Coordinator, in conjunction with each of its Transmission Planners, failed to determine and identify individual or joint responsibilities of the Planning Coordinator and each of the Transmission Planners in the Planning Coordinator's planning area for maintaining models and performing the studies needed to complete GMD Vulnerability Assessment(s).
R2	Long-term Planning	Medium	N/A	N/A	N/A	The responsible entity did not maintain System models and geomagnetically-induced current (GIC) System models of the responsible entity's planning area for performing the studies needed to complete

						GMD Vulnerability Assessment(s).
R3	Long-term Planning	High	The responsible entity completed a GMD Vulnerability Assessment but it was more than 60 calendar months and less than or equal to 64 calendar months since the last GMD Vulnerability Assessment.	The responsible entity completed a GMD Vulnerability Assessment but it was more than 64 calendar months and less than or equal to 68 calendar months since the last GMD Vulnerability Assessment; OR The responsible entity's completed GMD Vulnerability Assessment failed to satisfy one of elements listed in Requirement R3 Parts 3.1 through 3.3.	The responsible entity's completed GMD Vulnerability Assessment failed to satisfy two of the elements listed in Requirement R3 Parts 3.1 through 3.3; OR The responsible entity completed a GMD Vulnerability Assessment but it was more than 68 calendar months and less than or equal to 72 calendar months since the last GMD Vulnerability Assessment.	The responsible entity's completed GMD Vulnerability Assessment failed to satisfy three of the elements listed in Requirement R3 Parts 3.1 through 3.3; OR The responsible entity completed a GMD Vulnerability Assessment but it was more than 72 calendar months since the last GMD Vulnerability Assessment; OR The responsible entity does not have a completed GMD Vulnerability Assessment.
R4	Long-term Planning	Medium	N/A	N/A	N/A	The responsible entity did not have criteria for acceptable System steady state voltage limits for its System during the benchmark GMD event described in

						Attachment 1 as required.
R5	Long-term Planning	Medium	N/A	N/A	The responsible entity failed to provide one of the elements listed in Requirement R5 parts 5.1 to 5.2 to each Transmission Owner and Generator Owner in the planning area that owns an applicable power transformer.	The responsible entity failed to provide two of the elements listed in Requirement R5 parts 5.1 to 5.2 to each Transmission Owner and Generator Owner in the planning area that owns an applicable power transformer; OR The responsible entity did not provide geomagnetically-induced current (GIC) flow information to be used for the transformer thermal impact assessment specified in Requirement R6 to each Transmission Owner and Generator Owner in the planning area that owns an applicable power transformer.
R6	Long-term Planning	High	The responsible entity failed to conduct an assessment of thermal impact for 5% or less of its solely owned and jointly owned applicable power transformers where the maximum effective	The responsible entity failed to conduct an assessment of thermal impact for more than 5% up to (and including) 10% of its solely owned and jointly owned applicable power transformers where the	The responsible entity failed to conduct an assessment of thermal impact for more than 10% up to (and including) 15% of its solely owned and jointly owned applicable power transformers where the	The responsible entity failed to conduct an assessment of thermal impact for more than15% of its solely owned and jointly owned applicable power transformers where the maximum effective

			geomagnetically-induced current (GIC) value provided in Requirement R5 part 5.1 is 15 Amperes or greater per phase; OR The responsible entity conducted an assessment of thermal impact of its solely owned and jointly owned applicable power transformers where the maximum effective geomagnetically-induced current (GIC) value provided in Requirement R5 part 5.1 is 15 Amperes or greater per phase but did so more than 12 calendar months and less than or equal to 13 calendar months of receiving GIC flow information specified in Requirement R5; OR The responsible entity failed to include one of the required elements as listed in Requirement R6 parts 6.1 through 6.4.	maximum effective geomagnetically-induced current (GIC) value provided in Requirement R5 part 5.1 is 15 Amperes or greater per phase; OR The responsible entity conducted an assessment of thermal impact of its solely owned and jointly owned applicable power transformers where the maximum effective geomagnetically-induced current (GIC) value provided in Requirement R5 part 5.1 is 15 Amperes or greater per phase but did so more than 13 calendar months and less than or equal to 14 calendar months of receiving GIC flow information specified in Requirement R5; OR The responsible entity failed to include two of the required elements as listed in Requirement R6 parts 6.1 through 6.4.	maximum effective geomagnetically-induced current (GIC) value provided in Requirement R5 part 5.1 is 15 Amperes or greater per phase; OR The responsible entity conducted an assessment of thermal impact of its solely owned and jointly owned applicable power transformers where the maximum effective geomagnetically-induced current (GIC) value provided in Requirement R5 part 5.1 is 15 Amperes or greater per phase but did so more than 14 calendar months and less than or equal to 15 calendar months of receiving GIC flow information specified in Requirement R5; OR The responsible entity failed to include three of the required elements as listed in Requirement R6 parts 6.1 through 6.4.	geomagnetically-induced current (GIC) value provided in Requirement R5 part 5.1 is 15 Amperes or greater per phase; OR The responsible entity conducted an assessment of thermal impact of its solely owned and jointly owned applicable power transformers where the maximum effective geomagnetically-induced current (GIC) value provided in Requirement R5 part 5.1 is 15 Amperes or greater per phase but did so more than 15 calendar months of receiving GIC flow information specified in Requirement R5; OR The responsible entity failed to include four of the required elements as listed in Requirement R6 parts 6.1 through 6.4.

R7	Long-term Planning	High	N/A	The responsible entity's Corrective Action Plan failed to comply with one of the elements in Requirement R7 parts 7.1 and 7.3.	The responsible entity's Corrective Action Plan failed to comply with two of the elements in Requirement R7 parts 7.1 and 7.3.	The responsible entity's Corrective Action Plan failed to comply with three of the elements in Requirement R7 parts 7.1 and 7.3; OR The responsible entity did not have a Corrective Action Plan as required by Requirement R7.

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

None.

Guidelines and Technical Basis

Benchmark GMD Event (Attachment 1)

The benchmark GMD event defines the geoelectric field values used to compute GIC flows that are needed to conduct a GMD Vulnerability Assessment. A white paper that includes the event description, analysis, and example calculations is available on the Project 2013-03 Geomagnetic Disturbance Mitigation project page:

http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx

Requirement R2

A GMD Vulnerability Assessment requires a GIC System model, which is a dc representation of the System, to calculate GIC flow. In a GMD Vulnerability Assessment, GIC simulations are used to determine transformer Reactive Power absorption and transformer thermal response. Details for developing the GIC System model are provided in the NERC GMD Task Force guide: Application Guide for Computing Geomagnetically-Induced Current in the Bulk Power System. The guide is available at:

http://www.nerc.com/comm/PC/Geomagnetic%20Disturbance%20Task%20Force%20GMDTF%202013/GIC%20Application%20Guide%202013_approved.pdf

Requirement R3

The GMD Planning Guide developed by the NERC GMD Task Force provides technical information on GMD-specific considerations for planning studies. It is available at:

http://www.nerc.com/comm/PC/Geomagnetic%20Disturbance%20Task%20Force%20GMDTF%202013/GMD%20Planning%20Guide_approved.pdf

Requirement R5

The transformer thermal impact assessment specified in Requirement R6 is based on GIC time series information for the Benchmark GMD Event. This GIC information is determined by the planning entity through simulation of the GIC system model and must be provided to the entity responsible for conducting the thermal impact assessment.

The maximum effective GIC value provided in part 5.1 is used to screen the transformer fleet such that only those transformers that experience an effective GIC flow of 15A or greater are evaluated.

The effective GIC time series, GIC(t), provided in part 5.2 is used to conduct the transformer thermal impact assessment (see white paper for details).

The peak GIC value of 15 amps per phase has been shown through thermal modeling to be a conservative threshold below which the risk of exceeding known temperature limits established by technical organizations is low. Additional information is available in the transformer thermal impact assessment white paper:

http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx

Requirement R6

The thermal impact assessment of a power transformer may be based on manufacturer-provided GIC capability curves, thermal response simulation, or other technically justified means. A process for conducting the assessment is presented in the white paper posted on the project page.

http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx

The threshold criteria and transformer thermal impact must be evaluated on the basis of effective GIC. Refer to the white paper for additional information.

Requirement R7

Technical considerations for GMD mitigation planning are available in Chapter 5 of the GMD Planning Guide. Additional information is available in the 2012 Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances on the Bulk-Power System:

http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2012GMD.pdf

Implementation Plan

Project 2013-03 Geomagnetic Disturbance Mitigation

Implementation Plan for TPL-007-1 – Transmission System Planned Performance During Geomagnetic Disturbances

Approvals Required

TPL-007-1 – Transmission System Planned Performance for Geomagnetic Disturbance Events

Prerequisite Approvals

None

Retirements

None

Revisions to Glossary Terms

There is one new definition in the proposed standard, which shall become effective when TPL-007-1 is approved by the applicable governmental authority:

> **Geomagnetic Disturbance Vulnerability Assessment or GMD Vulnerability Assessment:** *Documented evaluation of potential susceptibility to voltage collapse, Cascading, or localized damage of equipment due to geomagnetic disturbances.*

Applicable Entities

Planning Coordinator with a Planning Coordinator planning area that includes an applicable power transformer as listed in *section 4.2 Facilities* of the standard;

Transmission Planner with a Transmission Planning area that includes an applicable power transformer as listed in *section 4.2 Facilities* of the standard;

Transmission Owner who owns a power transformer(s) as listed in *section 4.2 Facilities* of the standard; and

Generator Owner who owns a power transformer(s) as listed in *section 4.2 Facilities* of the standard.

Applicable Facilities

Facilities that include power transformer(s) with high side, wye-grounded winding with terminal voltage greater than 200 kV.

Conforming Changes to Other Standards

None

Effective Dates

Compliance with TPL-007-1 shall be implemented over a 4-year period as follows. Phased implementation provides:

- Necessary time for entities to develop the required models.
- Proper sequencing of assessments. The assessment of thermal impact on transformers is dependent upon geomagnetically-induced current (GIC) flow calculations that are determined in by the responsible planning entity.
- Necessary time for development of viable Corrective Action Plans, which may require entities to develop, perform, and or validate new and/or modified studies, assessments, procedures, etc., to meet the TPL-007-1 requirements. Some mitigation measures may have significant budget, siting, or construction planning requirements.

Requirement R1 shall become effective on the first day of the first calendar quarter that is 60 calendar days after the date that this standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, Requirement R1 shall become effective on the first day of the first calendar quarter that is 60 calendar days after the date this standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Requirement R2 shall become effective on the first day of the first calendar quarter that is 14 calendar months after the date that this standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, Requirement R2 shall become effective on the first day of the first calendar quarter that is 14 calendar months after the date this standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Requirement R5 shall become effective on the first day of the first calendar quarter that is 18 calendar months after the date that this standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, Requirement R5 shall become effective on the first day of the first calendar quarter that is 18 calendar months after the date this standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Requirement R6 shall become effective on the first day of the first calendar quarter that is 36 calendar months after the date that this standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is

required for a standard to go into effect. Where approval by an applicable governmental authority is not required, Requirement R6 shall become effective on the first day of the first calendar quarter that is 36 calendar months after the date this standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Requirement R3, Requirement R4, and **Requirement R7** shall become effective on the first day of the first calendar quarter that is 48 calendar months after the date that this standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, Requirement R3, Requirement R4, and Requirement R7 shall become effective on the first day of the first calendar quarter that is 48 calendar months after the date this standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Project 2013-03 Geomagnetic Disturbance Mitigation

Update to Background Information Distributed on June 4, 2014

During the standard drafting team's (SDT) supporting document review at the conclusion of their meeting on June 4, 2014, the SDT determined that a deletion and wording change to Table 1 in proposed standard TPL-007-1 would clarify the performance criteria to reflect the SDT's intent. The change is also consistent with feedback received from stakeholders during informal comments. The revised Table 1 no longer refers to criteria that some stakeholders indicated went beyond the steady state analysis explicitly called for in the requirements. A redlined version of Table 1 is attached and included in the agenda package.

Table 1 –Steady State Planning Events

Steady State:

a. ~~The System shall remain stable.~~ Voltage collapse, Cascading and uncontrolled islanding shall not occur.

b. Load loss as well as generation loss is acceptable as a consequence of the planning event.

c. Planned System adjustments such as Transmission configuration changes and re-dispatch of generation are allowed if such adjustments are executable within the time duration applicable to the Facility Ratings.

d. System steady state voltages shall be within acceptable limits as established by the Planning Coordinator and the Transmission Planner in accordance with Requirement R4.

Category	Initial Condition	Event	Interruption of Firm Transmission Service Allowed	Load Loss Allowed
GMD GMD Event with Outages	1. System as may be postured in response to space weather information[1], and then 2. GMD event[2]	Reactive Power compensation devices and other Transmission Facilities removed as a result of Protection System operation during the GMD event[3]	Yes[4]	Yes[4]

Table 1 – Steady State Performance Footnotes

1. The System condition for GMD planning may include adjustments to posture the System that are executable in response to space weather information.
2. The GMD conditions for the planning event are described in Attachment 1 (Benchmark GMD Event).
3. Protection Systems may trip due to the effects of harmonics. GMD planning analysis shall consider removal of equipment that the planner determines may be susceptible.
4. ~~The objective of the GMD Vulnerability Assessment is to prevent instability, uncontrolled separation, Cascading and uncontrolled islanding of the System during a GMD event.~~ Load loss and/or curtailment of Firm Transmission Service may be needed to meet BES performance requirements during studied GMD conditions but should not be used as the primary method of achieving required performance. GMD Operating Procedures should be based on predetermined triggers from studied GMD conditions so that the likelihood and magnitude of Load loss or curtailment of Firm Transmission Service is minimized during a GMD event.

Standards Committee Expectations

Approved by Standards Committee January 12, 2012

Background

Standards Committee (SC) members are elected by members of their segment of the Registered Ballot Body, to help the SC fulfill its purpose. According to the Standards Committee Charter, the SC's purpose is:

> *In compliance with the NERC Reliability Standards Development Procedure, the Standards Committee manages the NERC standards development process for the North American-wide reliability standards with the support of the NERC staff to achieve broad bulk power system reliability goals for the industry. The Standards Committee protects the integrity and credibility of the standards development process.*

The purpose of this document is to outline the key considerations that each member of the SC must make in fulfilling his or her duties. Each member is accountable to the members of the Segment that elected them, other members of the SC, and the NERC Board of Trustees for carrying out their responsibilities in accordance with this document.

Expectations of Standards Committee Members

1. SC Members represent their segment, not their organization or personal views. Each member is expected to identify and use mechanisms for being in contact with members of the segment in order to maintain a current perspective of the views, concerns, and input from that segment. NERC can provide mechanisms to support communications if an SC member requests such assistance.

2. SC Members base their decisions on what is best for reliability and must consider not only what is best for their segment, but also what is in the best interest of the broader industry and reliability.

3. SC Members should make every effort to attend scheduled meetings, and when not available are required to identify and brief a proxy from the same segment. Standards Committee business cannot be conducted in the absence of a quorum, and it is essential that each Standards Committee make a commitment to being present.

4. SC Members should not leverage or attempt to leverage their position on the SC to influence the outcome of standards projects.

5. The role of the Standards Committee is to manage the standards process and the quality of the output, not the technical content of standards.

Standards Committee Meeting Dates and Locations for 2014

Face-to-face meetings are typically conducted from 1-5 p.m. on Tuesday and 8 a.m.-12 p.m. on Wednesday, except for the March 2014 face-to-face meeting, which will be held from 1-5 p.m. on Wednesday and 8 a.m.-12 p.m. on Thursday due to space availability. Also, the January 2014 meeting will be a half-day face-to-face meeting. Conference calls are held each month on a Wednesday from 1-5 p.m. Eastern where the SC does not have a face-to-face meeting. The time for face-to-face meetings is based on the 'local' time zone. The time specified for all conference calls is based on the Eastern time zone.

- January 15, 2014 – Atlanta, GA from 1-5 p.m.
- February 12, 2014 – conference call from 1-5 p.m.
- March 12-13, 2014 – Atlanta, GA (1-5 p.m. March 12; 8 a.m.-12 p.m. March 13) **(Wed.-Thurs.)**
- April 9, 2014 – conference call from 1-5 p.m.
- May 14, 2014 – conference call from 1-5 p.m.
- June 10-11, 2014 – Denver, CO (1-5 p.m. June 10; 8 a.m.-12 p.m. June 11)
- July 16, 2014 – conference call from 1-5 p.m.
- August 20, 2014 – conference call from 1-5 p.m.
- September 30, 2014- October 1, 2014 – Portland, OR (1-5 p.m. September 30; 8 a.m.-12 p.m. October 1)
- October 22, 2014 – conference call from 1-5 p.m.
- November 19, 2014 – conference call from 1-5 p.m.
- December 9-10, 2014 – Atlanta, GA (1-5 p.m. December 9; 8 a.m.-12 p.m. December 10)

The Standards Committee has two subcommittees (Project Management and Oversight Committee (PMOS) and Process Subcommittee (SCPS)) which will schedule face-to-face meetings in Atlanta and Portland and conference calls as they deem necessary. They may choose to meet the morning (8 a.m.-12 p.m.) of the first day of the Standards Committee's face-to-face meetings.

Standards Committee
2014 Segment Representatives

Segment and Term	Representative	Organization
Chairman **2014-15**	Brian Murphy Manager, NERC Reliability Standards	NextEra Energy, Inc.
Vice-chairman **2014-15**	Scott Miller Manager Regulatory Policy	MEAG Power
Segment 1-2013-14	Lou Oberski Managing Director, NERC Compliance Policy	Dominion Resources Services, Inc.
Segment 1-2014-15	Laura Lee Manager of ERO Support and Event Analysis, System Operations	Duke Energy
Segment 2-2013-14	Charles Yeung Executive Director Interregional Affairs	Southwest Power Pool
Segment 2-2014-15	Ben Li Consultant	Independent Electric System Operator
Segment 3-2013-14	Jennifer Sterling Director, Exelon NERC Compliance Program	Exelon
Segment 3-2014-15	Ron Parsons General Manager of Transmission Interconnections and Operations	Alabama Power Company
Segment 4-2013-14	Joseph Tarantino Regulatory Compliance Coordinator	Sacramento Municipal Utility District
Segment 4-2014-15	Frank Gaffney Assistant General Manager of and Officer of Regulatory Compliance	Florida Municipal Power Authority
Segment 5-2013-14	Gary Kruempel Compliance Director, Energy Supply	MidAmerican Energy Company

Segment and Term	Representative	Organization
Segment 5-2014-15	Randy Crissman Vice President – Technical Compliance	New York Power Authority
Segment 6-2013-14	Brenda Hampton Regulatory Policy	Energy Future Holdings – Luminant Energy Company LLC
Segment 6-2014-15	Andrew Gallo Director, Reliability Compliance	City of Austin dba Austin Energy
Segment 7-2013-14	John A. Anderson President & CEO	Electricity Consumers Resource Council
Segment 7-2014-15	Frank McElvain Senior Consulting Manager	Siemens Energy, Inc.
Segment 8-2013-14	Robert Blohm Managing Director	Keen Resources Asia Ltd.
Segment 8-2014-15	Frederick Plett Utility Analyst	Massachusetts Attorney General
Segment 9-2014	Klaus Lambeck Chief Facilities, Siting and Environmental Analysis	Public Utilities Commission of Ohio/the Ohio Power Siting Board
Segment 9-2014-15	Jason Woodruff Electrical Engineer	Public Utilities Commission of Nevada
Segment 10-2013-14	Steve Rueckert Director of Standards	Western Electricity Coordinating Council
Segment 10-2014-15	Guy Zito Assistant Vice President of Standards	Northeast Power Coordinating Council

Parliamentary Procedures

Based on Robert's Rules of Order, Newly Revised, 10th Edition, plus "Organization and Procedures Manual for the NERC Standing Committees"

Motions

Unless noted otherwise, all procedures require a "second" to enable discussion.

When you want to…	Procedure	Debatable	Comments
Raise an issue for discussion	Move	Yes	The main action that begins a debate.
Revise a Motion currently under discussion	Amend	Yes	Takes precedence over discussion of main motion. Motions to amend an amendment are allowed, but not any further. The amendment must be germane to the main motion, and can not reverse the intent of the main motion.
Reconsider a Motion already approved	Reconsider	Yes	Allowed only by member who voted on the prevailing side of the original motion.
End debate	Call for the Question *or* End Debate	Yes	If the Chair senses that the committee is ready to vote, he may say "if there are no objections, we will now vote on the Motion." Otherwise, this motion is debatable and subject to 2/3 majority approval.
Record each member's vote on a Motion	Request a Roll Call Vote	No	Takes precedence over main motion. No debate allowed, but the members must approve by 2/3 majority.
Postpone discussion until later in the meeting	Lay on the Table	Yes	Takes precedence over main motion. Used only to postpone discussion until later in the meeting.
Postpone discussion until a future date	Postpone until	Yes	Takes precedence over main motion. Debatable only regarding the date (and time) at which to bring the Motion back for further discussion.
Remove the motion for any further consideration	Postpone indefinitely	Yes	Takes precedence over main motion. Debate can extend to the discussion of the main motion. If approved, it effectively "kills" the motion. Useful for disposing of a badly chosen motion that can not be adopted or rejected without undesirable consequences.
Request a review of procedure	Point of order	No	Second not required. The Chair or secretary shall review the parliamentary procedure used during the discussion of the Motion.

Notes on Motions

Seconds. A Motion must have a second to ensure that at least two members wish to discuss the issue. The "seconder" is not recorded in the minutes. Neither are motions that do not receive a second.

Announcement by the Chair. The Chair should announce the Motion before debate begins. This ensures that the wording is understood by the membership. Once the Motion is announced and seconded, the Committee "owns" the motion, and must deal with it according to parliamentary procedure.

Voting

Voting Method	When Used	How Recorded in Minutes
Unanimous Consent	When the Chair senses that the Committee is substantially in agreement, and the Motion needed little or no debate. No actual vote is taken.	The minutes show "by unanimous consent."
Vote by Voice	The standard practice.	The minutes show Approved or Not Approved (or Failed).
Vote by Show of Hands (tally)	To record the number of votes on each side when an issue has engendered substantial debate or appears to be divisive. Also used when a Voice Vote is inconclusive. (The Chair should ask for a Vote by Show of Hands when requested by a member).	The minutes show both vote totals, and then Approved or Not Approved (or Failed).
Vote by Roll Call	To record each member's vote. Each member is called upon by the Secretary,, and the member indicates either "Yes," "No," or "Present" if abstaining.	The minutes will include the list of members, how each voted or abstained, and the vote totals. Those members for which a "Yes," "No," or "Present" is not shown are considered absent for the vote.

Notes on Voting

(Recommendations from DMB, not necessarily Mr. Robert)

Abstentions. When a member abstains, he is not voting on the Motion, and his abstention is not counted in determining the results of the vote. The Chair should not ask for a tally of those who abstained.

Determining the results. The results of the vote (other than Unanimous Consent) are determined by dividing the votes in favor by the total votes cast. Abstentions are not counted in the vote and shall not be assumed to be on either side.

"Unanimous Approval." Can only be determined by a Roll Call vote because the other methods do not determine whether every member attending the meeting was actually present when the vote was taken, or whether there were abstentions.

Majorities. Robert's Rules use a simple majority (one more than half) as the default for most motions. NERC uses 2/3 majority for all motions.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Standards Committee Meeting

May 30, 2014 | 1:30 p.m. Eastern

Dial-in: 1-866-740-1260 | Meeting Code: 8314765 | Security Code: 053014

Click here: ReadyTalk Webinar Access

NERC Antitrust Compliance Guidelines and Public Announcement*

Introductions and Chair's Remarks

Agenda Items

1. **Review of Agenda — (Approve)** (1 minute)
2. **Project 2014-02: CIP Version 5 Revisions*— (Authorize)** (S. Noess) (15 minutes)
3. **Adjourn**

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Public Announcements

REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

Conference call version:
Participants are reminded that this conference call is public. The access number was posted on the NERC website and widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

August 10, 2010

May Conference Call
Standards Committee
May 30, 2014

CIP Version 5 Revisions Project

Action

Authorize the posting of Project 2014-02 CIP Version 5 Revisions Reliability Standards, Implementation Plan, and VSLs/VRFs for an initial 45-day formal comment period with ballot pool formation during the first 30 days and initial ballots and non-binding polls during the last 10 days of the comment period.

Background

On November 22, 2013, the Federal Energy Regulatory Commission (FERC) issued Order No. 791, Version 5 Critical Infrastructure Protection Reliability Standards, in which FERC approved Version 5 of the Critical Infrastructure Protection (CIP) standards and directed several modifications, including the following for standards development:

1. Modify or remove the "identify, assess, and correct" (IAC) language found in 17 of the 32 CIP Version 5 requirements;
2. Develop modifications to the CIP standards to address security controls for low impact assets;
3. Develop requirements that protect transient electronic devices; and
4. Create a definition of "communication networks" and develop new or modified Reliability Standards that address the protection of communication networks.

NERC must submit new or revised standards responding to the directives related to the IAC language and communication networks by February 3, 2015, one year from the effective date of Order No. 791. FERC did not place a timeframe on responding to the other directives.

On January 16, 2014, the Standards Committee (SC) accepted the Project 2014-02 Standard Authorization Request (SAR) to post for a 30-day informal comment period from January 17 - February 18, 2014. NERC staff made minor revisions to the SAR based on submitted comments and posted the revised SAR to the project page on March 20, 2014.

On January 29, 2014, the SC seated 10 members to the Project 2014-02 Standard Drafting Team (SDT). The roster is available here. The SDT's drafting activity followed an aggressive meeting schedule, including four face-to-face meetings in Washington, DC, Sacramento, CA, Atlanta, GA, and Columbus, OH. When not meeting in person, the SDT held weekly full-team conference calls as well as weekly calls for subgroups. There were four subgroups, each one focusing on one of the four main directives, and the SDT designated two SDT members to lead each call. In total, the SDT held 10 hours of calls each week. As a result of these open meetings and calls, the SDT received input from a variety of stakeholders participating in drafting activity.

The SDT also focused on quality of the revisions to the standards throughout development, and incorporated quality review as part of the fabric of standards development activities. The SDT sought regular and meaningful input from a variety of sources over the past few months. For instance, various stakeholders participated in standards drafting activity and provided their viewpoints for the SDT's consideration through direct participation, email, in-person outreach opportunities, and other means. These stakeholders included participants from a variety of industry segments, trade association representatives, governmental authority staff, members of the Standards Committee and the SDT's Project Management Oversight Subcommittee (PMOS) liaison, and other interested participants. In addition, the SDT coordinated extensively with NERC Technical, Compliance, Legal, and Enforcement staffs to garner a comprehensive view of the revisions' effects once approved. Finally, the SDT considered other relevant input, such as the P 81 criteria, throughout development to ensure the quality of the proposed revisions.

In addition to a focus on quality during development, NERC staff coordinated a quality review prior to the posting of the Reliability Standards, Implementation Plan, Violation Risk Factors, and Violation Severity Levels. During this check, reviewers, including the SDT's PMOS liaison, focused on consistency and clarity in language.

As a complement to incorporating quality review, NERC staff and the SDT focused heavily on outreach during standards development and will continue to focus on outreach during the proposed comment and ballot period. In January, NERC staff conducted two technical conferences to gather input from industry on the directives from Order No. 791. Once the SDT was seated, the SDT's weekly calls and monthly meetings had active participation from observers. Members of the SDT met with trade association representatives at NERC's office mid-way through development to update the trade associations' members on the drafting activity and to receive feedback. In late April, the SDT hosted a webinar to introduce the revisions to a broad audience. Furthermore, NERC staff provided updates to the NERC Board of Trustees and the SC as appropriate. Finally, once the standards are approved to post as proposed, NERC staff and the SDT have several outreach events planned, such as speaking at regional CIP working groups and a webinar on June 19.

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

BES Cyber Asset (BCA): A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. A Transient Cyber Asset is not a BES Cyber Asset.

Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Transient Cyber Asset is not a Protected Cyber Asset.

Removable Media: Portable media, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media.

Transient Cyber Asset: A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

BES Cyber Asset (BCA): A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. ~~(~~A Transient Cyber Asset is not a BES Cyber Asset. ~~if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)~~

Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Transient Cyber Asset is not a Protected Cyber Asset. ~~if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.~~

Removable Media: Portable media, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media.

Transient Cyber Asset: A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-6

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to low impact BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements by CIP Senior Manager approval of the policies specified in Part 2.1.

The language in Requirement R2, Part 2.4 "external routable protocol paths" and "Dial-up Connectivity" was included to acknowledge the support given in FERC Order No. 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.4 uses the phrase "external routable protocol paths" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems. The Standard Drafting Team (SDT) intent in using the phrase "external routable protocol paths" is to focus only on the paths to the low impact BES Cyber Systems and not the paths to other networks (e.g., corporate paths).

The additions to Requirement R2, in particular the processes required under Parts 2.2-2.6, address FERC Order No. 791 paragraphs 106-110, which require the standard to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for low impact assets. The SDT pulled language and concepts from CIP-004, CIP-005, CIP-006, and CIP-008 in order to add objective criteria to each of the previous policy topic areas in CIP-003, Requirement R2.

In FERC Order No. 791 paragraphs 111-112, FERC upheld that creating and maintaining an inventory of low impact assets for audit purposes would be unduly burdensome, so the inventory statements remain unchanged.

R2. Each Responsible Entity for its assets containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence must include each of the applicable documented policies and processes that collectively include each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* and any additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	Low Impact BES Cyber Systems	Review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the topics in CIP-003-6, Requirement R2, Parts 2.2 – 2.6.	An example of evidence may include, but is not limited to, one or more documented cyber security policies that address each of the areas in Requirement R2, Parts 2.2 – 2.6 and includes evidence of review and CIP Senior Manager approval at least every 15 calendar months.
2.2	Low Impact BES Cyber Systems	Implement one or more documented processes that include operational or procedural control(s) to restrict physical access.	An example of evidence may include, but is not limited to, documentation of the operational or procedural control(s).
2.3	Low Impact BES Cyber Systems at Control Centers	Implement one or more documented processes that collectively include the following: 2.3.1. Escorted access of visitors; and 2.3.2. For Control Centers with external routable protocol paths, monitoring physical access point(s).	Examples of evidence may include, but are not limited to: • For 2.3.1, documentation of visitor escort procedure(s) at Control Centers. • For 2.3.2, documentation describing how the Responsible Entity monitors physical access points into Control Centers that have external routable protocol paths.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	Low Impact BES Cyber Systems	Implement one or more documented processes that collectively include the following: 2.4.1. All external routable protocol paths, if any, must be through one or more identified access point(s). 2.4.2. For each identified access point, if any, require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. 2.4.3. Authentication when establishing Dial-up Connectivity, per Cyber Asset capability.	Examples of evidence may include, but are not limited to: • For 2.4.1, documentation of external routable protocol paths through identified access points. • For 2.4.2, a representative sample of a list of restrictions (e.g., firewall rules, access control lists, data diode, etc.) that demonstrates that only permitted access is allowed and that each access rule has a reason documented individually or by group. • For 2.4.3, documentation of authentication controls applied to dial-up access connections.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	Low Impact BES Cyber Systems	Implement one or more Cyber Security Incident response plan(s) that collectively include the following: 2.5.1. Identification, classification, and response to Cyber Security Incidents. 2.5.2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident. 2.5.3. Notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. 2.5.4. The roles and responsibilities of Cyber Security Incident response groups or individuals. 2.5.5. Incident handling procedures for Cyber Security Incidents. 2.5.6. Testing of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to: • One or more documented cyber security incident response plans that include the requirement parts. • Dated evidence that shows the testing or execution of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Low Impact BES Cyber Systems	Implement a security awareness program that reinforces cyber security practices at least quarterly. Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.	An example of evidence may include, but is not limited to, one or more documents describing how the Responsible Entity is implementing its cyber security awareness program per 2.6.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These

delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1)	the previous approval. (R1)		months of the previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address one of the topics as required by Requirement R2, Part 2.1. (2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 15	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address two of the topics as required by Requirement R2, Part 2.1. (2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 16	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address three of the topics as required by Requirement R2, Part 2.1. (2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity did not have any documented cyber security policies for assets with a low impact rating that address the topics as required by Requirement R2, Part 2.1. (2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 18

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 16 calendar months but did complete this approval in less than	calendar months of the previous review. (2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (2.1) OR The Responsible Entity documented and implemented one or more processes for	calendar months of the previous review. (2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 18 calendar months of the previous approval. (2.1) OR The Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (2.1) OR The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity did not reinforce cyber security practices at least quarterly but did reinforce cyber security practices at least every two quarters. (2.6)	or equal to 17 calendar months of the previous approval. (2.1) OR The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include two of the topics as	assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.3. (2.3) OR The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include two of the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include three of the	document or implement any processes for assets with a low impact rating to include the operational or procedural control(s) to restrict physical access as required by Requirement R2, Part 2.2. (2.2) OR The Responsible Entity did not document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.3. (2.3) OR The Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.5 for assets with a low impact rating in less than or equal to 16 calendar months. (2.6)	required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices at least quarterly but failed to include one of the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security	topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices at least quarterly but failed to include two of the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security practices every three quarters. (2.6) OR	document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity did not implement any Cyber Security Incident response plans for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity did not implement a security awareness program

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				practices every three quarters. (2.6) OR The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 in more than 16 calendar months but less than or equal to 17 calendar months. (2.6)	The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 for assets with a low impact rating in more than 17 calendar months but less than or equal to 18 calendar months. (2.6)	for assets with a low impact rating that collectively included the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not implement a security awareness program for assets with a low impact rating that reinforced cyber security practices at least every 15 months. (2.6) OR The Responsible Entity did not implement a security awareness program for assets with a low impact rating that reinforced the topics

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						within 18 calendar months as required by Requirement R2, Part 2.6. (2.6)
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but	The Responsible Entity has used delegated authority for actions where allowed by the CIP

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-6, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-6, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-6, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of the requirement is to outline a set of protections designed for all low impact BES Cyber Systems. The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do meet the definition of having a 15-minute adverse impact so some protections are needed. The intent is that such protections are part of a program that covers the low impact BES Cyber Systems collectively either at a programmatic or site level, not an individual device or system level.

There are four main areas that must be covered by this security program: physical security, electronic access controls for all external routable protocol paths or Dial-up Connectivity, a security awareness program, and cyber security incident response plans.

The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not necessary.

2.1 - As with Requirement R1, the number of policies and the specific language used in them would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas in CIP-003-6, Requirement R2, Parts 2.2 through 2.6. The Responsible Entity has flexibility in the number and structure of its policies to meet its needs and organization. Examples include developing a single comprehensive cyber security policy covering these topics for all in-scope assets, several comprehensive cyber security policies based on asset type, or a single high-level umbrella policy with additional policy detail in lower level documents in its documentation hierarchy.

2.2 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at a BES asset. The Responsible Entity has flexibility in the controls used and the granularity of those controls. The entity is to document its operational or physical controls that restrict access to the low impact BES Cyber Systems at the asset. Entities may utilize perimeter controls (fences with locked gates, guards, site access policies, etc.) and/or more granular areas of access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. Lists of authorized users are not required.

2.3 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at Control Centers. For Control Centers, the entity should further describe the process for handling escorted access of visitors. For Control Centers that have external routable connectivity, monitoring of physical access points is also required. Monitoring does not imply logging and maintaining logs, but monitoring that access has been granted through an access point (door alarm, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the level as determined by the entity’s controls.

2.4 – The Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. The electronic access controls should address the risk of using the asset’s external connectivity to gain access to the low impact BES Cyber Systems. The entity should be able to describe how its electronic access controls on the external connectivity paths protect the collection of low impact BES Cyber Systems at the site. The intent is to reduce the risk of aggregation of numerous low impact BES Cyber Systems at the site or across multiple sites through external connectivity.

Examples of sufficient access controls may include:

- All the external routable protocol connectivity paths to the asset pass through a firewall that denies all traffic by default with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are shielded from or to the world-wide-web (e.g. IP addresses, ports, services, and data diode) for scenarios representative of the Responsible Entity's sites having Low Impact BES Cyber Systems.

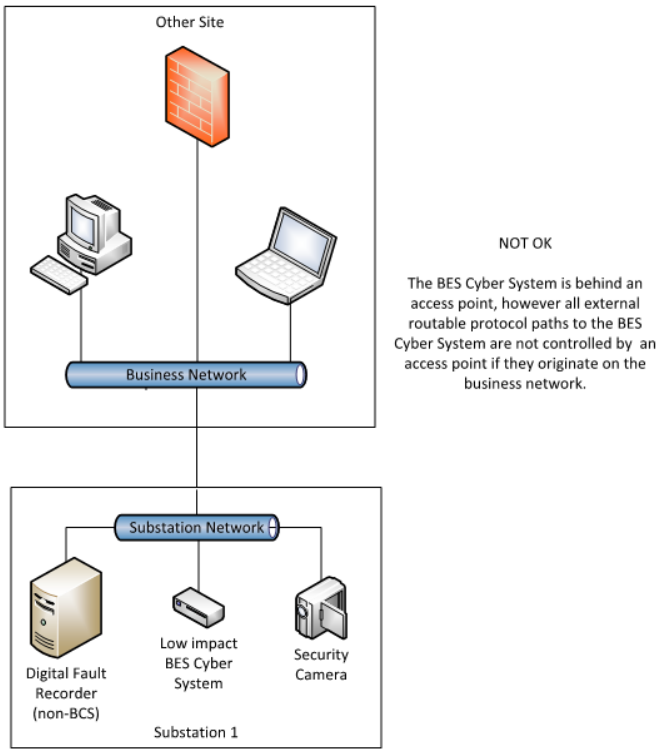
- Dialup Connectivity to a low impact BES Cyber System is set to dial out only (no autoanswer) to a preprogrammed number to deliver data. Incoming Dialup Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

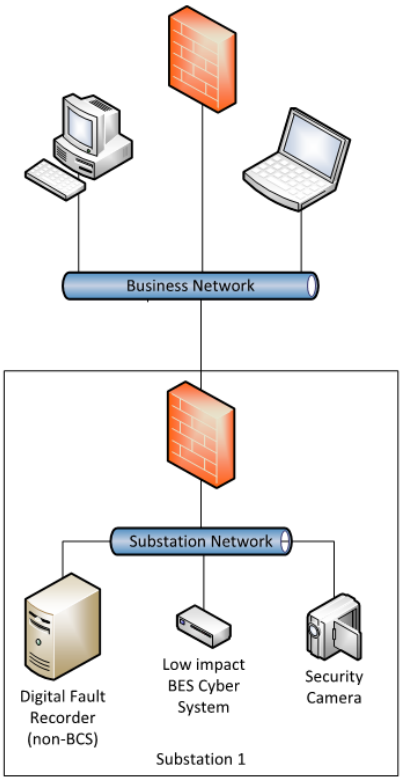
Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has dialup connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset which has a default password. There is no access control in this instance.
- An asset has external routable connectivity due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier which allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.

The SDT also notes that in topic 2.4, the SDT uses the term “electronic access control” in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

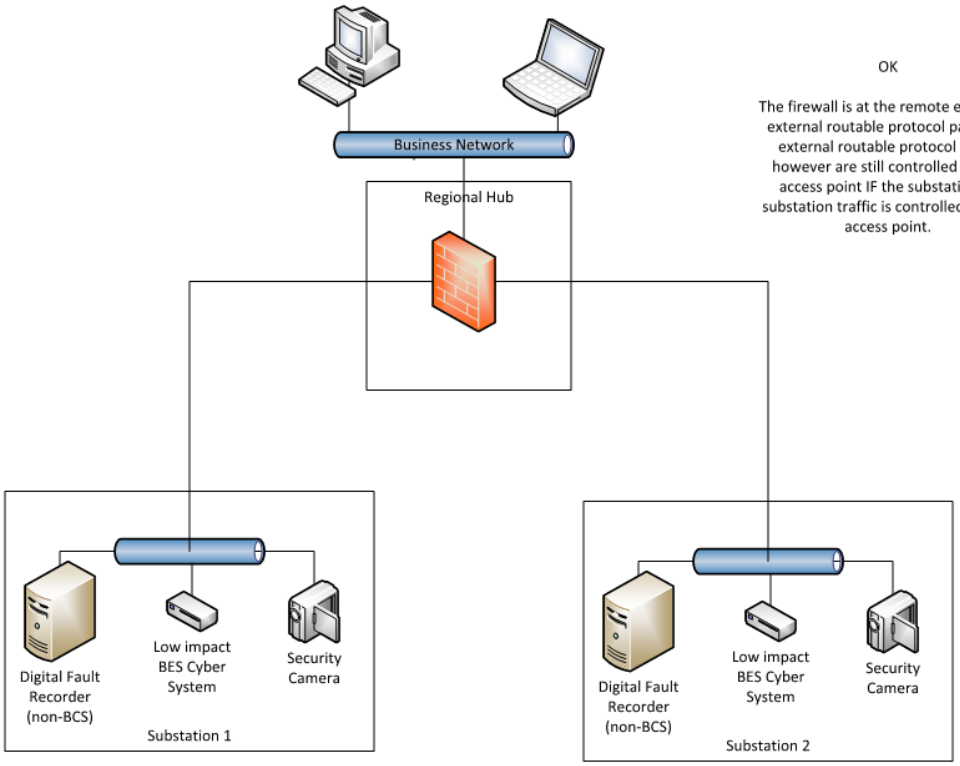
The following diagrams explain the SDT’s rationale.





OK

All the external traffic to the BES Cyber System is controlled by an access point.



OK

The firewall is at the remote end of an external routable protocol path. All external routable protocol paths however are still controlled by the access point IF the substation to substation traffic is controlled via the access point.

2.5 - The entity should have a documented cyber security incident response plan that includes each of the topics listed. For assets that have limited or no connectivity, it is not the intent to increase their risk by increasing the level of connectivity in order to have real-time monitoring. The intent is if in the normal course of business suspicious activities are noted at an asset containing low impact BES Cyber Systems, there is a cyber security incident response plan that will guide the entity through responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident. The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as well as other forms of tabletop exercises or paper drills. NERC-led exercises such as GridEx participation would also count as an exercise if the entity's response plan is followed.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

2.6 - The intent of the security awareness program is for entities to reinforce good cyber security practices with their personnel on at least a quarterly basis. The physical security, electronic access controls, and the cyber security incident response plan should be covered at least every 15 months. It is up to the entity as to the topics and how it schedules these topics. It should be sufficient for an entity to produce the awareness material that it delivered quarterly and the delivery method(s) (posters, emails, topics at staff meetings, etc.). The intent is that tracking of reception of the messages by personnel is not required.

Requirement R3:

The intent of CIP-003-6, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-6, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to

the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-~~5~~6

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 **Balancing Authority**

4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 **Generator Operator**

4.1.4 **Generator Owner**

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

6. Background:

Standard CIP-003~~-5~~ exists as part of a suite of CIP Standards related to cyber security, which ~~. CIP-002-5.1~~ require~~s~~ the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~ This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement~~ **~~in a manner that identifies, assesses, and corrects deficiencies, . . .~~**

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes,

but ~~they~~ it must address the applicable requirements. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to ~~its~~ low impact BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements by CIP Senior Manager approval of the policies specified in Part 2.1.

The language in Requirement R2, Part 2.~~3~~ 4 "~~. . . for~~ external routable protocol ~~connections~~ paths" and "Dial-up Connectivity~~. . .~~" was included to acknowledge the support given in FERC Order No. 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.~~3~~ 4 uses the phrase "external routable protocol ~~connections~~paths" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems. The Standard Drafting Team (SDT) intent in using the phrase "external routable protocol paths" is to focus only on the paths to the low impact BES Cyber Systems and not the paths to other networks (e.g., corporate paths).

The additions to Requirement R2, in particular the processes required under Parts 2.2-2.6, address FERC Order No. 791 paragraphs 106-110, which require the standard to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for low impact assets. The SDT pulled language and concepts from CIP-004, CIP-005, CIP-006, and CIP-008 in order to add objective criteria to each of the previous policy topic areas in CIP-003, Requirement R2.

In FERC Order No. 791 paragraphs 111-112, FERC upheld that creating and maintaining an inventory of low impact assets for audit purposes would be unduly burdensome, so the inventory statements remain unchanged.

R2. Each Responsible Entity for its assets ~~identified in CIP-002-5, Requirement R1, Part R1.3~~containing low impact BES Cyber Systems~~),~~ shall perform each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* ~~implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months:~~. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~Cyber security awareness;~~

~~Physical security controls;~~

~~Electronic access controls for external routable protocol connections and Dial-up Connectivity; and~~

~~Incident response to a Cyber Security Incident.~~

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence must include each of the applicable documented policies and processes that collectively include each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* and any additional evidence to demonstrate implementation as described in the Measures column of the table~~. If any asset locations have been identified per R2 of this Standard, then the following bulleted evidence may be included~~.

~~Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.~~

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	Low Impact BES Cyber Systems	Review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the topics in CIP-003-6, Requirement R2, Parts 2.2 – 2.6.	An example of evidence may include, but is not limited to, one or more documented cyber security policies that address each of the areas in Requirement R2, Parts 2.2 – 2.6 and includes evidence of review and CIP Senior Manager approval at least every 15 calendar months.
2.2	Low Impact BES Cyber Systems	Implement one or more documented processes that include operational or procedural control(s) to restrict physical access.	An example of evidence may include, but is not limited to, documentation of the operational or procedural control(s).
2.3	Low Impact BES Cyber Systems at Control Centers	Implement one or more documented processes that collectively include the following: 2.3.1. Escorted access of visitors; and 2.3.2. For Control Centers with external routable protocol paths, monitoring physical access point(s).	Examples of evidence may include, but are not limited to: • For 2.3.1, documentation of visitor escort procedure(s) at Control Centers. • For 2.3.2, documentation describing how the Responsible Entity monitors physical access points into Control Centers that have

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
			external routable protocol paths.
2.4	Low Impact BES Cyber Systems	Implement one or more documented processes that collectively include the following: 2.4.1. All external routable protocol paths, if any, must be through one or more identified access point(s). 2.4.2. For each identified access point, if any, require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. 2.4.3. Authentication when establishing Dial-up Connectivity, per Cyber Asset capability.	Examples of evidence may include, but are not limited to: • For 2.4.1, documentation of external routable protocol paths through identified access points. • For 2.4.2, a representative sample of a list of restrictions (e.g., firewall rules, access control lists, data diode, etc.) that demonstrates that only permitted access is allowed and that each access rule has a reason documented individually or by group. • For 2.4.3, documentation of authentication controls applied to dial-up access connections.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	Low Impact BES Cyber Systems	Implement one or more Cyber Security Incident response plan(s) that collectively include the following: 2.5.1. Identification, classification, and response to Cyber Security Incidents. 2.5.2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident. 2.5.3. Notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. 2.5.4. The roles and responsibilities of Cyber Security Incident response groups or individuals. 2.5.5. Incident handling procedures for Cyber Security Incidents. 2.5.6. Testing of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to: • One or more documented cyber security incident response plans that include the requirement parts. • Dated evidence that shows the testing or execution of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Low Impact BES Cyber Systems	Implement a security awareness program that reinforces cyber security practices at least quarterly. Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.	An example of evidence may include, but is not limited to, one or more documents describing how the Responsible Entity is implementing its cyber security awareness program per 2.6.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager

may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1)	the previous approval. (R1)		months of the previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only three~~one of the topics as required by Requirement R2, Part 2.1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (~~R2~~2.1) ~~OR~~ ~~The Responsible Entity documented and implemented one or more cyber~~	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only~~ two of the topics as required by Requirement R2, Part 2.1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (~~R2~~2.1) ~~OR~~ ~~The Responsible Entity documented and implemented~~	The Responsible Entity ~~documented and implemented~~had one or more documented cyber security policies for assets with a low impact rating ~~that~~ but failed to address ~~only one~~three of the topics as required by Requirement R2, Part 2.1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (~~R2~~2.1) ~~OR~~ ~~The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2~~	The Responsible Entity did not ~~document or implement~~have any documented cyber security policies for assets with a low impact rating that address the topics as required by Requirement R2, Part 2.1. (~~R2~~2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~security policies for assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the	~~one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of	~~but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (~~R2~~2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by	Part 2.1 within 18 calendar months of the previous review. (~~R2~~2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 18 calendar months of the previous approval. (~~R2~~2.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			previous review. (~~R2~~2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (~~R2~~2.1) OR	the previous review. (~~R2~~2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (~~R2~~2.1)	Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (~~R2~~2.1) OR The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.3. (2.3) OR The Responsible Entity documented and implemented one or	The Responsible Entity did not document or implement any processes for assets with a low impact rating to include the operational or procedural control(s) to restrict physical access as required by Requirement R2, Part 2.2. (2.2) OR The Responsible Entity did not document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.3. (2.3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity did not reinforce cyber security practices at least quarterly but did reinforce cyber security practices at least every two quarters. (2.6) OR The Responsible Entity did not	OR The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include two of the topics as required by Requirement R2, Part 2.5. (2.5) OR	more processes for assets with a low impact rating but failed to include two of the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include three of the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices	The Responsible Entity did not document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity did not implement any Cyber Security Incident response plans for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.5 for assets with a low impact rating in less than or equal to 16 calendar months. (2.6)	The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices at least quarterly but failed to include one of the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security practices every three quarters. (2.6) OR	at least quarterly but failed to include two of the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security practices every three quarters. (2.6) OR The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 for assets with a low impact rating in more than 17 calendar months but less than or equal to 18 calendar months. (2.6)	implement a security awareness program for assets with a low impact rating that collectively included the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not implement a security awareness program for assets with a low impact rating that reinforced cyber security practices at least every 15 months. (2.6) OR The Responsible Entity did not implement a security awareness program for assets with a low

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 in more than 16 calendar months but less than or equal to 17 calendar months. (2.6)		impact rating that reinforced the topics within 18 calendar months as required by Requirement R2, Part 2.6. (2.6)
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				50 calendar days of the change. (R3)		Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	~~The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and has Identified deficiencies but did not assess or correct the deficiencies.(R4)~~ ~~OR~~ ~~The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or~~	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~correct the deficiencies.(R4)~~ ~~OR~~ The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-6~~5~~, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-6~~5~~, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-6~~5~~, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

~~As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not~~

~~necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.~~

The intent of the requirement is to outline a set of protections designed for all low impact BES Cyber Systems. The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do meet the definition of having a 15-minute adverse impact so some protections are needed. The intent is that such protections are part of a program that covers the low impact BES Cyber Systems collectively either at a programmatic or site level, not an individual device or system level.

There are four main areas that must be covered by this security program: physical security, electronic access controls for all external routable protocol paths or Dial-up Connectivity, a security awareness program, and cyber security incident response plans.

The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not necessary.

2.1 - As with Requirement R1, the number of policies and the specific language used in them would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas in CIP-003-6, Requirement R2, Parts 2.2 through 2.6. The Responsible Entity has flexibility in the number and structure of its policies to meet its needs and organization. Examples include developing a single comprehensive cyber security policy covering these topics for all in-scope assets, several comprehensive cyber security policies based on asset type, or a single high-level umbrella policy with additional policy detail in lower level documents in its documentation hierarchy.

2.2 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at a BES asset. The Responsible Entity has flexibility in the controls used and the granularity of those controls. The entity is to document its operational or physical controls that restrict access to the low impact BES Cyber Systems at the asset. Entities may utilize perimeter controls (fences with locked gates, guards, site access policies, etc.) and/or more granular areas of access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. Lists of authorized users are not required.

2.3 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at Control Centers. For Control Centers, the entity should further describe the process for handling escorted access of visitors. For Control Centers that have external routable connectivity, monitoring of physical access points is also required. Monitoring does not imply logging and maintaining logs, but monitoring that access has been

granted through an access point (door alarm, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the level as determined by the entity's controls.

2.4 – The Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. The electronic access controls should address the risk of using the asset's external connectivity to gain access to the low impact BES Cyber Systems. The entity should be able to describe how its electronic access controls on the external connectivity paths protect the collection of low impact BES Cyber Systems at the site. The intent is to reduce the risk of aggregation of numerous low impact BES Cyber Systems at the site or across multiple sites through external connectivity.

Examples of sufficient access controls may include:

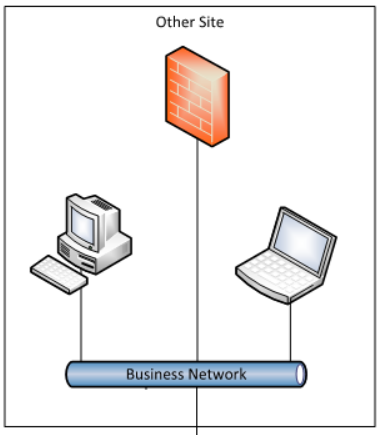
- All the external routable protocol connectivity paths to the asset pass through a firewall that denies all traffic by default with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are shielded from or to the world-wide-web (e.g. IP addresses, ports, services, and data diode) for scenarios representative of the Responsible Entity's sites having Low Impact BES Cyber Systems.
- Dialup Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dialup Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has dialup connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset which has a default password. There is no access control in this instance.
- An asset has external routable connectivity due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier which allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.

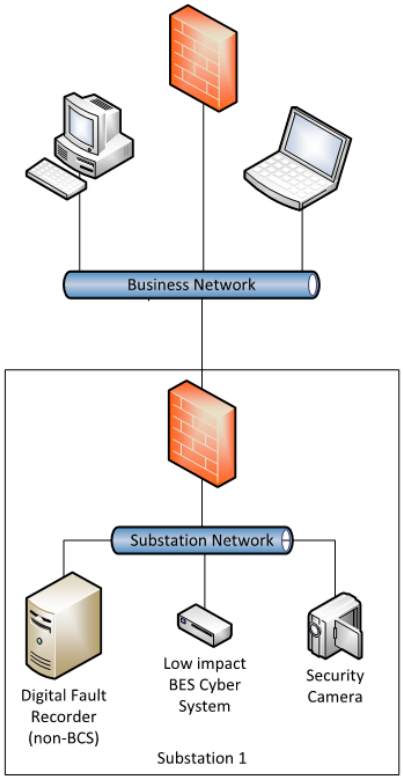
The SDT also notes that in topic 2.4, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

The following diagrams explain the SDT's rationale.



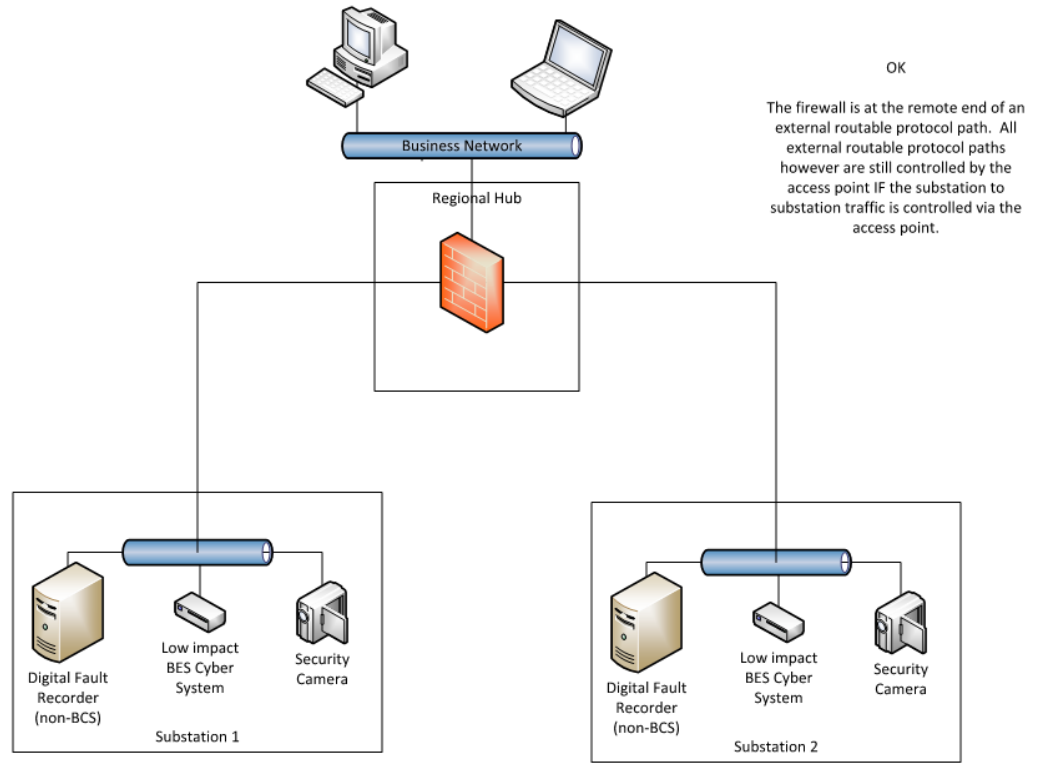
NOT OK

The BES Cyber System is behind an access point, however all external routable protocol paths to the BES Cyber System are not controlled by an access point if they originate on the business network.



OK

All the external traffic to the BES Cyber System is controlled by an access point.



2.5 - The entity should have a documented cyber security incident response plan that includes each of the topics listed. For assets that have limited or no connectivity, it is not the intent to increase their risk by increasing the level of connectivity in order to have real-time monitoring. The intent is if in the normal course of business suspicious activities are noted at an asset containing low impact BES Cyber Systems, there is a cyber security incident response plan that will guide the entity through responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident. The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as well as other forms of tabletop exercises or paper drills. NERC-led exercises such as GridEx participation would also count as an exercise if the entity's response plan is followed.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

2.6 - The intent of the security awareness program is for entities to reinforce good cyber security practices with their personnel on at least a quarterly basis. The physical security, electronic access controls, and the cyber security incident response plan should be covered at least every 15 months. It is up to the entity as to the topics and how it schedules these topics. It should be sufficient for an entity to produce the awareness material that it delivered quarterly and the delivery method(s) (posters, emails, topics at staff meetings, etc.). The intent is that tracking of reception of the messages by personnel is not required.

Requirement R3:

The intent of CIP-003-6~~5~~, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-6~~5~~, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-6

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-6:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-004-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is six calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-6Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or

CIP-004-6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-0046 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)			The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			years of the previous PRA completion date. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary. (4.3)	and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or			OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unnecessary. (4.4)			
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4) OR The Responsible Entity has implemented	individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR The Responsible Entity has implemented			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the

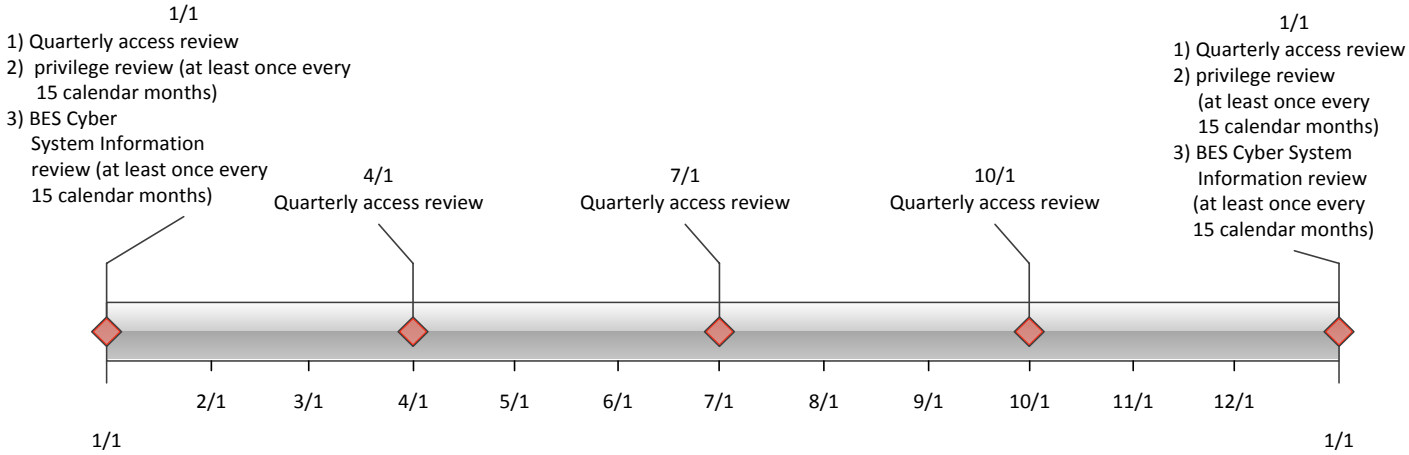
criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group



assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-~~5.1~~6

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~5.1~~6:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-004-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is six calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-004 ~~5.1~~ exists as part of a suite of CIP Standards related to cyber security, which ~~CIP-002-5~~ requires the initial identification and categorization of BES Cyber Systems ~~CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards.*~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement **in a manner that identifies, assesses, and corrects deficiencies, . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements~~

~~described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~ 6Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or

CIP-004-~~5.1~~6 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ ~~a~~ one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~5.1~~6 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-~~5.1~~6 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-~~5~~6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-~~5~~ 6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-~~5.1~~6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~5.1~~6 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-~~5.1~~6 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess~~	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess~~	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	~~and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized	~~and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9~~, and did not identify, assess and correct the deficiencies~~. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access~~, and did not~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access~~, and did not identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)	unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)	~~identify, assess and correct the deficiencies~~. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date~~, and did not identify, assess and correct the deficiencies~~. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date~~, and did not identify, assess and correct the deficiencies~~. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals~~, and did not identify, assess, and~~	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals~~, and did not identify, assess, and~~	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual~~, and did not identify, assess, and correct the deficiencies~~. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	~~correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted	~~correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual~~, and did not identify, assess, and correct the deficiencies~~. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	physical access within 7 calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)	physical access within 7 calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date ~~and has identified deficiencies, and did not identify, assess, and correct the deficiencies~~. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual~~, and did not identify, assess, and correct the deficiencies~~. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date~~, and did not identify, assess, and correct the deficiencies~~. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter~~, and did not identify, assess and correct the deficiencies~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	BES Cyber System Information is located~~, and did not identify, assess, and correct the deficiencies~~. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters~~, and did not identify, assess, and correct the deficiencies~~. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is	calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)	calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary~~, and did not identify, assess and correct the deficiencies~~. (4.4)			were incorrect or unnecessary~~, and did not identify, assess, and correct the deficiencies~~. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3) OR The Responsible Entity has implemented	complete the removal within 24 hours of the termination action but did not initiate those removals for one individual~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that~~-~~ an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that ~~-~~an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that ~~-~~an individual no longer

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.4) OR The Responsible Entity has implemented one or more process(es) to	day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3)	day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action~~, and did not identify, assess, and correct the deficiencies~~. (5.3)	requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date~~, and did not identify, assess, and correct the deficiencies~~. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals~~, and did not identify, assess, and correct the deficiencies~~. (5.5) OR The Responsible			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances~~, and did not~~			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~5.1~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~identify, assess, and correct the deficiencies~~. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but

a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the

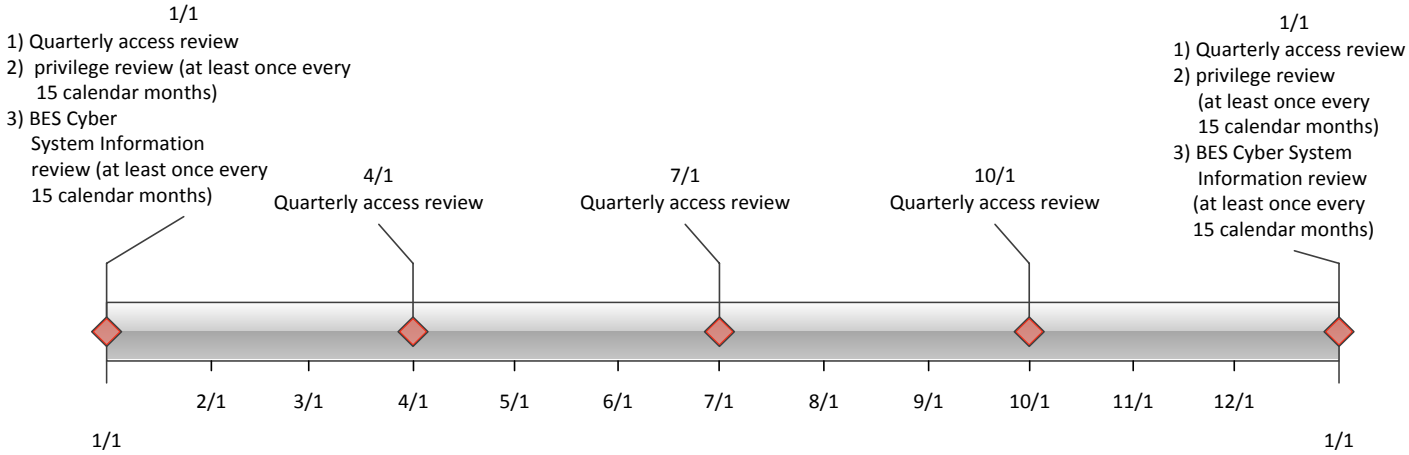
criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group



assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-6

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

6. Background:

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

R2. Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)
R2	**Same-Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)
R3	**Long Term Planning**	**Lower**	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)			Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-3 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-56

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

6. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security, which ~~, CIP-002-5~~ requires the initial identification and categorization of BES Cyber Systems~~, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of

300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access

authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6~~7~~ and 1.7~~8~~ beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-~~5~~ 6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-~~5~~ 6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-~~5~~ 6 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-~~5~~ 6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.10	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~5~~ 6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-~~5~~6 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-~~5~~ 6 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~5~~ 6 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	N/A ~~The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8)~~ ~~OR~~	N/A ~~The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7)~~ ~~OR~~ ~~The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7)~~ ~~OR~~ ~~The Responsible Entity has a process communicate alerts within 15 minutes to~~	N/A ~~The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5)~~ ~~OR~~	The Responsible Entity did not document or implement physical security plans. (R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) ~~OR~~ ~~The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1)~~ ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-65)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8)~~ ~~OR~~ ~~The Responsible Entity has a process to retain physical access logs for~~	~~identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7)~~ ~~OR~~ ~~The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)~~	~~The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not~~	~~The Responsible Entity documented and implemented operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1)~~ OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) ~~OR~~ ~~The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies,~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)		assess or correct the deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)	but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3)~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or correct the deficiencies. (1.4)~~ ~~OR~~ ~~The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4)~~ OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical ~~security~~ Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-65)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Same-Day Operations**	**Medium**	N/A	N/A ~~The Responsible Entity included a visitor control program that requires logging of each of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or~~	N/A ~~The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)~~	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~correct the deficiencies. (2.2)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3)~~ ~~OR~~ ~~The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)~~		retain visitor logs for at least ninety days. (2.3)
R3	**Long Term Planning**	**Lower**	The Responsible Entity has documented and	The Responsible Entity has documented and implemented a maintenance and testing program for	The Responsible Entity has documented and implemented a maintenance and testing program for	The Responsible Entity ~~has~~ did not document~~ed and~~ or implement~~ed~~ a maintenance and testing program for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6~~7~~ and 1.7~~8~~ beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-3 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the

physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-6

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-007-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-6, Requirement R1, Parts 1.2 and Parts 1.3 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until six calendar months after the effective date of Reliability Standard CIP-007-6.

6. Background:

Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

Rationale for Requirement R5 (continued):

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R1. (R1)
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes,	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an	including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or	installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented	CIP-007-6 Table R2. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)	process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (R3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					missed two or more intervals. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-6 Table R5*. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or	known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for

individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement but do not meet the additional obligations for transient devices.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period

called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common

configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password

guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-~~5~~6

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-007-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-6, Requirement R1, Parts 1.2 and Parts 1.3 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until six calendar months after the effective date of Reliability Standard CIP-007-6.

6. Background:

Standard CIP-007 ~~-5~~ exists as part of a suite of CIP Standards related to cyber security, which~~. CIP-002-5.1~~ requires the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ 2~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on~~

~~*whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies,** . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is

specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-~~5~~ 6 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or ~~removable~~ Removable ~~media~~Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-~~5~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-~~5~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-~~5~~ 6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

R3. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-~~5~~ 6 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

R4. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-~~5~~ 6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

Rationale for Requirement R5 (continued):

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

R5. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~5~~ 6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~5~~ 6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or ~~removable~~ Removable ~~media~~Media ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (1.2) ~~OR~~ ~~The Responsible Entity has~~	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (1.1) ~~OR~~ ~~The Responsible Entity has implemented and documented processes for determining~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R1 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R1) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R1 but did not identify, assess, or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)~~	~~necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)~~	~~the deficiencies. (R1)~~
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R2 ~~and has identified deficiencies but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but~~	sources, for tracking or evaluating cyber security patches for applicable Cyber Assets ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1)~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or~~	applicable Cyber Assets ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1)~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)~~ OR The Responsible Entity has documented and	~~not assess or correct the deficiencies~~. (R2)~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R2 but did not identify, assess, or correct the deficiencies. (R2)~~ OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35	~~correct the deficiencies. (2.1)~~ OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2)	implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (2.2) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for~~	security patches for applicable Cyber Assets~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.1) ~~OR~~ ~~The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1)~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but less than 50 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation~~	OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct~~	~~applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation	The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.4)~~OR~~ ~~The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)~~	~~the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess,~~	plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.3) ~~OR~~ ~~The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an~~	~~not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4)~~ OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (2.4) ~~OR~~ ~~The Responsible Entity documented~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~or correct the deficiencies. (2.3)~~	~~existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)~~	~~a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the deficiencies. (2.4)~~
R3	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns ~~and has identified deficiencies but did~~	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code ~~and has identified deficiencies but did not assess or correct~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R3 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R3) ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~not assess or correct the deficiencies~~. (3.3) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)~~	~~the deficiencies~~. (3.2)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and did not identify, assess, or correct the deficiencies. (3.2)~~ OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used,	~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R3 and did not identify, assess, or correct the deficiencies. (R3)~~ OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code~~ and has identified deficiencies but did not assess or correct~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					the Responsible Entity did not update malicious code protections ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (3.3)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies.~~ ~~(3.3)~~	~~the deficiencies~~. (3.1) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.4) ~~The Responsible Entity has documented and~~	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2~~and has identified deficiencies but did not assess or correct the deficiencies~~. (4.2)~~OR~~ ~~The Responsible Entity has documented and~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~5~~ 6 Table R4 ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (R4)~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-5 Table R4 and did not identify, assess, or correct the deficiencies. (R4)~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4~~	~~implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2)~~ OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in	The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3~~and has identified deficiencies but did not assess or correct the deficiencies~~. (4.1) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to log events for the~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (4.3) ~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional~~	~~Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3)~~OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals~~ and has identified deficiencies but did~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~not assess or correct the deficiencies~~. (4.4)~~OR~~ ~~The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)~~	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented	The Responsible Entity has implemented one or more documented	The Responsible Entity has implemented one or more documented	The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for~~	process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~The Responsible Entity has implemented one or more documented process(es) for password-only~~	process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) ~~and has identified deficiencies but did not assess or correct the deficiencies~~. (5.2) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the~~	more process(es) that included the applicable items in *CIP-007-~~5~~ 6 Table R5 ~~and has identified deficiencies but did not assess or correct the deficiencies~~*. (R5) ~~OR~~ ~~The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5)~~OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~password only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2)~~OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts~~ and has identified deficiencies but did~~	process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~not assess or correct the deficiencies~~. (5.3) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)~~OR The Responsible Entity has implemented one or more documented process(es) for password-only	authentication of interactive user access~~ and did not identify, assess, or correct the deficiencies~~. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.4) ~~OR~~ ~~The Responsible Entity has~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce	~~implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4)~~OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					one of the two password parameters as described in 5.5.1 and 5.5.2~~ and did not identify, assess, or correct the deficiencies~~. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months	described in 5.5.1 and 5.5.2~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.5) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify, assess,~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6) ~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password~~	~~or correct the deficiencies. (5.5)~~ OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.6)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~change and did not identify, assess, or correct the deficiencies. (5.6)~~	~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)~~OR The Responsible Entity has implemented one or more documented process(es) for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts~~ and has identified deficiencies but did not assess or correct the deficiencies~~. (5.7)~~OR~~ ~~The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)~~

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for

individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, ~~portable storage media policies,~~ Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code

cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement but do not meet the additional obligations for transient devices.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible

Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of R~~r~~emovable M~~m~~edia in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor.

Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-6

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-65 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	between tests of the plan. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

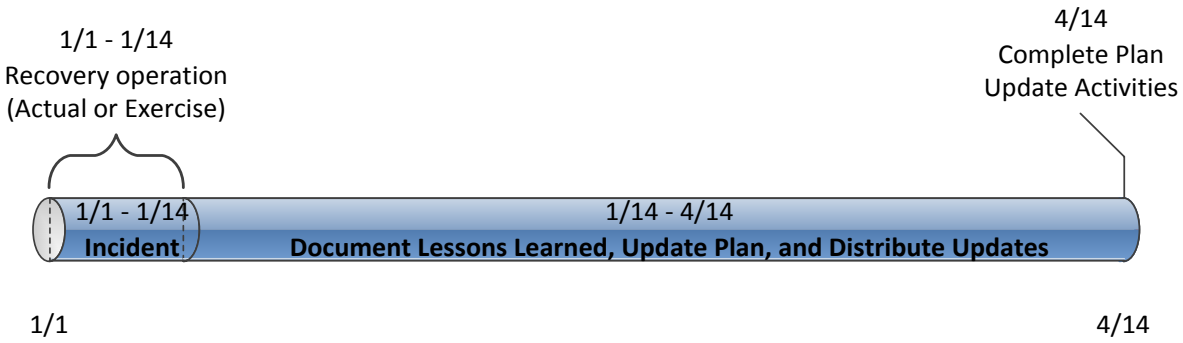


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

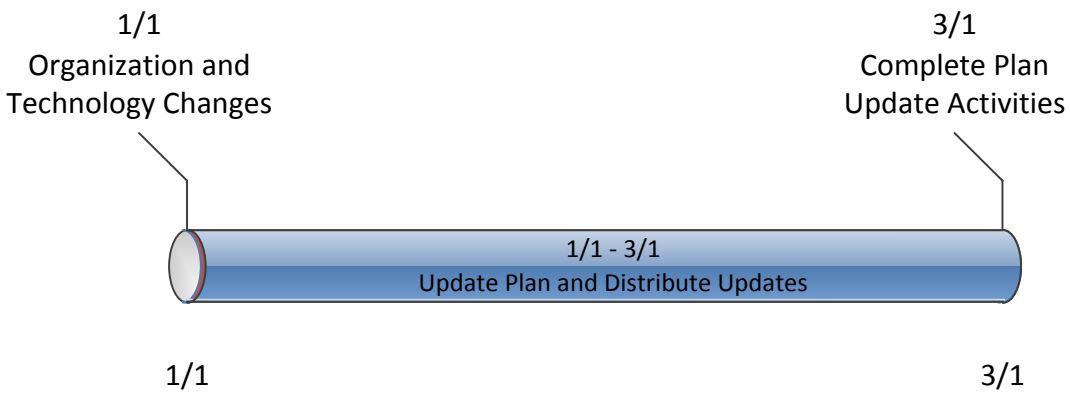


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-~~5~~6

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-~~5~~6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-009~~-5~~ exists as part of a suite of CIP Standards related to cyber security, which~~. CIP-002-5.1~~ require~~s~~ the initial identification and categorization of BES Cyber Systems~~. CIP-003-5~~6, CIP-004-56, CIP-005-5, CIP-006-56, CIP-007-56, CIP-008-5, CIP-009-56, CIP-010-12, and CIP-011-1 2 and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies,** . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications*.

CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-~~5~~ 6 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-~~5~~ 6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-6~~5~~ Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-~~5~~ 6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-~~5~~ 6 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-~~5~~ 6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-~~5~~ 6 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-~~5~~ 6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-~~5~~ 6 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests~~, and~~	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests~~, and when tested, any~~	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests~~, and~~	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1)~~ ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~when tested, any deficiencies were identified, assessed, and corrected~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.3)	~~deficiencies were identified, assessed, and corrected~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.3)	~~when tested, any deficiencies were identified, assessed, and corrected~~. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests~~, and when tested, any deficiencies were identified, assessed, and corrected~~. (2.3)	~~OR~~ The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) ~~OR~~ ~~The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)~~ ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2)~~ OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~deficiencies, but did not assess or correct the deficiencies. (2.3)~~ ~~OR~~ ~~The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)~~
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1) OR	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-~~5~~6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					• Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

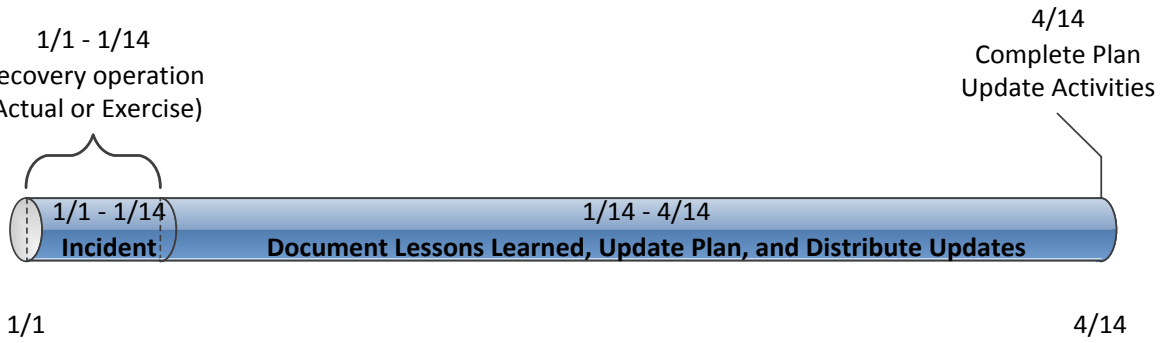


Figure 1: CIP-009-~~5~~ 6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

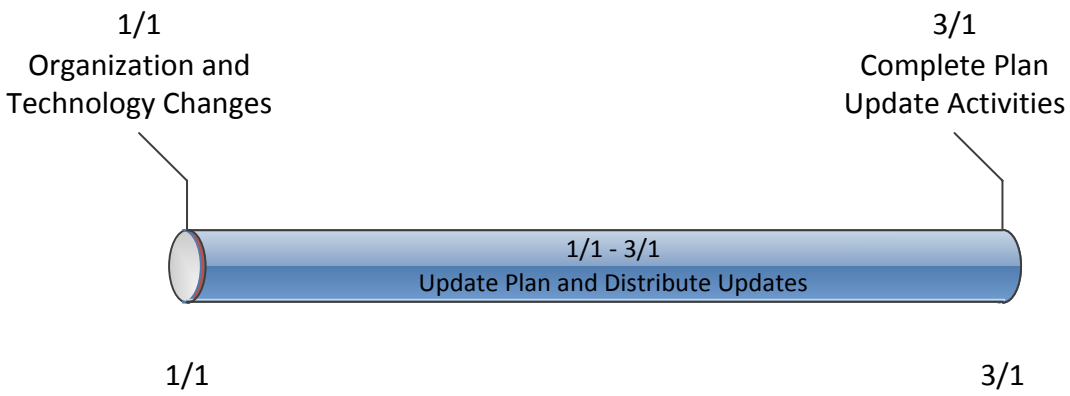


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-2

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-010-2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

Rationale for R4:

Requirement R4 is to address FERC Order No. 791 Paragraphs 6 and 136, which require the standards to address security-related issues associated with tools specifically used for data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To that end, the requirement goals are as follows:

(1) Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and

(2) Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

The SDT has incorporated the concepts of other requirements from FERC-approved CIP-010-1 and CIP-007-5 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: This is a new requirement. All requirements related to Transient Devices and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. While the requirements are similar, they are not to the same rigor of those found in CIP-007 protecting the permanent assets identified by an entity. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances. Authorization shall include: 4.1.1. Users, individually or by group/role; 4.1.2. Locations, individually or by group/role; 4.1.3. Defined acceptable use; and 4.1.4. Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the authorized software for each Transient Cyber Asset, individually or by group; or • A record in an asset management system that identifies the authorized configuration for each Transient Cyber Asset individually or by group.
4.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability).	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus hardening, policies, verification of method(s) employed by vendors, etc.).

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to detect malicious code on Removable Media prior to use on applicable systems.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus scanning techniques, verification of method(s) employed by vendors, etc.).
4.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
4.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.6	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4. For a modification that deviates from the state in Part 4.1.4, either: • Remediate by returning the Transient Cyber Asset to the state in Part 4.1.4; or • Update Part 4.1.4.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any remediation activities.
4.7	High Impact BES Cyber Systems and associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, within 35 calendar days prior to use, to ensure security patches are up-to-date. For security patches that are not up-to-date, take one of the following actions: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any mitigation activities.

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

b. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints Text

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity did not document or implement process(es) that collectively address the requirement

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of Transient Cyber Assets, but failed to include one of the required items listed in 4.1.1 through 4.1.4. (4.1)	of Transient Cyber Assets, but failed to include two of the required items listed in 4.1.1 through 4.1.4. (4.1)	of Transient Cyber Assets, but failed to include three of the required items listed in 4.1.1 through 4.1.4. (4.1) OR The Responsible Entity documented and implemented a process to evaluate Transient Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 but did not take one of the actions required by Requirement R4, Part 4.6. (4.6) OR The Responsible Entity documented and implemented a process to evaluate	parts as required by Requirement R4. (R4) OR The Responsible Entity did not use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability) as required by Requirement R4, Part 4.2. (4.2) OR The Responsible Entity did not use method(s) to detect malicious code on Removable Media prior to use on applicable systems as required by Requirement R4, Part 4.3. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Transient Cyber Assets within 35 calendar days prior to use but did not take one of the actions required by Requirement R4, Part 4.7. (4.7)	OR The Responsible Entity did not mitigate the threat of detected malicious code for Transient Cyber Assets or Removable Media as required by Requirement R4, Part 4.4. (4.4) OR The Responsible Entity did not update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns as required by Requirement R4, Part 4.5. (4.5) OR The Responsible Entity did not evaluate Transient

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 as required by Requirement R4, Part 4.6. (4.6) OR The Responsible Entity did not evaluate Transient Cyber Assets within 35 calendar days prior to use as required by Requirement R4, Part 4.7. (4.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT

believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.

2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

This Requirement applies to any transient devices (i.e. Transient Cyber Assets and Removable Media) that will be connected temporarily to an applicable system. Examples of these devices include, but are not limited to:

- Hardware/software diagnostic test equipment
- Hardware/software packet sniffers
- Hardware/software used for BES Cyber System maintenance
- Hardware/software used for BES Cyber System configuration
- Hardware/software used to perform vulnerability assessments

Transient Cyber Assets can be in the form of a laptop, desktop, or tablet. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

This requirement does not cover hardware/software components that may support information system maintenance yet are a part of the system, for example the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of a switch.

Requirement Parts 4.1, 4.3, 4.6, and 4.7 refer to the term “prior to use” related to when specific actions must occur. For purposes of this standard, "use" is considered to be the interaction between transient devices and applicable systems. The interaction between transient devices and multiple applicable systems within the same ESP or PSP would be considered a single use. For example, a technician would need to have a laptop evaluated only once according to Part 4.6 when working in the same PSP. The technician would not need to have the evaluation performed each time it connects to a different Cyber Asset.

Requirement Part 4.1:

Requirement Part 4.1 requires the entity to document and implement its process to authorize the use of Transient Cyber Assets. This allows entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1. User(s), individually or by group/role, allowed to use Transient Cyber Assets. This is intended to provide assurance around who has physical proximity to the Transient Cyber Assets. These user(s) must have authorized electronic and unescorted physical access to the applicable system in accordance with CIP-004.
2. Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group/role of locations. Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e. high impact, medium impact, low impact). These impact areas have differing levels of protection under the CIP Requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. It may be reasonable to have separate Transient Cyber Assets for each impact level.
3. The intended or approved use of each Transient Cyber Asset. Activities not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals on the activities or uses that are not allowed (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).
4. The operating system, firmware, and intentionally installed software. All of this information may not be available or relevant to each Transient Cyber Asset. Having this information facilitates the review in Part 4.6. The use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The Standard Drafting Team does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included.

CAUTION: Entities should exercise caution when using Transient Cyber Assets and ensure they do not have wireless or Bluetooth features enabled in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber

Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Requirement Parts 4.2, 4.3, 4.4, and 4.5:

Requirement Parts 4.2 and 4.3 address the protection against the introduction of malicious code by Transient Cyber Assets or Removable Media. For Transient Cyber Assets, the entity may either pre-authorize an inventory of Cyber Assets or authorize devices at the time of connection. Pre-authorized Transient Cyber Assets may have the malicious code prevention maintained on the device and do not require specific actions for each use.

It is the responsibility of the entity to ensure that the Transient Cyber Assets it owns and manages have methods deployed to deter, detect, or prevent malicious code. It is also the entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not own or manage, including vendor assets.

For Removable Media and Transient Cyber Assets authorized at the time of connection, the detection of malicious code must be addressed prior to use. This can be performed by scanning the Transient Cyber Assets or Removable Media in an environment outside of the Electronic Security Perimeter (ESP). Entities should use caution not to place kiosks or other scanning devices used to comply with this Requirement inside the ESP.

For Requirement R4, Part 4.4, if malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Part 4.5 requires a process to update signatures or patterns, where applicable. This process is to be documented in the overarching program. As with CIP-007-6, Requirement R3, the process is to include testing and installing of updated signatures or patterns.

Requirement Parts 4.6 and 4.7:

Requirement R4, Part 4.6 requires the entity to evaluate Transient Cyber Assets to ensure that no unauthorized modifications have been made to the operating system, firmware, or software. This is a review of the current state against what is currently documented pursuant to Part 4.1.4. If there are differences, the modified code may be removed or the documentation updated to align to the authorized or current state.

Similarly, Requirement R4, Part 4.7 requires the entity to evaluate Transient Cyber Assets to ensure that patches are up-to-date. This is a review of the patches currently installed against what is currently documented. If there are missing patches, these should be tested and applied or a mitigation plan should be created to mitigate the vulnerabilities addressed by each uninstalled security patch. This should be performed prior to connecting the Transient Cyber Asset to an applicable system. For a device that the entity does not manage (i.e. vendor laptop), this can be performed immediately prior to connecting the Transient Cyber Asset to an applicable system. For an entity-managed device, the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-~~1~~2

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-~~1~~2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

6. Background:

Standard CIP-010 ~~-1~~ exists as part of a suite of CIP Standards related to cyber security, which~~. CIP-002-5~~ require~~s~~ the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~ This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to~~

~~change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement~~**~~, in a manner that identifies, assesses, and corrects deficiencies,~~** ~~. . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~ 2 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-~~1~~ 2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-~~1~~ 2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-~~1~~2 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~ 2 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~1~~ 2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~1~~ 2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~1~~ 2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~1~~ 2 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

Rationale for R4:

Requirement R4 is to address FERC Order No. 791 Paragraphs 6 and 136, which require the standards to address security-related issues associated with tools specifically used for data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To that end, the requirement goals are as follows:

(1) Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and

(2) Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

The SDT has incorporated the concepts of other requirements from FERC-approved CIP-010-1 and CIP-007-5 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: This is a new requirement. All requirements related to Transient Devices and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. While the requirements are similar, they are not to the same rigor of those found in CIP-007 protecting the permanent assets identified by an entity. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances. Authorization shall include: 4.1.1. Users, individually or by group/role; 4.1.2. Locations, individually or by group/role; 4.1.3. Defined acceptable use; and 4.1.4. Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the authorized software for each Transient Cyber Asset, individually or by group; or • A record in an asset management system that identifies the authorized configuration for each Transient Cyber Asset individually or by group.
4.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability).	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus hardening, policies, verification of method(s) employed by vendors, etc.).

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Use method(s) to detect malicious code on Removable Media prior to use on applicable systems.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus scanning techniques, verification of method(s) employed by vendors, etc.).
4.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
4.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.6	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4. For a modification that deviates from the state in Part 4.1.4, either: • Remediate by returning the Transient Cyber Asset to the state in Part 4.1.4; or • Update Part 4.1.4.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any remediation activities.
4.7	High Impact BES Cyber Systems and associated: • PCA Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA	Evaluate Transient Cyber Assets, within 35 calendar days prior to use, to ensure security patches are up-to-date. For security patches that are not up-to-date, take one of the following actions: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch.	An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any mitigation activities.

C. Compliance

1. Compliance Monitoring Process:

a. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

b. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

c. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigation

Self-Reporting

Complaints Text

d. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified~~	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~OR~~ ~~The Responsible Entity has documented and~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ ~~OR~~	~~identified deficiencies but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to determine required~~	~~deficiencies but did not assess and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has a process(es) that requires authorization and documentation for~~	~~implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)~~ OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify,~~	~~security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1)~~	~~changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to update~~	update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~assess, or correct the deficiencies in the verification documentation. (1.4.3)~~		~~baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess,~~	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~or correct the deficiencies. (1.3)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to verify that required~~	from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2)~~ ~~OR~~ ~~The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~the deficiencie (1.5.1)~~ ~~OR~~ ~~The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1)~~ ~~OR~~ ~~The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~environments and identified deficiencies but did not assess or correct the deficiencies. (1.5.2)~~ ~~OR~~ ~~The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)~~OR~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~not identify, assess, or correct the deficiencies. (2.1)~~
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months,	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months,	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity has documented and implemented process(es) addressing authorization of use	The Responsible Entity did not document or implement process(es) that collectively address the requirement

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of Transient Cyber Assets, but failed to include one of the required items listed in 4.1.1 through 4.1.4. (4.1)	of Transient Cyber Assets, but failed to include two of the required items listed in 4.1.1 through 4.1.4. (4.1)	of Transient Cyber Assets, but failed to include three of the required items listed in 4.1.1 through 4.1.4. (4.1) OR The Responsible Entity documented and implemented a process to evaluate Transient Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 but did not take one of the actions required by Requirement R4, Part 4.6. (4.6) OR The Responsible Entity documented and implemented a process to evaluate	parts as required by Requirement R4. (R4) OR The Responsible Entity did not use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability) as required by Requirement R4, Part 4.2. (4.2) OR The Responsible Entity did not use method(s) to detect malicious code on Removable Media prior to use on applicable systems as required by Requirement R4, Part 4.3. (4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-12)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Transient Cyber Assets within 35 calendar days prior to use but did not take one of the actions required by Requirement R4, Part 4.7. (4.7)	OR The Responsible Entity did not mitigate the threat of detected malicious code for Transient Cyber Assets or Removable Media as required by Requirement R4, Part 4.4. (4.4) OR The Responsible Entity did not update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns as required by Requirement R4, Part 4.5. (4.5) OR The Responsible Entity did not evaluate Transient

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Cyber Assets prior to use for modifications that deviate from documentation per Part 4.1.4 as required by Requirement R4, Part 4.6. (4.6) OR The Responsible Entity did not evaluate Transient Cyber Assets within 35 calendar days prior to use as required by Requirement R4, Part 4.7. (4.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-~~5~~6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-~~5~~ 6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT

believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.

2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

This Requirement applies to any transient devices (i.e. Transient Cyber Assets and Removable Media) that will be connected temporarily to an applicable system. Examples of these devices include, but are not limited to:

- Hardware/software diagnostic test equipment
- Hardware/software packet sniffers
- Hardware/software used for BES Cyber System maintenance
- Hardware/software used for BES Cyber System configuration
- Hardware/software used to perform vulnerability assessments

Transient Cyber Assets can be in the form of a laptop, desktop, or tablet. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

This requirement does not cover hardware/software components that may support information system maintenance yet are a part of the system, for example the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of a switch.

Requirement Parts 4.1, 4.3, 4.6, and 4.7 refer to the term “prior to use” related to when specific actions must occur. For purposes of this standard, "use" is considered to be the interaction between transient devices and applicable systems. The interaction between transient devices and multiple applicable systems within the same ESP or PSP would be considered a single use. For example, a technician would need to have a laptop evaluated only once according to Part 4.6 when working in the same PSP. The technician would not need to have the evaluation performed each time it connects to a different Cyber Asset.

Requirement Part 4.1:

Requirement Part 4.1 requires the entity to document and implement its process to authorize the use of Transient Cyber Assets. This allows entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1. User(s), individually or by group/role, allowed to use Transient Cyber Assets. This is intended to provide assurance around who has physical proximity to the Transient Cyber Assets. These user(s) must have authorized electronic and unescorted physical access to the applicable system in accordance with CIP-004.
2. Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group/role of locations. Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e. high impact, medium impact, low impact). These impact areas have differing levels of protection under the CIP Requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. It may be reasonable to have separate Transient Cyber Assets for each impact level.
3. The intended or approved use of each Transient Cyber Asset. Activities not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals on the activities or uses that are not allowed (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).
4. The operating system, firmware, and intentionally installed software. All of this information may not be available or relevant to each Transient Cyber Asset. Having this information facilitates the review in Part 4.6. The use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The Standard Drafting Team does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included.

CAUTION: Entities should exercise caution when using Transient Cyber Assets and ensure they do not have wireless or Bluetooth features enabled in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber

Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Requirement Parts 4.2, 4.3, 4.4, and 4.5:

Requirement Parts 4.2 and 4.3 address the protection against the introduction of malicious code by Transient Cyber Assets or Removable Media. For Transient Cyber Assets, the entity may either pre-authorize an inventory of Cyber Assets or authorize devices at the time of connection. Pre-authorized Transient Cyber Assets may have the malicious code prevention maintained on the device and do not require specific actions for each use.

It is the responsibility of the entity to ensure that the Transient Cyber Assets it owns and manages have methods deployed to deter, detect, or prevent malicious code. It is also the entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not own or manage, including vendor assets.

For Removable Media and Transient Cyber Assets authorized at the time of connection, the detection of malicious code must be addressed prior to use. This can be performed by scanning the Transient Cyber Assets or Removable Media in an environment outside of the Electronic Security Perimeter (ESP). Entities should use caution not to place kiosks or other scanning devices used to comply with this Requirement inside the ESP.

For Requirement R4, Part 4.4, if malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Part 4.5 requires a process to update signatures or patterns, where applicable. This process is to be documented in the overarching program. As with CIP-007-6, Requirement R3, the process is to include testing and installing of updated signatures or patterns.

Requirement Parts 4.6 and 4.7:

Requirement R4, Part 4.6 requires the entity to evaluate Transient Cyber Assets to ensure that no unauthorized modifications have been made to the operating system, firmware, or software. This is a review of the current state against what is currently documented pursuant to Part 4.1.4. If there are differences, the modified code may be removed or the documentation updated to align to the authorized or current state.

Similarly, Requirement R4, Part 4.7 requires the entity to evaluate Transient Cyber Assets to ensure that patches are up-to-date. This is a review of the patches currently installed against what is currently documented. If there are missing patches, these should be tested and applied or a mitigation plan should be created to mitigate the vulnerabilities addressed by each uninstalled security patch. This should be performed prior to connecting the Transient Cyber Asset to an applicable system. For a device that the entity does not manage (i.e. vendor laptop), this can be performed immediately prior to connecting the Transient Cyber Asset to an applicable system. For an entity-managed device, the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-2

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-011-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples

may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset, Transient Cyber Asset, or Removable Media is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-~~1~~2

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-~~1~~2:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

Reliability Standard CIP-011-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. Background:

Standard CIP-011 ~~-1~~ exists as part of a suite of CIP Standards related to cyber security, which~~. CIP-002-5~~ require~~s~~ the initial identification and categorization of BES Cyber Systems~~. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~ and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. ~~This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.~~

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

~~The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:~~

~~Each Responsible Entity shall implement, **in a manner that identifies, assesses, and corrects deficiencies,** . . .~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it~~-~~ believes necessary in ~~their~~ its documented processes, but ~~they~~ it must address the applicable requirements in the table. ~~The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.~~

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

R1. Each Responsible Entity shall implement~~, in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-~~1~~ 2 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~1~~ 2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~1~~ 2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-~~1~~ 2 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

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

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

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	N/A ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify,~~	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~assess, or correct the deficiencies. (1.1)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2)~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information~~	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-~~1~~2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~but did not identify, assess, or correct the deficiencies. (1.2)~~	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-~~1~~ 2 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. ~~Furthermore,~~

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset, Transient Cyber Asset, or Removable Media is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Implementation Plan

Project 2014-02 CIP Version 5 Revisions

May 30, 2014

Requested Approvals

- CIP-003-6 — Cyber Security — Security Management Controls
- CIP-004-6 — Cyber Security — Personnel and Training
- CIP-006-6 — Cyber Security — Physical Security
- CIP-007-6 — Cyber Security — Systems Security Management
- CIP-009–6 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-2 — Cyber Security — Configuration Change Management
- CIP-011-2 — Cyber Security — Information Protection

Requested Retirements

- CIP-003-5 — Cyber Security — Security Management Controls
- CIP-004-5 — Cyber Security — Personnel and Training
- CIP-006-5 — Cyber Security — Physical Security
- CIP-007-5 — Cyber Security — Systems Security Management
- CIP-009-5 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP-010-1 — Cyber Security — Configuration Change Management
- CIP-011-1 — Cyber Security — Information Protection

Prerequisite Approvals

None

Revisions to Defined Terms in the NERC Glossary

The standards drafting team proposes modifying the following defined terms in the NERC Glossary:

BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. A Transient Cyber Asset is not a BES Cyber Asset.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Transient Cyber Asset is not a Protected Cyber Asset.

The standards drafting team proposes the following new defined terms for incorporation into the NERC Glossary:

Removable Media	Portable media, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media.
Transient Cyber Asset	A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Effective Dates

The effective dates for each of the proposed Reliability Standards and NERC Glossary terms are provided below. Where the standard drafting team identified the need for a longer implementation period for compliance with a particular element (i.e., an entire Requirement or a portion thereof) of a proposed Reliability Standard, the additional time for compliance with that element is specified below. The compliance date for those particular elements represents the date that entities must begin to comply that particular element of the Reliability Standard, even where the Reliability Standard goes into effect at an earlier date.

1. CIP-003-6 — Cyber Security — Security Management Controls

   Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-003-6, Requirement R2

   Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

2. CIP-004-6 — Cyber Security — Personnel and Training

   Reliability Standard CIP-004-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is six calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

3. CIP-006-6 — Cyber Security — Physical Security

Reliability Standard CIP-006-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-006-6, Requirement R1, Part 1.10

For new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3, Registered Entities shall not be required to comply with Reliability Standard CIP-006-6, Requirement R1, Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6.

4. CIP-007-6 —Cyber Security — Systems Security Management

Reliability Standard CIP-007-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Compliance Date for CIP-007-6, Requirement R1, Parts 1.2 and 1.3

Registered Entities shall not be required to comply with the elements of Reliability Standard CIP-007-6, Requirement R1, Parts 1.2 and Parts 1.3 that apply to PCAs and nonprogrammable communication components located inside a PSP and inside an ESP and associated with High and Medium Impact BES Cyber Systems until six calendar months after the effective date of Reliability Standard CIP-007-6.

5. CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems

   Reliability Standard CIP–009-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

6. CIP-010-2 — Cyber Security — Configuration Change Management

   Reliability Standard CIP-010-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

   Compliance Date for CIP-010-2, Requirement R4

   Registered Entities shall not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2.

7. CIP-011-2 — Cyber Security — Information Protection

   Reliability Standard CIP-011-2 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the later of April 1, 2016 or on the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

8. New and Modified NERC Glossary Terms

   The new and modified NERC Glossary Terms BES Cyber Asset, Protected Cyber Asset, Removable Media, and Transient Cyber Asset shall become effective on the same compliance date as when Reliability Standard CIP-010-2, Requirement R4 is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective the same compliance date as when Reliability Standard CIP-010-2, Requirement R4 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

9. Standards for Retirement

   Midnight of the day immediately prior to the Effective Date in the particular jurisdiction in which the new standard or definition is becoming effective.

Certain Compliance Dates in the Implementation Plan for Version 5 CIP Cyber Security Standards Remain the Same

The following sections of the Implementation Plan for Version 5 CIP Cyber Security Standards[1] (Version 5 Plan) remain the same:

- *Initial Performance of Certain Periodic Requirements*
  - For those requirements with recurring periodic obligations, refer to the Version 5 Plan for compliance dates. These compliance dates are not extended by the effective date of CIP Version 5 Revisions.
- *Previous Identity Verification*
  - The same concept in this section applies for CIP Version 5 Revisions. A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be repeated under CIP-004-6, Requirement R3, Part 3.1.
- *Planned or Unplanned Changes Resulting in a Higher Categorization*
  - The same concept applies for CIP Version 5 Revisions.

[1] Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012, available online at http://www.nerc.com/pa/Stand/CIP00251RD/Implementation_Plan_clean_4_(2012-1024-1352).pdf

Notes of Standards Committee Meeting (in Italic)

June 10, 2014 | 1:00 – 5:00 p.m. Mountain
June 11, 2014 | 8:00 – Noon Mountain

Xcel Energy
1800 Larimer Street
Denver, CO 80212

1. **Review of Agenda — (Approve)** (5 minutes)

   SC waived the 5-day rule to allow it taking action on the proposed Phase 2 GMD standard (Item 12). Relevant materials were distributed on June 4, less than 5 days before this meeting. Staff wanted to post these standard for commenting/balloting before end of this week.

2. ***Consent Agenda — (Approve)*** *(5 minutes)*

   a. May 14, 2014 Meeting Minutes*- **(Approve)**

   b. May 16, 2014 Meeting Minutes*- **(Approve)**

   Both sets approved, with slight amendment to the May 14 minutes. The issue with showing names of subcommittee members or SDT members approved by the SC continued to be tabled until the July CS meeting.

3. **Three-Month Outlook on Upcoming Standard Projects or Issues*— (Update)** (V. Agnew, S. Miller) (10 minutes)

   There is a typo in the July posting. The standard to be posted is PRC-006-1, not PRC-010-1.

4. **Projects Under Development — (Review)**

   a. Project Tracking Spreadsheet (R. Parsons, V. Agnew, L. Hussey, S. Noess) (15 minutes)

      Jennifer Sterling presented. No issues.

   b. Projected Posting Schedule (B. Nutter) (5 minutes)

      Staff presented. No issues.

5. **Project 2008-02 Undervoltage Load Shedding*— (Authorize)** (V. Agnew) (15 minutes)

   Raised a concern issue that a revised SAR for this project is being posted for commenting. Posting the revised standards for commenting and balloting before closure of the SAR commenting period is premature, and sends a message to the industry that we ignore industry comments on the revised SAR and just move ahead with the changes we have in mind.

Also raised the issue on PRC-004-2 where the UVLS was excluded by UFLS was included. Staff's response was that misoperations of both UFLS and UVLS will be addressed by the PRC-004-2 project.

Made a motion to approve posting of the draft standard after the SAR commenting period is closed. Motion was approved unanimously.

6. **Project 2010-05.2 Special Protection Systems*— (Authorize)** (V. Agnew) (15 minutes)

   Approved to post the revised definition of "Remedial Action Scheme" ("RAS"), the affected Reliability Standards (43 of them) revised to reflect use of the single term RAS, and the associated Implementation Plan for an initial 45-day formal comment period.

7. **Project 2010-14.2 Periodic Review of BAL Standards*— (Accept, Appoint)** (L. Hussey) (15 minutes)

   Suggested to extract one of the recommendations: "Appoint the BAL PRT as the standard drafting team for the new Project 2010-14.2 Implementation of BAL Periodic Review Recommendations." To be placed under a separate motion for discussion.

   Raised the issue that regardless of how good the PRT members are and how many of them are recommended to stay on with the SDT, there needs to be public solicitation to at least add some new members if not to open all seats for potential candidates. If the recommendation is approved as is, we are sending a message to the industry that: if you are not with us during the informal development/outreach stage, you won't be able to join us in standard drafting.

   Most members shared this concern. Made a motion to openly solicit nominations. Existing PRT members are encouraged to submit their names. Motion was approved unanimously.

8. **Project 2014-01 Dispersed Generation Resources*— (Authorize)** (L. Hussey) (15 minutes)

   Approved to post the following revised sets of standards for commenting and balloting to avoid generating resource owners having to incur in unnecessary cost to comply with existing VAR-002 and PRC-005 standards only to be excluded from applicability when the proposed standard revisions are approved:

   - *VAR-002-2b(X), and VAR-002-4);*
   - *PRC-005-2(X), PRC-005-3(X), PRC-005-X(X)*

   The reasons for posting more than one version of each standard is to manage the uncertainties with FERC's final decisions on the industry-approved VAR-002-3 and PRC-005-3, both already filed with FERC, and the proposed PRC-005-X standard which is being developed and to be balloted soon. Having the (x) versions commenting and approved by the industry will allow NERC to file the appropriate version depending on FERC's action or inaction.

9. **Subcommittee Reports**

   a. **PMOS Update*** - **(Update)** (J. Sterling) (10 Minutes)

      Ron Parson provided an update. No issues.

b. **Process Subcommittee*— (Update)** (L. Lee) (15 minutes)

i. **Ballot Pool Management*** - **(Informational)** (L. Lee) (15 minutes)

Laura provided an update. No issues.

ii. **Consensus Building and SAR Development*** - **(Endorse)** (B. Li) (15 minutes)

SC approved the scope of task. Task to be initiated soon.

iii. **Review of Standards Processes and Procedures*** - **(Endorse)** (L. Lee) (15 minutes)

Laura provided an update. No issues.

10. **Communication Updates and Activities* — (Update)** (S. Miller, M. Huggins) (10 minutes)

Mallory Huggins provided an update. Starting next week or the week after, the NERC Standards Bulletin will cover both standards and compliance matters.

11. **Upcoming Standards Filings* — (Review)** (S. Tyrewala) (10 minutes)

NERC Legal provided an update. Some recently approved standards have been filed with FERC for approval (e.g. MOD-031, VAR-001-4).

Agenda Items for June 11, 2014

12. **Project 2013-03 Geomagnetic Disturbance Mitigation* — (Authorize)** (L. Hussey) (15 minutes)

Laura Hussey presented. Approved to post the draft standards (TPL-007-1) for commenting and balloting.

13. **Informational Items — (Enclosed)**

a. SC Expectations*

b. 2014 Meeting Dates and Locations*

c. 2014 Standards Committee Roster*

d. Highlights of Parliamentary Procedure*

14. **Adjourn**

Background materials included in agenda package.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Standards Committee Meeting

May 14, 2014 | 1:00 - 4:00 p.m. Eastern

Dial-in: 1-866-740-1260 | Meeting Code: 8314765 | Security Code: 051414

Click here for ReadyTalk web registration

NERC Antitrust Compliance Guidelines and Public Announcement*

Introductions and Chair's Remarks

Agenda Items

1. **Review of Agenda — (Approve)** (5 minutes)
2. **Consent Agenda — (Approve)** (5 minutes)
   a. April 9, 2014 Meeting Minutes* **– (Approve)**
3. **Three-Month Outlook on Upcoming Standard Projects or Issues* — (Update)** (M. Lauby, B. Murphy, S. Miller) (10 minutes)
4. **Projects Under Development — (Review)**
   a. Project Tracking Spreadsheet (R. Parsons, V. Agnew, L. Hussey, S. Noess) (15 minutes)
   b. Projected Posting Schedule (B. Nutter) (5 minutes)
5. **Draft 2015-2017 Reliability Standards Development Plan and Enhanced Periodic Review* — (Authorize)** (B. Murphy, V. Agnew) (30 minutes)
6. **SC Meeting Schedule for 2015* — (Approve)** (B. Murphy, B. Hampton) (5 minutes)
7. **Detail of Minutes re: Appointment of Drafting Teams* — (Approve)** (B. Murphy) (10 minutes)
8. **Reliability Issues Steering Committee Triage Diagram* — (Informational item)** (B. Murphy) (20 minutes)
9. **Update on Reaching Quorum for Standards Ballots* — (Informational item)** (B. Murphy, L. Lee) (10 minutes)
10. **Subcommittee Reports**

a. **PMOS* – (Update)** (J. Sterling) (15 Minutes)

b. **Process Subcommittee***

   i. **Process Subcommittee Membership* – CONFIDENTIAL (Approve)** (L. Lee) (15 minutes)

11. **Communication Updates and Activities* — (Update)** (S. Miller, M. Huggins) (10 minutes)

12. **Upcoming Standards Filings* — (Review)** (S. Tyrewala) (10 minutes)

13. **Informational Items — (Enclosed)**

    a. SC Expectations*

    b. 2014 Meeting Dates and Locations*

    c. 2014 Standards Committee Roster*

    d. Highlights of Parliamentary Procedure*

14. **Adjourn**

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Public Announcements

REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

Conference call version:
Participants are reminded that this conference call is public. The access number was posted on the NERC website and widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Minutes
Standards Committee Meeting

April 9, 2014 | 1:00-4:00 p.m. Eastern

NERC Antitrust Compliance Guidelines and Public Announcement*

S.J. Kim started the meeting and determined there was a quorum. She reviewed the NERC Antitrust Compliance Guidelines and reminded participants that the meeting is public and that notice of the meeting had been widely distributed.

Introductions and Chair's Remarks

B. Murphy informed the Standards Committee (SC) that the Executive Committee (SCEC) did meet to authorize posting a BES reference document, NUC, and FAC standards. He also informed the SC that he expected the SCEC to convene prior to the May 2014 SC call to authorize the posting of PRC-005 and PRC-023.

M. Lauby also addressed the SC and said thank you for working so diligently on the various Standards activities. He also updated the SC that the new balloting system was being implemented, and that a team was working diligently to address any outstanding issues. M. Lauby ended by noting that a new Standards Developer would be joining NERC. The new developer is both an engineer and a lawyer.

Agenda Items

1. **Review of Agenda — (Approve)**

   -The Committee approved the motion with no objections or abstentions.

2. **Consent Agenda — (Approve)**

   -G.Zito motioned to approve the consent agenda. F. McElvain seconded the motion.

   -The Committee approved the motion with no objections or abstentions.

   a. March 12, 2014 Meeting Minutes*- **(Approve)**

   b. March 21, 2014 Meeting Minutes*- **(Approve)**

3. **Three-Month Outlook on Upcoming Standard Projects or Issues*— (Update)** M. Lauby announced that the outlook was updated and reflects some of the updates from the project plan and RSDP.

4. **Projects Under Development — (Review)**

   a. Project Tracking Spreadsheet

B. Hampton asked if the spreadsheet can track issues that are preventing projects from moving forward, or is this an item that the PMOS representative should bring forward. B. Murphy replied this information should be brought forward by PMOS representatives, and R. Parsons noted the PMOS representative should also highlight the positive attributes of the projects. B. Hampton then posed the general question of whether any PMOS representatives had anything to report. B. Murphy noted that CIP is moving forward with a projected posting date of early June 2014 and, as well, that the meetings he attended on TOP/IRO were going well. R. Crissman announced that COM-002 passed, and that standard will be going to the BOT in May 2014.

R. Crissman asked whether Project 2014-02 CIP Version 5 was back on schedule. S. Noess stated the project was back on track, and that the team is actively discussing the "identify, assess, and correct" language a lot. B. Murphy confirmed that the team was working on that issue, and that everyone is trying to assist with the project.

b. Projected Posting Schedule

B. Murphy commented that the updates on Mondays worked well. R. Crissman asked when the schedule was posted, and B. Nutter said that the schedule is updated typically by 10 a.m. Eastern. B. Murphy clarified that SC members should expect the posting on Tuesday if the Monday is a holiday.

5. **Project 2014-04 Initial Formal Comment and Ballot*- (Authorize)**

R. Crissman motioned to approve the agenda item as written. J. Sterling seconded the motion.

B. Murphy reminded everyone that FERC's ex parte rules have been invoked and this would be an appropriate time for non-approved Commission staff to step away. L. Oberski provided an overview of the drafting efforts. He explained that the 11 team members have been working diligently since the April 1, 2014 Technical Conference at which 130 stakeholders attended in person, while over 500 individuals attended via the phone and webinar. He went on to state the drafting team closely followed the FERC order, and the drafting team did not expand the scope of the project. He also said the drafting team was being responsive to all directives.

S. Noess also explained that the drafting team was very concerned about putting out a high quality standard, and the team had implemented several quality review processes. He went further to explain there was extensive input from NERC legal, in addition to other NERC departments. He anticipated posting the documents immediately, but the official ballot would run from April 10-24. 2014.

L. Oberski commended the work of the drafting team. He noted that FERC-designated staff member have been heavily involved in this project. F. McElvain complimented the team on the excellent product, but did recommend adding in sub-sections under Requirement R1. P. Brown stated the team did excellent work, but asked if the current draft was addressing FERC's concern on third party verifications. L. Oberski answered by stating the draft standard addresses this in two ways. The standard ensures the list of critical assets is correct and that there is an assessment of threat vulnerabilities. The drafting team had several

conversations around this topic, and that was the basis for Requirements R6.1 and R6.4. P. Brown then asked for clarification on whether the quality of the risk assessment mattered. L. Oberski answered the verifying party will serve a tradition auditing role. The verifying party will ensure the review took place and that the underlying assumptions are correct. F. Plett then asked how the confidentiality with regard to facilities will be maintained; he asked that it go further than CEII data. L. Oberski replied a procedure and plan will need to be in place to maintain such confidential data. S. Noess also explained that Compliance will have a counterpart in this process to maintain confidentiality. G. Kruempel asked if the RSAW would also be posted along with a timeline. L. Oberski and S. Noess confirmed both would be posted.

-The Committee approved the motion with no objections or abstentions.

Before moving to the next topic L. Oberski thanked the SC for the support and commented on the number of hours put into this effort. S. Noess added that the ballot body is growing, and he asked everyone to remember to vote so the ballot reaches a quorum. Further, he added that two webinars will be held in the following week. The details of both are listed on the project page.

J. Tarantino raised a concern that FERC may request more projects to be completed in 90 days. He asked if this project was setting a precedent. R. Crissman echoed his concern. L. Oberski stated that he does not recommend the same timeframe for future projects. B. Murphy announced that he would convey this concern to both NERC and FERC staff to assure 90 days does not become a normal timeframe for completing standards.

6. **Report on Assessing the Need to Introduce Demand Response Functions and Entities to the NERC Reliability Functional Model*- (Approve)**

F. Plett motioned to approve the agenda item as written. G. Zito seconded the motion.

J. Cyrulewski provided an update on the project, and introduced S. Knapp from the Functional Model Demand Response Action Team (FMDRAT). He also provided a background on this effort, and he explained that the report took a few years to complete. The Planning Committee took issue with some technical points, and both groups met to discuss the concerns. S. Knapp explained that since 2010, when the original report was drafted, technology has changed greatly, and FMDRAT concluded the penalties and markets out there today are enough to not require adding the entities to the Functional Model. Both groups agreed that there will be a time in the future where it is likely Demand Response (DR) providers should be added to the Functional Model. M. Lauby added that this is a very difficult project, and it is very hard for entities to plan down to their reserves. A. Gallo asked if markets and penalties apply to generators today. S. Knapp reiterated that there will be a time in the future to revisit adding DR to the Functional Model. A. Gallo if a threshold or a trigger has been established. S. Knapp said there is no threshold now, and DR does not currently comprise more than 20% of the market. J. Seelke and P. Heidrich added they believe this issue is something the technical committees should address in the future.

P. Heidrich asked whether there should be a concern if Reliability Standards were to be created for DR. He further added that he believed DR should be added to the Functional Model. J. Cyrulewski said that in that scenario it would have to come back the advisory group. S. Knapp acknowledged that there will eventually be a time when aggregators will likely need to be added to the Functional Model. J. Seelke asked who actually controls DR, and who will determine if DR providers have to be registered. F. Plett asked if there is a threshold trigger for another review of DR being added to the FM. J. Cyrulewski stated that would be an advisory group decision. B. Murphy called the item for a vote.

-The Committee approved the motion with no objections or abstentions.

7. **Subcommittee Reports**

   a. **No PMOS Update**

   b. **Process Subcommittee*— (Update)**

L. Lee provided a brief introduction, and explained there are several initiatives outlined in the supporting materials. L. Lee was leading the first item, and B. Li will discuss consensus building at a future meeting. She added that K. Porterfield has met with NERC staff to review QR goals. She also reported that J. Tarantino is currently working on a scope document to present shortly. Finally, she noted that E. Chanzes is drafting an announcement on the solicitation of committee members.

B. Murphy added that there is a RISC triage document that will be disseminated with the consensus building documents.

   i. **Resource Document Project, Action, and Status* – (Approve)**

E. Skiba (proxy for B. Li) motioned to approve the agenda item as written. A. Gallo seconded the motion.

-The Committee approved the motion with no objections or abstentions.

   ii. **Cost Effective Analysis Process (CEAP) Pilot Status and 2014 implementation* – (Endorse and Approve)**

F. Plett motioned to approve the agenda item as written. R. Crissman seconded the motion.

G. Zito explained that the pilot has concluded. B. Murphy asked if the pilot report has been shared. G. Zito responded that alternative approaches have been shared, and the results can be added to project pages. F. Gaffney commented that on page 8 of there was a paragraph he could not support because the paragraph implies that costs do not outweigh benefits. G. Zito explained this language was reviewed by individual not on a drafting team, and it was softened to show there were some inequities with regard to sufficient equipment. This language was crafted with RISC. F. Gaffney responded by questioning the quantifiable benefit for one installation and whether the SC should be justifying the standard based on cost. G. Zito explained there is room to transfer items to RISC. B. Murphy suggested discussing this item

on a separate call. S. Miller stated that CEAP is not an evaluation of the projects, and this is an endorsement of the methodology. F. Gaffney offered a friendly amendment to modify the paragraph that G. Zito was comfortable with. F. Plett and R. Crissman accepted the friendly amendment.

-The Committee approved the motion with the friendly amendment with no objections or abstentions.

iii. **Guidance Document for Management of Remanded Interpretations* – (Endorse)** (K. Smith)

G. Zito moved to approve the agenda item as written. R. Crissman seconded the motion.

K. Smith explained this project started with CIP and went on to provide an overview of the process for how remanded interpretations will be evaluated later. F. Gaffney opposed the requester having to decide whether a remand should move forward again. He suggested that the SC should be the appropriate action to determine any follow-up actions. K. Smith agreed to this, if NERC legal also supported this process change. S. Tyrewala stated she did not oppose making the change to the proposed process, but she did clarify the SC must make a new request if the standards have been remanded to have the project move forward in the Standards process. G. Zito and R. Crissman accepted F. Gaffney's friendly amendment.

-The Committee approved the motion with the friendly amendment with no objections or abstentions.

8. **Communication Updates and Activities* — (Update)**
9. **Upcoming Standards Filings* — (Review)**
10. **Informational Items — (Enclosed)**
    a. SC Expectations*
    b. 2014 Meeting Dates and Locations*
    c. 2014 Standards Committee Roster*
    d. Highlights of Parliamentary Procedure*
11. **Adjourn**

*Background materials included.

Standards Committee Meeting
April 9, 2014 Attendance List

Segment	Name	Company	Attendance
Chairman	Brian Murphy	NextEra Energy, Inc.	**X**
Vice Chairman	Scott Miller	MEAG Power	**X**
Segment 1-2013-14	**Lou Oberski**	**Dominion Resources Services, Inc.**	X
Segment 1-2014-15	**Laura Lee**	**Duke Energy**	X
Segment 2-2013-14	**Charles Yeung**	**Southwest Power Pool**	X
Segment 2-2013	**P.S. (Ben) Li** **Ed Skiba as proxy**	**Ben Li Associates, Inc.**	X
Segment 3-2013-14	**Jennifer Sterling**	**Exelon**	X
Segment 3-2014-15	**Ron Parsons**	**Alabama Power Company**	X
Segment 4-2013-14	**Joseph Tarantino**	**Sacramento Municipal Utility District**	X
Segment 4-2012-13	**Frank Gaffney**	**Florida Municipal Power Authority**	X
Segment 5-2013-14	**Gary Kruempel**	**MidAmerican Energy Company**	X
Segment 5-2013	**Randy Crissman**	**New York Power Authority**	X
Segment 6-2013-14	**Brenda Hampton**	**Energy Future Holdings – Luminant Energy Company LLC**	X
Segment 6-2013	**Andrew Gallo**	**City of Austin dba Austin Energy**	X
Segment 7-2013-14	**Michelle D'Antuono**	**Occidental Chemical**	X
Segment 7-2012-13	**Frank McElvain**	**Siemens Energy**	X
Segment 8-2013-14	**Robert Blohm**	**Keen Resources Asia Ltd.**	X
Segment 8-2012-13	**Fred Plett**	**Massachusetts Attorney General**	X
Segment 9-2014	**Klaus Lambeck**	**Public Utilities Commission of Ohio/the Ohio Power Siting Board**	X

Segment	Name	Company	Attendance
Segment 9-2014-15	Jason Woodruff Percy Lucban as proxy	Public Utilities Commission of Nevada	X
Segment 10-2013-14	Steve Rueckert	Western Electricity Coordinating Council	X
Segment 10-2014-15	Guy Zito	Northeast Power Coordinating Council	X
VP and Director of Standards	Mark Lauby	NERC	X
SC Secretary	Soo Jin Kim	NERC	X

A number of observers were also on the call.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Anticipated Standards Committee Actions

Brian Murphy, Standards Committee Chair
Mark Lauby, Vice President and Director, Standards
Standards Committee

RELIABILITY | ACCOUNTABILITY

Drafting Team Appointments

- May 2014
  - Project 2008-02- Undervoltage Load shedding expansion of the team to address UFLS

Authorize Posting

- May 2014:
  - Project 2014-03: Revisions to Transmission Operations/Interconnection Reliability Operations and Coordination Reliability Standards (TBD) (High)
  - Project 2008-02- Undervoltage Load shedding revised SAR to include UFLS

Authorize Posting

- June 2014:
  - Project 2013-03: GMD Stage 2 (45-day comment and initial ballot of 1 standard) (High)
  - Project 2009-03: Emergency Operations (45-day comment and initial ballot of 1 standard) (High)
  - Project 2008-02: Undervoltage Load shedding (45-day comment and initial ballot for PRC-010-1) (High)
  - Project 2010-05.2: Protection Systems (Special Protection Systems) (45-day comment and initial ballot of one revised definition) (Medium)
  - Project 2014-01: Standards Applicability for Dispersed Power Producing Resources (45-day comment and ballot of high-priority standards) (High)

Authorize Posting

- July 2014:
  - Project 2012-09: Implementation of Interconnection Reliability Operations and Coordination: Five-year Review (Medium)

Questions and Answers

Draft 2015-2017 Reliability Standards Development Plan and Enhanced Periodic Review

Action

1. Authorize the posting of the draft 2015-2017 Reliability Standards Development Plan (RSDP) for 30 days stakeholder comment. Concurrently, the Chair of the SC will present the draft 2015-2017 RSDP to the Reliability Issues Steering Committee (RISC) for its review and input on the Standard projects and prioritization. Thereafter, the Standards Committee Executive Committee (SECE) will work with NERC Staff on any changes to the draft 2015-2017 RSDP, based on stakeholder comments and RISC input, and, afterwards, present a final draft to the SC for approval.
2. Authorize the posting of draft Enhanced Periodic Review for 30 day stakeholder comment; Thereafter, the SECE will work with NERC Staff on any changes to the draft Enhanced Periodic Review, based on stakeholder comments and RISC input, and, afterwards, present a final draft to the SC for approval.

   It is intended that the documents related to Actions 1 and 2 (attached) would be posted at the same time, so stakeholders can consider their interrelationship.

Background

Draft 2015-2017 RSDP

The draft 2015-2017 RSDP continues the 2014-2016 RSDP progress towards Steady-State.[1] As can be viewed in the draft 2015-2017 RSDP, the number of active projects will dramatically decrease on or before the end of 2015, providing for the transition to a predominate format of enhanced periodic reviews (discussed next). The draft 2015-2017 appears to be a straightforward extension of the 2014-2016 RSDP, and was briefly reviewed by the Chair and Vice Chair of the SC prior to placing on the agenda. Given the apparent straightforward nature of the draft 2015-2017 RSDP, it is thought that it would be best to send out for stakeholder comment at this time, rather than assembling an SC task force to review prior to sending to stakeholders or otherwise delaying its posting.

Draft Enhanced Periodic Review

The below background was developed by the SCEC, Chairs of PMOS, SCPS and NERC Staff, and will also be used in the enhanced periodic review comment form to provide stakeholders with an overview of the enhanced periodic review.

At the February 6, 2014 Board of Trustees (Board) meeting, the Board requested that NERC management and the leadership of the SC work together to develop a mutually acceptable metric for 2015-2017, including a content and quality grading system for the Reliability Standards as part of the metric. Jointly, the following approach was developed, which was

[1] As stated in the 2014-2016 RSDP and 2014-2016 Standards Committee Strategic Work Plan, Steady State means a set of clear, concise, high quality and technically sound Reliability Standards that are results-based, while retiring requirements that do little to promote reliability.

endorsed by the SC on March 12, 2014, and, in summary form, adopted by Corporate Governance and Human Resources Subcommittee of the Board on March 20, 2014:

2014 and 2015 metric

The metric for 2014 and 2015 focuses on ensuring certain Reliability Standard projects are timely completed. For 2014, the Standard projects are all high priority Standard projects, many with regulatory deadlines.

2016 and 2017 metric

The implementation of an enhanced Reliability Standard periodic review for quality and content that takes into consideration the following issues: (1) folding the enhanced quality and content periodic review into the period review required by Section 13 of the Standards Processes Manual; (2) a quality and content review of the steady state Standards developed, considering the use of, or adaptation of, the 2013 Independent Expert Review Team's quality and content scoring system; (3) the formation of a cross-functional task force to conduct, periodic reviews of steady state Reliability Standards, potentially consisting of Committee chairs, NERC management, NERC and stakeholder subject matter experts (all task force meetings shall be open to the public); (4) the task force to use the quality and content system developed in response to 2), above, to identify needed enhancements to steady state standards for inclusion in a Standards Authorization Request (SAR) processed through the standards development process and completed within a year from the date of posting of the SAR, unless technical review and study is needed (To the extent possible, the inclusion of identified enhancements in a SAR shall be limited focusing enhancements rather than re-opening an entire Standard(s); and (5) the development of an annual task force review timeline starting with the cross-functional task force being operational no later than mid-2015, so it can identify which standards will undergo the enhanced period review for inclusion in the 2016-2018 Reliability Standards Development Plan.

The above summary of the metric approach shows a focus on the completion of transforming NERC's Reliability Standards to a steady state by the end of 2015,[2] and, thereafter, the initiation of an enhanced periodic review to address quality and content issues related to the steady state Reliability Standards. It is contemplated that approximately 25 percent of the steady state Reliability Standards will undergo the enhanced period review in 2016, and another 25 percent in 2017.

At its March meeting, the SC appointed a periodic review development team (consisting of the SC Executive Committee and the Project Management and Oversight and Process Subcommittees chairs) to work with NERC Staff and Legal to develop the attributes of the enhanced quality and content periodic review. This team developed an approach to address the Board's direction summarized below and set forth in the attached template, along with a stakeholder comment form. The approach has been preliminarily reviewed by the SC and

[2] Steady state as set forth in the 2014-2016 Reliability Standards Development Plan and 2014-2016 Standards Committee Strategic Work Plan is a set of clear, concise, high quality and technically sound Reliability Standards that are results-based, while retiring requirements that do little to promote reliability.

approved for posting for stakeholder comment. Based on stakeholder comments, the SC will consider if the proposed approach should be enhanced, prior to its endorsement and requesting NERC's Board consideration.

Summary of draft enhanced periodic review approach

- The enhanced periodic review approach will satisfy NERC's obligations under Section 13 of the Standard Processes Manual, and will be conducted in accordance with that section.
- The SC shall appoint a standing cross-functional team including NERC staff and the NERC standing committee representatives to work with the Section 13 *"review team of subject matter experts."* This team will be appointed by the SC, who will review and adopt the results of the team's deliberations.
- The cross-functional team shall be operational no later than beginning of 2015 making recommendations to the SC on the Reliability Standards that should undergo the enhanced periodic review in 2016-2018, and to be included 2016-2018 Reliability Standards Development Plan.
- NERC's five-year periodic review template that was successfully employed for number of standards in 2013 and 2014 has been revised and adapted to include quality and content questions developed by the Independent Expert Review Panel not already included. The template was further adapted to eliminate duplicative questions, and to provide the cross-functional review team with a clear framework to conduct the periodic reviews.
    - A new question was added to consider whether the applicability section or requirements can be revised for smaller entities, provided that there is technical justification to support the enhanced applicability.
    - A dashboard will be developed for each reviewed Standard indicating if whether it has a score of Green, Yellow or Red Green, according to the following grading system:
        - Green = no quality and content changes needed – Standard confirmed as steady state;
        - Yellow = quality and content issues identified, but those identified are not sufficient to justify revising Standard at this time – i.e., continue to monitor; and
        - Red = Standard needs to be revised to address identified quality and content issues.
- Standards graded as "Red" by the cross-functional review team will be revised consistent with applicable sections of the Standards Processes Manual.

Alternative

As an alternative to the proposed actions in 1 and 2, the Standards Committee could decide to review the draft documents for a period of time if there was a concern the documents are not ready for posting, and then convene a call to discuss and authorize the posting.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standards Development Plan

2015–2017

DRAFT April 29, 2014

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Table of Contents i
Executive Summary 2
Steady-State 4
Directives 4
Paragraph 81 Candidates and IERP Recommendations for Retirement 6
2014 Progress Report 8
2015 Projects 10
Projects continuing from 2014 10
New Projects for 2015 10
Sustainable Approach to Periodic Reviews 11
Appendix 1 – New Projects for 2015 14
Project 2015-01 TPL Directives 14
Project 2015-02 Periodic Review of EOP-004, EOP-005, EOP-006 and EOP-008 14
Project 2015-03 Periodic Review of System Operating Limit Standards (FAC-010, -011, and -014) 14
Project 2015-04 Alignment of Definitions in *Glossary of Terms used in NERC Reliability Standards* and NERC *Rules of Procedure*, Appendix 2 15

Executive Summary

The 2015-2017 Reliability Standards Development Plan (2015-2017 RSDP) is another bold step toward transforming the NERC Reliability Standards. During 2015, the NERC Reliability Standards will reach Steady-State[1] and the number of active projects will dramatically decrease. Concurrently, to begin the final transition in the transformation process, the industry-endorsed criteria for evaluating the content and quality of standards will be applied to standards or standard families during enhanced periodic reviews, focused on continuous improvement.

With the support from the Standards Committee and industry stakeholders, NERC Reliability Standards have made great strides over the last two years. By the end of 2015, the majority of the Paragraph 81 candidates,[2] the Independent Expert Review Panel's (IERP) recommendations for requirement retirement, and Federal Energy Regulatory Commission (FERC) directives issued prior to December 2012 will be addressed. Projects that were languishing for years, as well as five-year reviews will be completed. The industry will also have completed large projects to respond to FERC orders, including, for example, Geomagnetic Disturbances, CIP Version 5 Revisions, and CIP-014 Physical Security, revised the TOP and IRO standards to address concerns identified in FERC's proposed remand, and will have addressed the majority of FERC directives issued after December 2012. This is a significant achievement – the Standards Committee worked diligently with NERC to determine project schedules and manage industry workload. Stakeholders engaged throughout North America to provide expertise during standard development ensuring projects could reach completion.

Now, in the 2015-2017 RSDP, the number of projects necessary to reach Steady-State by 2015 is reduced and the pace of the work will likely become more deliberate. Six projects that began during 2014 will be completed in 2015, while four new projects will be initiated in 2015, with one focused on aligning the Glossary of Terms used in NERC Reliability Standards with the Definitions used in the Rules of Procedure (Rules of Procedure, Appendix 2). This reduction in planned projects provides a bandwidth for projects required to respond to emerging risks, if any, to reliability, establish a quality and content enhanced periodic review, as well as any new FERC orders or directives. Also, given the increased focus on quality during the standard development process as well as active engagement of FERC Office of Electric Reliability staff during the standards development process, FERC directives and orders on existing standards are expected to trend lower.

Arriving to Steady-State provides an opportunity for critical assessment of the existing reliability standards through enhanced periodic reviews, and following the reviews to implement recommendations for quality, content, or alignment with other standards using industry-developed criteria,[3] building on the foundation established by the IERP.[4] Over the last 7 years, the Electric Reliability Organization (ERO) and industry have gained experience in understanding the characteristics of quality, results-based standards, while targeting their applicability based on risk to achieve a reliability benefit without creating undue burden on industry.

---

[1] As stated in the 2014-2016 RSDP and 2014-2016 Standards Committee Strategic Work Plan, Steady State means a set of clear, concise, high quality and technically sound Reliability Standards that are results-based, while retiring requirements that do little to promote reliability.

[2] There are 6 P81 candidates that will be addressed during the enhanced periodic reviews.

[3] The Independent Experts developed criteria is described in their final report, Standards Independent Experts Review Project, however this criteria was not vetted with industry.

[4] The North American Electric Reliability Corporation (NERC) retained five industry experts to independently review the NERC Reliability Standards, setting the foundation for a plan that will result in a set of clear, concise and sustainable body of Reliability Standards. The primary scope was an assessment of the content and quality of the Reliability Standards, including identification of potential Bulk-Power System (BPS) risks that were not adequately mitigated.

The NERC model is unique in the realm of regulation and, with the participation by stakeholders, the Standards Committee, and applicable regulatory authorities, we are demonstrating that this regulatory model works.

Steady-State

The NERC Reliability Standards will reach Steady-State in 2015.

This section provides information on the status of FERC directives, Paragraph 81 candidates, and the IERP's recommendations for retirement. Completion of projects is discussed in the next section, "2014 Status Report."

Directives

In 2013, NERC set out to address the 191 FERC directives that were issued and unaddressed prior to December 2012:

	2012 Directives	2013/2014 Directives	Total
Issued prior to year-end 2012	191		
Issued in 2013/2014		46	
Resolved as of March 1, 2014	122	11	
Remaining	**69**	**35**	**104**
Projected to be resolved in 2014	45	29	74
Projected to be remaining at year-end 2014	**24**	**6**	**30**

*Does not include non-standards' related directives

Table 1. Completion of Directives

While this is one benchmark, it is also imperative to address the FERC directives issued post-December 2012 in a timely fashion. As noted in the footnote to the chart above, FERC issued some directives that require work from groups outside of standards, such as the NERC technical committees, or another internal NERC department, such as Reliability Assessment and Performance Analysis (RAPA). These directives, as they cannot be resolved through a Standards process, are not included in the above numbers.

As depicted in Chart 1, the majority of the 191 Directives (115 or 60%) were addressed in 2013. Depending upon project completion, 171 will be addressed at yearend 2014.

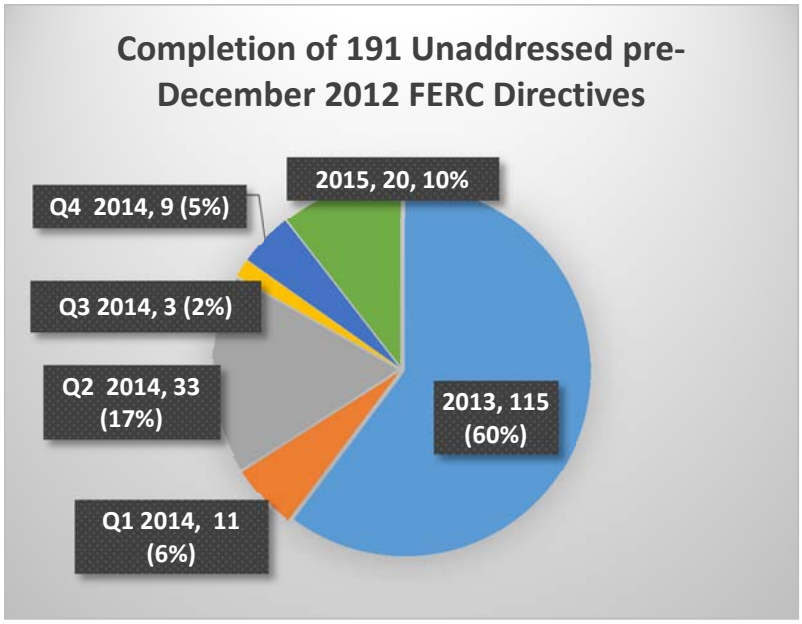


Chart 1. Completion of 191 Directives

FERC has issued 55 directives since December 2012. Nine of those pertain to areas outside of standards. Eleven have been addressed. Of the remaining 35, 29 are projected to be addressed in 2014 and 6 in 2015, as shown in Chart 3.

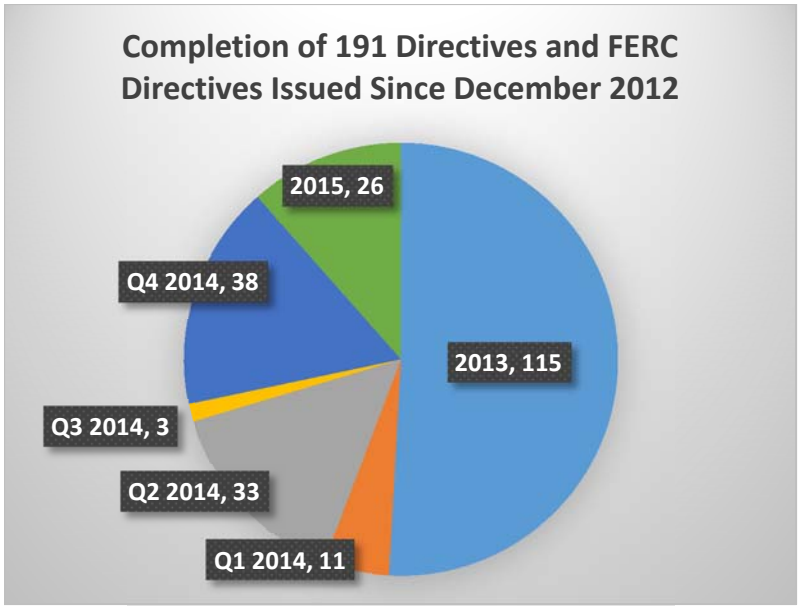


Chart 3. Completion of Remaining Directives

Paragraph 81 Candidates and IERP Recommendations for Retirement

The Paragraph 81 (or P81) project was initiated in response to paragraph 81 of FERC's March 15, 2012 Order.[5,6] Candidate requirements in a Phase 1 of the project were approved by FERC in Order 788, issued on November 21, 2013.[7] In addition to candidates requirements filed in Phase 1, stakeholders identified 217 additional candidates for consideration. These candidates were addressed through standard development projects for each standard rather than in one project for efficiency. Further, the IERP recommended 147 candidates for retirement.[8]

There was some overlap in the 217 candidate requirements identified as part of the Paragraph 81 project, and the 147 recommended for retirement by the IERP. When combined, a total of 281 unique requirements were identified and have been or are projected for standard development team consideration as follows:

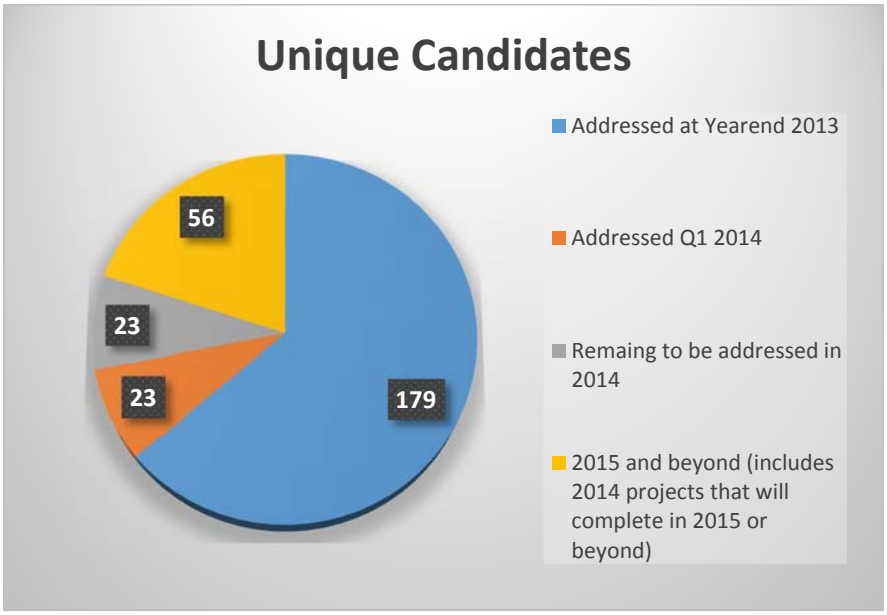


Chart 4. Candidates Unique for P81 and IERP

[5] 138 FERC 61,193, Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing, March 15, 2012.

[6] Id., p. 81:

> …The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently.

[7] FERC Order No. 788, 145 FERC 61,147, Electric Reliability Organization Proposal to Retire Requirements in Reliability Standards, November 21, 2013.

[8] See Appendix E of the Independent Experts Review Project.

Resolution

Recommendations for retirement are tracked at the requirement level. If the entire requirement was recommended for retirement, drafting teams may have considered one action (or part of a requirement) suitable for retirement, but determined that another action within a requirement should be retained. In conducting the analysis to determine whether the drafting team followed a recommendation for retirement, if the intent of the recommendation was met or if the majority of the requirement was retired, this analysis considers the recommendation addressed. With those considerations, the status of the resolution for 179 candidates addressed as of the second quarter of 2014 is:

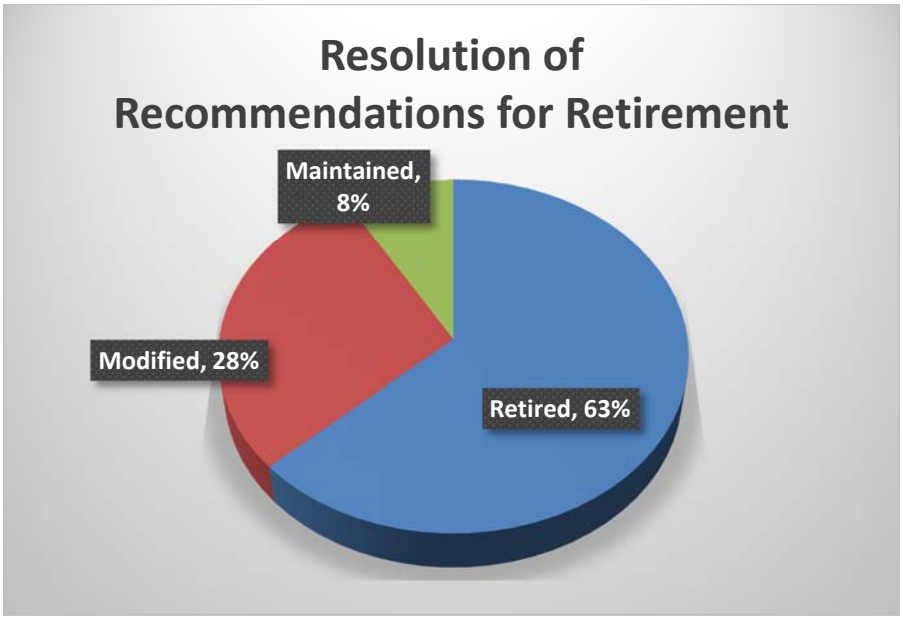


Chart 5. Resolution of Recommendation for Retirement

2014 Progress Report

The 2014-2016 RSDP identified 13 active projects to be conducted over the three-year period, of which 8 are projected to be completed by yearend 2014. There are 10 additional projects that have continued development from the 2013-2015 RSDP, all of which are scheduled to be completed in 2014. Finally, there are 4 projects that were initiated in 2014 as a result of a reliability need or to respond to a FERC order or directive.

Projects that were listed in the 2014–2016 RSDP that are scheduled to be completed in 2014:

- Project 2008-02 Undervoltage Load Shedding and Underfrequency Load Shedding
- Project 2007-11 Disturbance Monitoring
- Project 2009-02 Real-Time Reliability Monitoring and Analysis Capabilities (consolidated into Project 2014-03 TOP/IRO Revisions)[9]
- Project 2009-03 Emergency Operations
- Project 2010-02 Connecting New Facilities to the Grid
- Project 2010-05.2 Phase 2 of Protection System Misoperations: SPS/RAS
- Project 2010-08 Functional Model Glossary Revisions
- Project 2010-14.2 Periodic Review and Revisions of BAL-004, -005, and -006
- Project 2012-09 Implementation of IRO Five-year Review Recommendations
- Project 2012-13 NUC Review and Implementation
- Project 2013-03 Geomagnetic Disturbance Mitigation Measures (Stage 2)

Two projects were listed as pending technical committee input and initiated in the first quarter of 2014:

- Project 2007-17.3 Protection System Maintenance and Testing Auxiliary Relays
- Project 2010-13.3 Generator Relay Loadability Stable Power Swings

The following projects are 2013 projects that were (or are anticipated to be) completed in 2014, and all have been completed or are scheduled to be completed by the end of 2014:

- Project 2007-02 Operating Personnel Communications Protocol
- Project 2007-06 System Protection Coordination
- Project 2008-12 Coordinate Interchange Standards
- Project 2010-01 Operations Personnel Training
- Project 2010-03 Modeling Data – MOD B
- Project 2010-04 Demand Data – MOD C
- Project 2010-05.1 Phase 1 of Protection Systems: Misoperations
- Project 2010-14.1 Phase 1 of Balancing Authority Reliability-Based Control: Reserves
- Project 2012-05 ATC Revisions – MOD A
- Project 2013-04 Voltage and Reactive Control

The following projects were identified as either an emerging issue or developed in response to a FERC order or directive:

- Project 2014-02 CIP Version 5 Revisions

[9] The issues and directives assigned to Project 2009-02 are being addressed in Project 2014-03 Revisions to TOP/IRO Reliability Standards, which has a filing deadline of January 31, 2015, subject to the outcome of balloting in that project.

- Project 2014-01 Standards Applicability for Dispersed Generation Resources
- Project 2014-03 Revisions to TOP/IRO Standards
- Project 2014-04 Physical Security

Of the above projects, all are on track to be completed in 2014, except several projects that were either withdrawn or have a longer timeline due to 1) coordination with other projects, or 2) a significant overlap in drafting team membership with projects being completed in 2013.

- Project 2010-08 Functional Model Glossary Revisions - withdrawn because it was determined that the project was not needed for reliability.
- Project 2012-09 Implementation of IRO Review - put on hold to facilitate coordination with Project 2014-03 Revisions to TOP and IRO Reliability Standards.
- Project 2008-02 Undervoltage Load Shedding and Underfrequency Load Shedding - being coordinated with Project 2009-03 Emergency Operations and the definition of Special Protection System being revised in Project 2010-05.2 Phase 2 of Protection System Misoperations: SPS/RAS
- Project 2009-03 Emergency Operations - being coordinated with Project 2008-02 Undervoltage Load Shedding and Underfrequency Load Shedding, which is being coordinated with the definition of Special Protection Systems.
- Project 2010-05.2 Phase 2 of Protection System Misoperations: SPS/RAS - being coordinated with Project 2008-02 Undervoltage Load Shedding and Underfrequency Load Shedding.
- Project 2010-14.2 Phase 2 of BAL-004, -005, and -006 – a periodic review of the three standards in this project was delayed because of significant drafting team membership overlap with other BAL projects that were not completed as soon as anticipated.

2015 Projects

As discussed in the prior section, there are 6 projects that were in progess in 2014 that are projected to continue into 2015. Three of these projects, Project 2008-02 Undervoltage Load Shedding and Underfrequency Load Shedding, Project 2009-03 Emergency Operations, and Project 2010-14.2 Revisions of BAL-004, BAL-005 and BAL-006, may complete in 2014, reducing the number of projects continuing to 2.

Two of the projects that are identified below as new are directly related to resolving remaining FERC Directives, one is to complete the review of the FAC standards from the 2013 periodic reviews, and the remaining project is being conducted to align the Glossary of Terms used in the NERC Reliability Standards and the Definitions used in the Rules of Procedure. The project to complete the FAC standards review may be included with the 2015 Periodic Review.

Additionally, the IERP identified three high level gaps that were reviewed by the NERC Operating Committee in 2014. It is anticipated that two of the issues, Outage Coordination and Situational Awareness, will be addressed by the TOP/IRO Revisions project. Depending upon the outcome of that project, additional work may be necessary. The third issue, Governor Frequency Response, was determined by the Operating Committee as a potential area of concern, but one that is being monitored. Depending upon the findings of the Operating Committee on this issue, more work may be necessary for this concern as well.

Projects continuing from 2014 into 2015

As stated above, the following projects will continue from 2014:

- Project 2012-09 Implementation of IRO Review (on hold pending completion of the TOP/IRO Revisions)
- Project 2008-02 Undervoltage Load Shedding and Underfrequency Load Shedding
- Project 2009-03 Emergency Operations
- Project 2010-05.2 Phase 2 of Protection System Misoperations: SPS/RAS
- Project 2010-14.2 Phase 2 of BAL-004, BAL-005, and BAL-006

New Projects for 2015[10]

To achieve Steady-State, the following projects will be initiated in 2015. The EOP and FAC periodic review projects planned for initiation in 2015 complete reviews that were deferred by review teams in 2013, either due to interdependencies with standards that were pending regulatory approval, or to gain compliance experience prior to conducting the review.

Consistent with the approach applied to prioritize projects in the 2014-2014 RSDP and used by the SC for new projects such as Project 2014-01 Standards Applicability for Dispersed Generation Resources, new projects for 2015 have been assigned a prioritization of High, Medium, Low, or Pending Technical Committee input. Specific elements considered in prioritization include: (1) RISC Category Rankings; (2) regulatory directives; (3) regulatory deadlines; (4) Reliability Standard requirement candidates for retirement; (5) the IERP content and quality assessments; and (6) additional considerations (fill-in-the-blank status and five-year assessment commitments). The prioritization gave primary consideration to RISC Category Rankings, regulatory directives, and regulatory deadlines, which was further informed by the other prioritization elements. Based on the application of these

[10] See Appendix 1 for new project detail.

elements, this section prioritizes each Reliability Standard project as High, Medium, Low, or Pending Technical Committee input.

The prioritization in this RSDP does not include projects in progress at yearend 2014, since those projects have been previously prioritized.

Prioritization Considerations for 2015 Projects:

Medium Priority

- Project 2015-01 TPL Directives (prioritized by SC in 2014)
  - 2 FERC directives
  - RISC: high priority area
  - IERP considerations: minor quality and content
- Project 2015-02 Periodic Review of EOP-004, EOP-005, EOP-006 and EOP-008
  - 1 FERC directive
  - RISC: high priority area
  - IERP considerations: some content and some quality
  - 3 Paragraph 81 Candidates
- Project 2015-03 Periodic Review of System Operating Limit Standards (FAC-010, -011, and -014)
  - RISC: low priority area
  - IERP: content and quality issues
  - 2 Paragraph 81 candidates

Low Priority

- Project 2015-04 Alignment of Glossary of Terms used in NERC Reliability Standards and the Definitions used in the Rules of Procedure (Rules of Procedure Appendix 2)

Sustainable Approach to Periodic Reviews[11]

At the February 6, 2014 Board of Trustees (Board) meeting, the Board requested that NERC management and the leadership of the Standards Committee (SC) work together to develop a mutually acceptable metric for 2015-2017, including a content and quality grading system for the Reliability Standards as part of the metric. Jointly, the following approach was developed, which was endorsed by the SC on March 12, 2014 and, in summary form, adopted by Corporate Governance and Human Resources Subcommittee of the Board on March 20, 2014.

2014 and 2015 Metric

The metric for 2014 and 2015 focuses on ensuring certain Reliability Standard projects are timely completed. For 2014, the Standard projects are all high priority Standard projects, many with regulatory deadlines.

2016 and 2017 metric

[11] During 2014 this framework is being presented for stakeholder comment, and then Board approval, so the final framework may differ in some respects to the approach outlined here.

> The implementation of an enhanced Reliability Standard periodic review for quality and content that takes into consideration the following issues: (1) folding the enhanced quality and content periodic review into the period review required by Section 13 of the Standards Processes Manual; (2) a quality and content review of the steady state Standards developed, considering the use of, or adaptation of, the 2013 Independent Expert Review Team's quality and content scoring system; (3) the formation of a cross-functional task force to conduct, periodic reviews of steady state Reliability Standards, potentially consisting of Committee chairs, NERC management, NERC and stakeholder subject matter experts (all task force meetings shall be open to the public); (4) the task force to use the quality and content system developed in response to 2), above, to identify needed enhancements to steady state standards for inclusion in a Standards Authorization Request (SAR) processed through the standards development process and completed within a year from the date of posting of the SAR, unless technical review and study is needed (to the extent possible, the inclusion of identified enhancements in a SAR shall be limited to focusing enhancements rather than re-opening an entire Standard(s)); and (5) the development of an annual task force review timeline starting with the cross-functional task force being operational no later than mid-2015, so it can identify which standards will undergo the enhanced period review for inclusion in the 2016-2018 Reliability Standards Development Plan.

The above summary of the metric approach shows a focus on the completion of transforming NERC's Reliability Standards to a steady state by the end of 2015[12] and, thereafter, the initiation of an enhanced periodic review to address quality and content issues related to the steady state Reliability Standards. It is contemplated that approximately 25 percent of the steady state Reliability Standards will undergo the enhanced period review in 2016, and another 25 percent in 2017.

At its March 2014 meeting, the SC appointed a periodic review development team (consisting of the SC Executive Committee and the Project Management and Oversight and Process Subcommittees chairs) to work with NERC Staff and Legal to develop the attributes of the enhanced quality and content periodic review. This team developed an approach to address the Board's direction, as summarized below.

Summary of draft enhanced periodic review approach

- The enhanced periodic review approach will satisfy NERC's obligations under Section 13 of the *Standard Processes Manual*, and will be conducted in accordance with that section.

- The SC shall appoint a standing cross-functional team including NERC staff and the NERC standing committee representatives to work with the Section 13 *"review team of subject matter experts."* This team will be appointed by the SC, who will review and adopt the results of the team's deliberations.

- The cross-functional team shall be operational no later than beginning of 2015 making recommendations to the SC on the Reliability Standards that should undergo the enhanced periodic review in 2016-2018, and to be included 2016-2018 Reliability Standards Development Plan.

- NERC's five-year periodic review template that was successfully employed for number of standards in 2013 and 2014 has been revised and adapted to include quality and content questions developed by the

[12] Steady state as set forth in the 2014-2016 Reliability Standards Development Plan and 2014-2016 Standards Committee Strategic Work Plan is a set of clear, concise, high quality and technically sound Reliability Standards that are results-based, while retiring requirements that do little to promote reliability.

Independent Expert Review Panel not already included. The template was further adapted to eliminate duplicative questions, and to provide the cross-functional review team with a clear framework to conduct the periodic reviews. A new question was added to consider whether the applicability section or requirements can be revised for smaller entities, provided that there is technical justification to support tailoring the applicability.

- A dashboard will be developed for each reviewed Standard indicating whether it has a score of Green, Yellow, or Red, according to the following grading system:
  - Green = no quality and content changes needed – Standard confirmed as steady state;
  - Yellow = quality and content issues identified, but those identified are not sufficient to justify revising Standard at this time – i.e., continue to monitor; and
  - Red = Standard needs to be revised to address identified quality and content issues.

- Standards graded as "Red" by the cross-functional review team will be revised consistent with applicable sections of the Standards Processes Manual.

In 2015, the cross-functional Review Team appointed by the Standards Committee will prioritize families or groups of standards for review in 2015 and beyond. As resources permit, reviews of standards may begin in 2015.

Appendix 1 – New Projects for 2015

Project 2015-01 TPL Directives

Total: 2

This project will address two directives and consider other improvements to TPL-001-4 -- Transmission System Planning Performance Requirements.

Order 678:

- Para 40 - Direct NERC to modify Reliability Standard TPL-001-4 to address the concern that the six month threshold could exclude planned maintenance outages of significant facilities from future planning assessments.
- Para 89 - Directs NERC to consider a similar spare equipment strategy for stability analysis upon the next review cycle of Reliability Standard TPL-001-4.

Project 2015-02 Periodic Review of EOP-004, EOP-005, EOP-006 and EOP-008

Total: 1

This periodic review project will review four EOP standards for which the review was delayed to allow the ERO and industry to gain compliance experience with revisions to the standards that became enforceable in 2013 and early 2014. The review team will also consider one directive and, as part of its recommendation on EOP-006, recommend whether a guideline should be developed.

Order 749:

- Para 24 - (EOP-006) once the standard is effective, if industry determines that ambiguity with the term arises, it would be appropriate for NERC to consider its proposal to develop a guideline to aid entities in their compliance obligations.

Project 2015-03 Periodic Review of System Operating Limit Standards (FAC-010, -011, and -014)

Total: 0

The three NERC Standards in this periodic review project concern methodologies for determining and communicating System Operating Limits. In 2013, a five-year review team (FYRT) assigned to review the FAC family of standards recommended review of these three standards be delayed until shortly after approval of the TPL, TOP, and IRO standards, which were pending regulatory approval at the time of the FAC five-year review. TPL-001-4 was approved by FERC in October 2013; the TOP and IRO standards are being revised in 2014 for filing with applicable regulators in early 2015.

Project 2015-04 Alignment of Definitions in *Glossary of Terms used in NERC Reliability Standards* and NERC *Rules of Procedure*, Appendix 2

Total: 0

This project will review the NERC *Glossary of Terms Used in Reliability Standards* (Glossary) to determine what changes are necessary to align the Glossary definitions with definitions of the same terms used in the NERC Rules of Procedure, Appendix 2.

Periodic Review Template: [Insert Standard Number/Name]
Updated April, 2014

Introduction

The North American Electric Reliability Corporation (NERC) is required to conduct a periodic review of each NERC Reliability Standard at least once every ten years, or once every five years for Reliability Standards approved by the American National Standards Institute as an American National Standard.[1] The Reliability Standard identified below has been included in the current cycle of periodic reviews. The Review Team shall consist of two subgroups, a standing review team which is appointed annually by the Standards Committee for periodic reviews, and a stakeholder SME team, solicited and appointed by the Standards Committee for expertise specific to the standards being reviewed. The standing review team will be comprised of the chairs of the Standards Committee, (Operating Committee and Planning Committee for non CIP-Standards and CIPC for CIP cyber security Standards), NERC management of Standards and RAPA, and NERC SMEs familiar with the Standard(s) to be reviewed. Together, the standing review team and SME stakeholder team is the Review Team for a particular periodic review project.

The Review Team will use the background information and the questions below, along with any associated worksheets or reference documents, to guide a comprehensive review that results in a recommendation from one of the following three choices:

1. Recommend reaffirming the Standard as steady state (Green); or
2. Recommend that the standard could be revised, but revisions are not necessary for reliability (Yellow); or
3. Recommend that the standard needs revision or retirement (Red).,

If the team recommends a revision to or a retirement of the Reliability Standard, it must also submit a Standard Authorization Request (SAR) outlining the proposed scope and technical justification for the revision or retirement.

A completed Periodic Review Template and any associated documentation should be submitted by email to [insert NERC contact for project].

[1] NERC Standard Processes Manual 45 (2013), posted at http://www.nerc.com/pa/Stand/Documents/Appendix_3A_StandardsProcessesManual.pdf.

Applicable Reliability Standard: standard and version
Team Members (include name and organization): 1. name, Company 2. name (Standard Developer)
Date Review Completed:

Background Information *(to be completed initially by NERC staff)*

1. Are there any outstanding Federal Energy Regulatory Commission (FERC) directives associated with the Reliability Standard? (*If so, NERC staff will attach a list of the directives with citations to associated FERC orders for inclusion in a SAR.)*

   ☐ Yes

   ☐ No

2. Have stakeholders requested clarity on the Reliability Standard in the form of an Interpretation (outstanding, in progress, or approved) or Compliance Application Notice (CAN) (outstanding, in progress, or approved)? (*If there are, NERC staff will include a list of the Interpretation(s), CAN(s), or other stakeholder-identified issue(s) that apply to the Reliability Standard*.)

   ☐ Yes

   ☐ No

   Please explain:

3. Is the Reliability Standard one of the most violated Reliability Standards? If so, does the cause of the frequent violation appear to be a lack of clarity in the language?

   ☐ Yes

   ☐ No

   Please explain:

Questions for the Review Team

If NERC staff answered "Yes" to any of the questions above, the Reliability Standard probably requires revision. The questions below are intended to further guide your review. Some of the questions reference documents provided by NERC staff as indicated in the Background questions above.

I. Quality

1. **Reliability Need, Paragraph 81:** Does one or more of the requirements in the Reliability Standard meet criteria for retirement or modification based on Paragraph 81 concepts? *Use Attachment 2: Paragraph 81 Criteria to make this determination.*

   ☐ Yes

   ☐ No

   Please summarize your application of Paragraph 81 Criteria, if any:

2. **Clarity:** From Background Information section of this template, has the Reliability Standard been the subject of an Interpretation, CAN, or issue associated with it, or is frequently violated because of ambiguity?
   a. Does the Reliability Standard have obviously ambiguous language?
   b. Does the Reliability Standards have language that requires performance that is not measurable?
   c. Are the requirements consistent with the purpose of the Reliability Standard?
   d. Does the requirement align with the purpose?
   e. Should the requirement stand alone as is or should it be consolidated with other standards?
   f. Is it complete and self-contained?
   g. Does it use consistent terminology?

   ☐ Yes

   ☐ No

   Please summarize your assessment:

3. **Definitions**: Do any of the defined terms used within the Reliability Standard need to be refined?

   ☐ Yes

   ☐ No

   Please explain:

4. **Compliance Elements:** Are the compliance elements associated with the requirements (Measures, Data Retention, Violation Risk Factors (VRF), and Violation Severity Levels (VSL)) consistent with the direction of the Reliability Assurance Initiative and FERC and NERC guidelines?

   ☐ Yes

   ☐ No

   If you answered "No," please identify which elements require revision, and why:

5. **Consistency with Other Reliability Standards:** Does the Reliability Standard need to be revised for formatting and language consistency among requirements within the Reliability Standard or consistency with other Reliability Standards?

   ☐ Yes

   ☐ No

   If you answered "Yes," please describe the changes needed to achieve formatting and language consistency:

6. **Changes in Technology, System Conditions, or other Factors:** Does the Reliability Standard need to be revised to account for changes in technology, system conditions, or other factors?

   ☐ Yes

   ☐ No

   If you answered "Yes," please describe the changes and specifically what the potential impact is to reliability if the Reliability Standard is not revised:

7. **Practicable**:
   a. Can the Reliability Standard be practically implemented?

      ☐ Yes

      ☐ No

   b. Is there a concern that it is not cost effective as drafted?

      ☐ Yes

      ☐ No

   Please summarize your assessment of the practicability of the standard:

8. **Consideration of Generator Interconnection Facilities:** Is responsibility for generator interconnection Facilities appropriately accounted for in the Reliability Standard?

   ☐ Yes

   ☐ No

   Guiding Questions:

   a. If the Reliability Standard is applicable to GOs/GOPs, is there any ambiguity about the inclusion of generator interconnection Facilities? (If generation interconnection Facilities could be perceived to be excluded, specific language referencing the Facilities should be introduced in the Reliability Standard.)

   b. If the Reliability Standard is not applicable to GOs/GOPs, is there a reliability-related need for treating generator interconnection Facilities as transmission lines for the purposes of this Reliability Standard? (If so, GOs and GOPs that own or operate relevant generator interconnection Facilities should be explicit in the applicability section of the Reliability Standard.)

9. **Results Based Standard:** Is the Reliability Standards drafted as a results-based standard (RBS) requirement (performance, risk (prevention) or capability) and does it follow the RBS format (e.g., sub-requirement structure? (*See Attachment 1: Results-based Standards*)

   ☐ Yes

   ☐ No

   If not, please summarize your assessment:

II. Content

10. **Technical accuracy:** Is the content of the Requirements technically correct, including identifying who does what and when?

    ☐ Yes

    ☐ No

    If not, please summarize your assessment:

11. **Functional Model:** Are the correct functional entities assigned to perform the requirements, consistent with the Functional Model?

    ☐ Yes

    ☐ No

    If not, please summarize your assessment:

12. **Applicability:** Is there a technical justification for revising the applicability of the Reliability Standard, or specific requirements within the standard, to account for differences in reliability risk?

    ☐ Yes

    ☐ No

    If so, please summarize your assessment:

13. **Reliability Gaps:** Are the appropriate actions, for which there should be accountability, included or is there a gap?

    ☐ Yes

    ☐ No

    If a gap is identified, please explain:

14. **Technical Quality:** Does the Reliability Standard have a technical basis in engineering and operations?

    ☐ Yes

    ☐ No

    If not, please summarize your assessment:

15. **Does the Reliability Standard reflect a higher solution than the lowest common denominator?**

    ☐ Yes

    ☐ No

    If not, please summarize your assessment:

RED, YELLOW GREEN GRADING

Using the questions above, the Review Team shall come to a consensus on whether the Standard is Green – i.e., affirm as steady state; Yellow – could be improved, but there is not a sufficient technical, content or quality issues to require revision at this time or Red but not necessary or Red – needs revision and thus a SAR should be developed to process the Standard through the Standards development process for revision. The reasons for the cross functional team conclusions of Green, Yellow, or Red shall be documented. If a consensus is not reached within the Review Team, minority reviews shall be posted for stakeholder comment, along with the majority opinion on whether the Standard is Green, Yellow or Red.

Recommendation

The answers to the questions above, along with its Red, Yellow, Green grading and the recommendation of the Review Team, will be posted for a 45-day comment period, and the comments publicly posted. The Review Team will review the comments to evaluate whether to modify its initial recommendation, and will document the final recommendation which will be presented to the Standards Committee.

Preliminary Recommendation (to be completed by the Review Team after its review and prior to posting the results of the review for industry comment):

- ☐ REAFFIRM (GREEN)
- ☐ REVISE (Indicate whether the revisions are necessary to support reliability (YELLOW), or discretionary (RED))
- ☐ RETIRE (RED)

Technical Justification *(If the Review Team recommends that the Reliability Standard be revised, a draft SAR may be included and the technical justification included in the SAR)*:

Preliminary Recommendation posted for industry comment (date):

Final Recommendation (to be completed by the Review Team after it has reviewed industry comments on the preliminary recommendation):

☐ REAFFIRM *(This should only be checked if there are no outstanding directives, interpretations or issues identified by stakeholders.) GREEN*

☐ REVISE RED

☐ RETIRE RED

Technical Justification *(If the Review Team recommends that the Reliability Standard be revised, a draft SAR may be included and the technical justification included in the SAR)*:

Date submitted to Standards Committee:

Attachment 1: Results-Based Standards

Question 9 for the Review Team asks if the Reliability Standard is results-based. The information below will be used by the Review Team in making this determination.

Transitioning the current body of standards into a clear, concise, and effective body will require a comprehensive application of the RBS concept. RBS concepts employ a defense-in-depth strategy for Reliability Standards development where each requirement has a role in preventing system failures, and the roles are complementary and reinforcing. Reliability Standards should be viewed as a portfolio of requirements designed to achieve an overall defense-in-depth strategy and comply with the quality objectives identified in the resource document titled, "Acceptance Criteria of a Reliability Standard."

Accordingly, the Review Team shall consider whether the Reliability Standard contains results-based requirements with sufficient clarity to hold entities accountable without being overly prescriptive as to how a specific reliability outcome is to be achieved. The RBS concept, properly applied, addresses the clarity and effectiveness aspects of a standard.

A Reliability Standard that adheres to the RBS format should strive to achieve a portfolio of performance-, risk-, and competency-based mandatory reliability requirements that support an effective defense-in-depth strategy. Each requirement should identify a clear and measurable expected outcome, such as: a) a stated level of reliability performance, b) a reduction in a specified reliability risk, or c) a necessary competency.

a. **Performance-Based**—defines a particular reliability objective or outcome to be achieved. In its simplest form, a results-based requirement has four components: who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome?

b. **Risk-Based**—preventive requirements to reduce the risks of failure to acceptable tolerance levels. A risk-based reliability requirement should be framed as: who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome that reduces a stated risk to the reliability of the bulk power system?

c. **Competency-Based**—defines a minimum set of capabilities an entity needs to have to demonstrate it is able to perform its designated reliability functions. A competency-based reliability requirement should be framed as: who, under what conditions (if any), shall have what capability, to achieve what particular result or outcome to perform an action to achieve a result or outcome or to reduce a risk to the reliability of the bulk power system?

Additionally, each RBS-adherent Reliability Standard should enable or support one or more of the eight reliability principles listed below. Each Reliability Standard should also be consistent with all of the reliability principles.

1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.

5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected bulk power systems.

6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

7. The reliability of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.

8. Bulk power systems shall be protected from malicious physical or cyber attacks.

If the Reliability Standard does not provide for a portfolio of performance-, risk-, and competency-based requirements or consistency with NERC's reliability principles, NERC staff and the Review Team should recommend that the Reliability Standard be revised or reformatted in accordance with the RBS format.

Attachment 2: Paragraph 81 Criteria

The first question for the Review Team asks if one or more of the requirements in the Reliability Standard meet(s) criteria for retirement or modification based on Paragraph 81 concepts.[2] Use the Paragraph 81 criteria explained below to make this determination. Document the justification for the decisions throughout and provide them in the final assessment in the Periodic Review Template.

For a Reliability Standard requirement to be proposed for retirement or modification based on Paragraph 81 concepts, it must satisfy **both**: (i) Criterion A (the overarching criterion); and (ii) at least one of the Criteria B listed below (identifying criteria). In addition, for each Reliability Standard requirement proposed for retirement or modification, the data and reference points set forth below in Criteria C should be considered for making a more informed decision.

Criterion A (Overarching Criterion)

The Reliability Standard requirement requires responsible entities ("entities") to conduct an activity or task that does little, if anything, to benefit or protect the reliable operation of the BES.

Section 215(a) (4) of the United States Federal Power Act defines "reliable operation" as: "… operating the elements of the bulk power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

Criteria B (Identifying Criteria)

B1. Administrative

The Reliability Standard requirement requires responsible entities to perform a function that is administrative in nature, does not support reliability and is needlessly burdensome.

This criterion is designed to identify requirements that can be retired or modified with little effect on reliability and whose retirement or modification will result in an increase in the efficiency of the ERO compliance program. Administrative functions may include a task that is related to developing procedures or plans, such as establishing communication contacts. Thus, for certain requirements, Criterion B1 is closely related to Criteria B2, B3 and B4. Strictly administrative functions do not inherently negatively impact reliability directly and, where possible, should be eliminated or modified for purposes of efficiency and to allow the ERO and entities to appropriately allocate resources.

[2] In most cases, satisfaction of the Paragraph 81 criteria will result in the retirement of a requirement. In some cases, however, there may be a way to modify a requirement so that it no longer satisfies Paragraph 81 criteria. Recognizing that, this document refers to both options.

B2. Data Collection/Data Retention
These are requirements that obligate responsible entities to produce and retain data which document prior events or activities, and should be collected via some other method under NERC's rules and processes.

This criterion is designed to identify requirements that can be retired or modified with little effect on reliability. The collection and/or retention of data do not necessarily have a reliability benefit and yet are often required to demonstrate compliance. Where data collection and/or data retention is unnecessary for reliability purposes, such requirements should be retired or modified in order to increase the efficiency of the ERO compliance program.

B3. Documentation
The Reliability Standard requirement requires responsible entities to develop a document (*e.g.,* plan, policy or procedure) which is not necessary to protect reliability of the bulk power system.

This criterion is designed to identify requirements that require the development of a document that is unrelated to reliability or has no performance or results-based function. In other words, the document is required, but no execution of a reliability activity or task is associated with or required by the document.

B4. Reporting
The Reliability Standard requirement obligates responsible entities to report to a Regional Entity, NERC or another party or entity. These are requirements that obligate responsible entities to report to a Regional Entity on activities which have no discernible impact on promoting the reliable operation of the BES and if the entity failed to meet this requirement there would be little reliability impact.

B5. Periodic Updates
The Reliability Standard requirement requires responsible entities to periodically update (*e.g.,* annually) documentation, such as a plan, procedure or policy without an operational benefit to reliability.

This criterion is designed to identify requirements that impose an updating requirement that is out of sync with the actual operations of the BES, unnecessary, or duplicative.

B6. Commercial or Business Practice
The Reliability Standard requirement is a commercial or business practice, or implicates commercial rather than reliability issues.

This criterion is designed to identify those requirements that require: (i) implementing a best or outdated business practice or (ii) implicating the exchange of or debate on commercially sensitive information while doing little, if anything, to promote the reliable operation of the BES.

B7. Redundant
The Reliability Standard requirement is redundant with: (i) another FERC-approved Reliability Standard requirement(s); (ii) the ERO compliance and monitoring program; or (iii) a governmental regulation (*e.g.,* Open Access Transmission Tariff, North American Energy Standards Board ("NAESB"), etc.).

This criterion is designed to identify requirements that are redundant with other requirements and are, therefore, unnecessary. Unlike the other criteria listed in Criterion B, in the case of redundancy, the task or activity itself may contribute to a reliable BES, but it is not necessary to have two duplicative requirements on the same or similar task or activity. Such requirements can be retired or modified with little or no effect on reliability and removal will result in an increase in efficiency of the ERO compliance program.

Criteria C (Additional data and reference points)
Use the following data and reference points to assist in the determination of (and justification for) whether to proceed with retirement or modification of a Reliability Standard requirement that satisfies both Criteria A and B:

C1. Was the Reliability Standard requirement part of a FFT filing?
The application of this criterion involves determining whether the requirement was included in a FFT filing.

C2. Is the Reliability Standard requirement being reviewed in an ongoing Standards Development Project?
The application of this criterion involves determining whether the requirement proposed for retirement or modification is part of an active Standards Development Project, with consideration for the status of the project. If the requirement has been approved by Registered Ballot Body and is scheduled to be presented to the NERC Board of Trustees, in most cases it will not need to be addressed in the periodic review. The exception would be a requirement, such as the Critical Information Protection (CIP) requirements for Version 3 and 4, that is not due to be retired for an extended period of time. Also, for informational purposes, whether the requirement is included in a future or pending Standards Development Project should be identified and discussed.

C3. What is the VRF of the Reliability Standard requirement?
The application of this criterion involves identifying the VRF of the requirement proposed for retirement or modification, with particular consideration of any requirement that has been assigned as having a Medium or High VRF. Also, the fact that a requirement has a Lower VRF is not dispositive that

it qualifies for retirement or modification. In this regard, Criterion C3 is considered in light of Criterion C5 (Reliability Principles) and C6 (Defense in Depth) to ensure that no reliability gap would be created by the retirement or modification of the Lower VRF requirement. For example, no requirement, including a Lower VRF requirement, should be retired or modified if doing so would harm the effectiveness of a larger scheme of requirements that are purposely designed to protect the reliable operation of the BES.

C4. In which tier of the most recent Actively Monitored List (AML) does the Reliability Standard requirement fall?
The application of this criterion involves identifying whether the requirement proposed for retirement or modification is on the most recent AML, with particular consideration for any requirement in the first tier of the AML.

C5. Is there a possible negative impact on NERC's published and posted reliability principles?
The application of this criterion involves consideration of the eight following reliability principles published on the NERC webpage.

Reliability Principles
NERC Reliability Standards are based on certain reliability principles that define the foundation of reliability for North American bulk power systems. Each reliability standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of reliability of the North American bulk power systems. Each reliability standard shall also be consistent with all of the reliability principles, thereby ensuring that no standard undermines reliability through an unintended consequence.

Principle 1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.

Principle 2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

Principle 3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.

Principle 4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.

Principle 5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected bulk power systems.

Principle 6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.

Principle 7. The reliability of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.

Principle 8. Bulk power systems shall be protected from malicious physical or cyber attacks. (footnote omitted).

C6. Is there any negative impact on the defense in depth protection of the BES?
The application of this criterion considers whether the requirement proposed for retirement or modification is part of a defense in depth protection strategy. In order words, the assessment is to verify whether other requirements rely on the requirement proposed for retirement or modification to protect the BES.

C7. Does the retirement or modification promote results or performance based Reliability Standards?
The application of this criterion considers whether the requirement, if retired or modified, will promote the initiative to implement results- and/or performance-based Reliability Standards.

Attachment 3: Independent Expert Evaluation Process

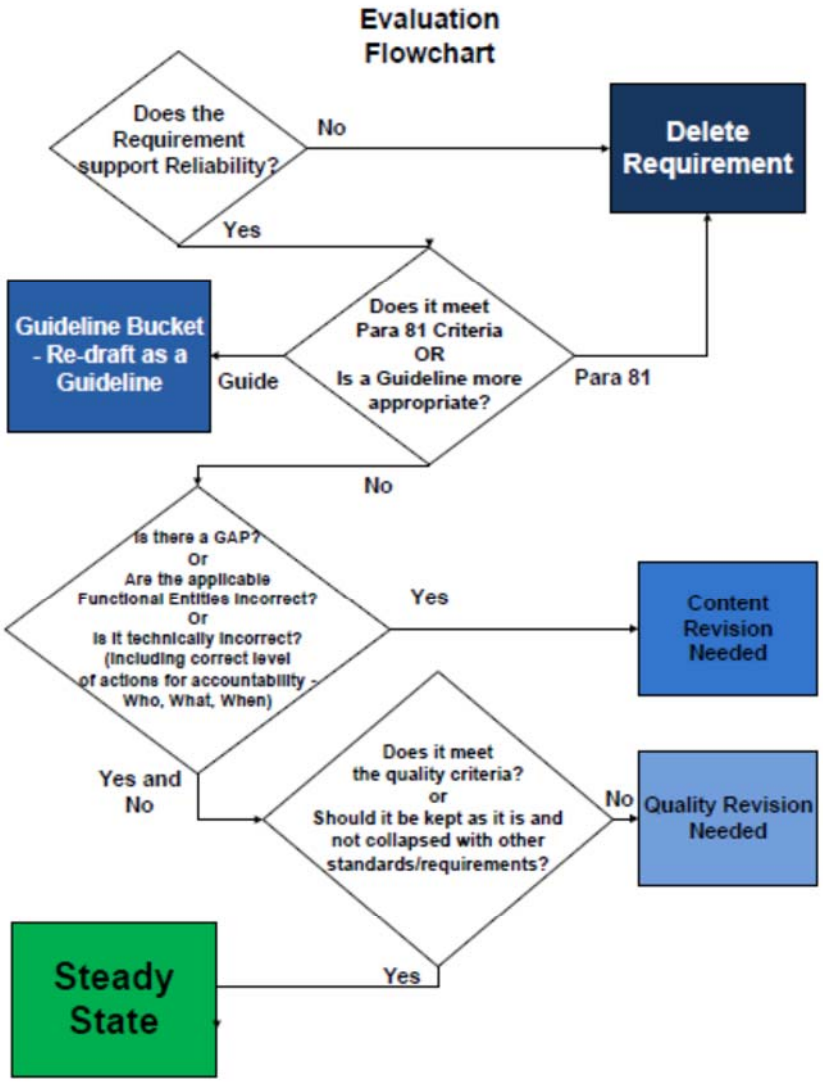


Figure 1: Evaluation Flow Chart

Background: Enhanced Period review for 2016, 2017 metric

At the February 6, 2014 Board of Trustees (Board) meeting, the Board requested that NERC management and the leadership of the Standards Committee (SC) work together to develop a mutually acceptable metric for 2015-2017, including a content and quality grading system for the Reliability Standards as part of the metric. Jointly, the following approach was developed, which was endorsed by the SC on March 12, 2014, and, in summary form, adopted by Corporate Governance and Human Resources Subcommittee of the Board on March 20, 2014:

2014 and 2015 metric

> The metric for 2014 and 2015 focuses on ensuring certain Reliability Standard projects are timely completed. For 2014, the Standard projects are all high priority Standard projects, many with regulatory deadlines.

2016 and 2017 metric

> The implementation of an enhanced Reliability Standard periodic review for quality and content that takes into consideration the following issues: (1) folding the enhanced quality and content periodic review into the period review required by Section 13 of the Standards Processes Manual; (2) a quality and content review of the steady state Standards developed, considering the use of, or adaptation of, the 2013 Independent Expert Review Team's quality and content scoring system; (3) the formation of a cross-functional task force to conduct, periodic reviews of steady state Reliability Standards, potentially consisting of Committee chairs, NERC management, NERC and stakeholder subject matter experts (all task force meetings shall be open to the public); (4) the task force to use the quality and content system developed in response to 2), above, to identify needed enhancements to steady state standards for inclusion in a Standards Authorization Request (SAR) processed through the standards development process and completed within a year from the date of posting of the SAR, unless technical review and study is needed (To the extent possible, the inclusion of identified enhancements in a SAR shall be limited focusing enhancements rather than re-opening an entire Standard(s); and (5) the development of an annual task force review timeline starting with the cross-functional task force being operational no later than mid-2015, so it can identify which standards will undergo the enhanced period review for inclusion in the 2016-2018 Reliability Standards Development Plan.

The above summary of the metric approach shows a focus on the completion of transforming NERC's Reliability Standards to a steady state by the end of 2015,[1] and, thereafter, the initiation of an enhanced periodic review to address quality and content issues related to the steady state Reliability Standards. It is contemplated that approximately 25 percent of the steady state Reliability Standards will undergo the enhanced period review in 2016, and another 25 percent in 2017.

[1] Steady state as set forth in the 2014-2016 Reliability Standards Development Plan and 2014-2016 Standards Committee Strategic Work Plan is a set of clear, concise, high quality and technically sound Reliability Standards that are results-based, while retiring requirements that do little to promote reliability.

At its March meeting, the SC appointed a periodic review development team (consisting of the SC Executive Committee and the Project Management and Oversight and Process Subcommittees chairs) to work with NERC Staff and Legal to develop the attributes of the enhanced quality and content periodic review. This team developed an approach to address the Board's direction summarized below and set forth in the attached template, along with a stakeholder comment form. The approach has been preliminarily reviewed by the SC and approved for posting for stakeholder comment. Based on stakeholder comments, the SC will consider if the proposed approach should be enhanced, prior to its endorsement and requesting NERC's Board consideration.

Summary of draft enhanced periodic review approach

- The enhanced periodic review approach will satisfy NERC's obligations under Section 13 of the Standard Processes Manual, and will be conducted in accordance with that section.

- The SC shall appoint a standing cross-functional team including NERC staff and the NERC standing committee representatives to work with the Section 13 *"review team of subject matter experts."* This team will be appointed by the SC, who will review and adopt the results of the team's deliberations.

- The cross-functional team shall be operational no later than beginning of 2015 making recommendations to the SC on the Reliability Standards that should undergo the enhanced periodic review in 2016-2018, and to be included 2016-2018 Reliability Standards Development Plan.

- NERC's five-year periodic review template that was successfully employed for number of standards in 2013 and 2014 has been revised and adapted to include quality and content questions developed by the Independent Expert Review Panel not already included. The template was further adapted to eliminate duplicative questions, andto provide the cross-functional review team with a clear framework to conduct the periodic reviews.

    - A new question was added to consider whether the applicability section or requirements can be revised for smaller entities, provided that there is technical justification to support the enhanced applicability.

    - A dashboard will be developed for each reviewed Standard indicating if whether it has a score of Green, Yellow or Red Green, according to the following grading system:
        - Green = no quality and content changes needed – Standard confirmed as steady state;
        - Yellow = quality and content issues identified, but those identified are not sufficient to justify revising Standard at this time – i.e., continue to monitor; and
        - Red = Standard needs to be revised to address identified quality and content issues.

- Standards graded as "Red" by the cross-functional review team will be revised consistent with applicable sections of the Standards Processes Manual.

Unofficial Comment Form

Enhanced Periodic Review Process and Draft 2015-2017 Reliability Standard Development Plan

Please **DO NOT** use this form for submitting comments. Please use the electronic form [insert hyperlink to electronic form] to submit comments on the Standard. The electronic comment form must be completed by [insert date].

If you have questions please contact [who] at [email address] or by telephone at [phone number].

[Insert Link to Posted Documents]

Background Information for Draft Enhanced Periodic Review Process

At the February 6, 2014 Board of Trustees (Board) meeting, the Board requested that NERC management and the leadership of the Standards Committee (SC) work together to develop a mutually acceptable metric for 2015-2017, including a content and quality grading system for the Reliability Standards as part of the metric. Jointly, the following approach was developed, which was endorsed by the SC on March 12, 2014 and, in summary form, adopted by Corporate Governance and Human Resources Subcommittee of the Board on March 20, 2014:

2014 and 2015 metric

The metric for 2014 and 2015 focuses on ensuring certain Reliability Standard projects are timely completed. For 2014, the Standard projects are all high priority Standard projects, many with regulatory deadlines.

2016 and 2017 metric

The implementation of an enhanced Reliability Standard periodic review for quality and content that takes into consideration the following issues: (1) folding the enhanced quality and content periodic review into the period review required by Section 13 of the Standards Processes Manual; (2) a quality and content review of the steady state Standards developed, considering the use of, or adaptation of, the 2013 Independent Expert Review Team's quality and content scoring system; (3) the formation of a cross-functional task force to conduct, periodic reviews of steady state Reliability Standards, potentially consisting of Committee chairs, NERC management, NERC and stakeholder subject matter experts (all task force meetings shall be open to the public); (4) the task force to use the quality and content system developed in response to 2), above, to identify needed enhancements to steady state standards for inclusion in a Standards Authorization Request (SAR) processed through the standards development process and completed within a year from the date of posting of the

SAR, unless technical review and study is needed (to the extent possible, the inclusion of identified enhancements in a SAR shall be limited focusing enhancements rather than re-opening an entire Standard(s)); and (5) the development of an annual task force review timeline starting with the cross-functional task force being operational no later than mid-2015, so it can identify which standards will undergo the enhanced period review for inclusion in the 2016-2018 Reliability Standards Development Plan.

The above summary of the metric approach shows a focus on the completion of transforming NERC's Reliability Standards to a steady state by the end of 2015[1] and, thereafter, the initiation of an enhanced periodic review to address quality and content issues related to the steady state Reliability Standards. It is contemplated that approximately 25 percent of the steady state Reliability Standards will undergo the enhanced period review in 2016, and another 25 percent in 2017.

At its March meeting, the SC appointed a periodic review development team (consisting of the SC Executive Committee and the Project Management and Oversight and Process Subcommittees chairs) to work with NERC Staff and Legal to develop the attributes of the enhanced quality and content periodic review. This team developed an approach to address the Board's direction summarized below and set forth in the attached template, along with a stakeholder comment form. The approach has been preliminarily reviewed by the SC and approved for posting for stakeholder comment. Based on stakeholder comments, the SC will consider if the proposed approach should be enhanced prior to its endorsement and requesting NERC's Board consideration.

Summary of draft enhanced periodic review approach:

- The enhanced periodic review approach will satisfy NERC's obligations under Section 13 of the Standard Processes Manual, and will be conducted in accordance with that section.
- The SC shall appoint a standing cross-functional team including NERC staff and the NERC standing committee representatives to work with the Section 13 *"review team of subject matter experts."* This team will be appointed by the SC, who will review and adopt the results of the team's deliberations.
- The cross-functional team shall be operational no later than beginning of 2015, making recommendations to the SC on the Reliability Standards that should undergo the enhanced periodic review in 2016-2018 and to be included 2016-2018 Reliability Standards Development Plan.
- NERC's five-year periodic review template that was successfully employed for number of standards in 2013 and 2014 has been revised and adapted to include quality and content questions developed by the Independent Expert Review Panel not already included. The template was further adapted to eliminate duplicative questions, and to provide the cross-functional review

[1] Steady state as set forth in the 2014-2016 Reliability Standards Development Plan and 2014-2016 Standards Committee Strategic Work Plan is a set of clear, concise, high quality and technically sound Reliability Standards that are results-based, while retiring requirements that do little to promote reliability.

team with a clear framework to conduct the periodic reviews. A new question was added to consider whether the applicability section or requirements can be revised for smaller entities, provided that there is technical justification to support the enhanced applicability.

- A dashboard will be developed for each reviewed Standard indicating if whether it has a score of Green, Yellow or Red, according to the following grading system:
  - Green = no quality and content changes needed – Standard confirmed as steady state;
  - Yellow = quality and content issues identified, but those identified are not sufficient to justify revising Standard at this time – i.e., continue to monitor; and
  - Red = Standard needs to be revised to address identified quality and content issues.
- Standards graded as "Red" by the cross-functional review team will be revised consistent with applicable sections of the Standards Processes Manual.

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

Questions

1. In order to provide both consistency in the approach to reviewing standards, as well as adequate subject matter expertise to thoroughly review specific standards, it is proposed the cross functional team reviewing and grading standards be comprised of the following: (i) a standing team made up of the Chairs of the Standards, Operating and Planning Committees (and CIPC for CIP Standards), and NERC's executive management of the Standards and RAPA groups; (ii) supplemented according to the standards being reviewed with specific subject matter experts (SMEs), including both stakeholder SMEs solicited by the standing team and NERC SMEs as assigned by NERC management.

   Do you agree with the composition of the cross functional review team? If not, please explain and suggest an alternative.

   ☐ Yes
   ☐ No
   Comments:

2. In 2013, representatives of the Standards Committee worked with NERC staff to develop a template to be used by five-year review teams. The template contained questions to ensure that review teams followed a consistent approach in reviewing standards and appendices for referencing the criteria developed by the Paragraph 81 standard drafting team to be used for

evaluating whether requirements should be retired because they do not contribute significantly to reliability. This template has been revised for use by the above-mentioned cross-functional review team, and is posted along with this comment form.

Do you agree with the questions in the template? If there are additional questions you believe should be added, please provide them in your comments.

☐ Yes
☐ No
Comments:

3. Do you agree with the grading system using Green, Yellow, and Red? If not, please explain and suggest improvements.

   ☐ Yes
   ☐ No
   Comments:

4. Do you believe that a question related to the cost effectiveness of the standard should be added to the template as a way to institutionalize considerations of cost effectiveness?

   ☐ Yes
   ☐ No
   Comments:

5. Are there any other comments you have on the template?

   ☐ Yes
   ☐ No
   Comments:

6. Chapter 4 of the 2013 Independent Experts' report recommends consolidating approximately 25 requirements and regrouping some requirements into a New Construct for clarity and simplification. NERC Staff and the Standards Committee is interested in whether you believe that consolidating and regrouping some of the requirements, either as recommended by the Independent Experts' or with modifications to the New Construct suggestion, would be beneficial? If you answered yes, please indicate in your comments whether the New Construct should be considered during the periodic reviews of standards or, if not, indicate when and how the New Construct should be initiated.

☐ Yes
☐ No
Comments:

7. If you have any other comments on the enhanced approach to periodic reviews that you haven't already mentioned above, please provide them here:

   Comments:

Background Information for Draft 2015-2017 Reliability Standards Development Plan

The 2015-2017 Reliability Standards Development Plan (2015-2017 RSDP) is another bold step toward transforming the NERC Reliability Standards. During 2015, the NERC Reliability Standards will reach Steady-State[2] and the number of active projects will dramatically decrease. Concurrently, to begin the final transition in the transformation process, the industry-endorsed criteria for evaluating the content and quality of standards will be applied to standards or standard families during enhanced periodic reviews, focused on continuous improvement.

With the support from the Standards Committee and industry stakeholders, NERC Reliability Standards have made great strides over the last two years. By the end of 2015, the majority of the Paragraph 81 candidates,[3] the Independent Expert Review Panel's (IERP) recommendations for requirement retirement, and Federal Energy Regulatory Commission (FERC) directives issued prior to December 2012 will be addressed. Projects that were languishing for years, as well as five-year reviews will be completed. The industry will also have completed large projects to respond to FERC orders, including, for example, Geomagnetic Disturbances, CIP Version 5 Revisions, and CIP-014 Physical Security, revised the TOP and IRO standards to address concerns identified in FERC's proposed remand, and will have addressed the majority of FERC directives issued after December 2012. This is a significant achievement – the Standards Committee worked diligently with NERC to determine project schedules and manage industry workload. Stakeholders engaged throughout North America to provide expertise during standard development ensuring projects could reach completion.

Now, in the 2015-2017 RSDP, the number of projects necessary to reach Steady-State by 2015 is reduced and the pace of the work will likely become more deliberate. Six projects that began during 2014 will be completed in 2015, while four new projects will be initiated in 2015, with one focused on aligning the Glossary of Terms used in NERC Reliability Standards with the Definitions used in the Rules of Procedure (Rules of Procedure, Appendix 2). This reduction in planned projects provides a bandwidth for projects

[2] As stated in the 2014-2016 RSDP and 2014-2016 Standards Committee Strategic Work Plan, Steady State means a set of clear, concise, high quality and technically sound Reliability Standards that are results-based, while retiring requirements that do little to promote reliability.
[3] There are 6 P81 candidates that will be addressed during the enhanced periodic reviews, starting in 2016.

required to respond to emerging risks, if any, to reliability, establish a quality and content enhanced periodic review, as well as any new FERC orders or directives. Also, given the increased focus on quality during the standard development process as well as active engagement of FERC Office of Electric Reliability staff during the standards development process, FERC directives and orders on existing standards are expected to trend lower.

Arriving to Steady-State provides an opportunity for critical assessment of the existing reliability standards through enhanced periodic reviews, and following the reviews to implement recommendations for quality, content, or alignment with other standards using industry-developed criteria,[4] building on the foundation established by the IERP.[5] Over the last 7 years, the Electric Reliability Organization (ERO) and industry have gained experience in understanding the characteristics of quality, results-based standards, while targeting their applicability based on risk to achieve a reliability benefit without creating undue burden on industry.

Questions

8. For the 2015-2017 RSDP, are there any outstanding reliability gaps or issues that are not addressed by the existing Standard projects that you believe need to be addressed by a new Standard project?

   ☐ Yes
   ☐ No
   Comments:

9. Do you agree with the prioritization ranking (high, medium, low) of the 2015 projects?

   ☐ Yes
   ☐ No
   Comments:

10. Please provide any other comments you have on the 2015-2017 RSDP.

    Comments:

[4] The Independent Experts developed criteria is described in their final report, Standards Independent Experts Review Project, however this criteria was not vetted with industry.

[5] The North American Electric Reliability Corporation (NERC) retained five industry experts to independently review the NERC Reliability Standards, setting the foundation for a plan that will result in a set of clear, concise and sustainable body of Reliability Standards. The primary scope was an assessment of the content and quality of the Reliability Standards, including identification of potential Bulk-Power System (BPS) risks that were not adequately mitigated.

Agenda Item 6
Standards Committee
May 14, 2014

SC Meetings in 2015

Action

Approve Brenda Hampton to work with NERC Staff on developing the meeting schedule (including locations of face-to-face meetings) for 2015 and present a mutually acceptable (Brenda and her team/NERC Staff) proposal to the Standards Committee for approval no later than its October 2014 call. Brenda will also seek out other interested Standards Committee members to work with her and NERC Staff on this matter.

Background

Brenda Hampton volunteered to proactively work with NERC Staff to develop a mutually acceptable meeting schedule (including locations of face-to-face meetings) for 2015. It seems in the interest of Standards Committee and NERC Staff to have a small team of Standard Committee members work with Staff on this matter and present a joint proposal for the Committee's consideration.

Agenda Item 7
Standards Committee
May 14, 2014

Detail of Minutes, Re: Appointment of Drafting Teams

Action

Approve one of the following approaches to capturing the appointment of drafting teams in the meeting minutes of the Standards Committee:

1. Add a hot link in the minutes to the Standards project page where the roster of the drafting team is maintained;
2. Include the names and organizations of appointed drafting team in the minutes; or
3. Maintain the status quo: the minutes only indicate that a drafting team was appointed for a certain Standard project.

Background

David Kiguel, a former member of the Standards Committee, brought the issue to the Chair and would like the Committee to consider adopting Option 2 to provide for greater transparency of Standard Committee activities. The Chair of the Standards Committee has worked with David to provide the Committee with the above options to consider.

According to David, reasons and advantages for adopting Option 2 are:

- Once appointed by the Standards Committee, the list of Standard Drafting Team members is no longer confidential.
- Minutes should reflect the fully approved motion.
- Meeting minutes, as approved by the Standards Committee, are the sole authoritative source of Standards Committee decisions, avoiding possible transcript inaccuracies.
- Posting of the Standard Drafting Team roster document in the project page may experience delays.

Reliability Issues Steering Committee Triage Diagram

Action

Informational update only

In the first quarter of 2013, the Standards Committee (SC) and the Reliability Issues Steering Committee (RISC) endorsed the use of "GUIDELINES FOR NERC STANDARDS COMMITTEE COORDINATION WITH THE RELIABILITY ISSUES STEERING COMMITTEE," which included, among other provisions, the following:

- The SC and NERC Staff will request RISC to review and provide recommendations on the next year's draft RSDP.
- Any Standards Authorization Request ("SAR") or proposed Reliability Standard submitted to the SC that implicates or identifies a new or emerging reliability risk may be sent by the SC through the SC Chair to RISC for its review and comment.

In addition, in the fourth quarter of 2013, the SC and RISC endorsed a consensus building approach (Option C) that indicated that RISC was in the best positioned to triage new problem statements on reliability, including recommending the appropriate tool (guideline, criteria, alert, standard) to address the new problem statement on reliability.

In light of the above, and for its own purposes, RISC developed and endorsed the attached diagram that illustrates the following:

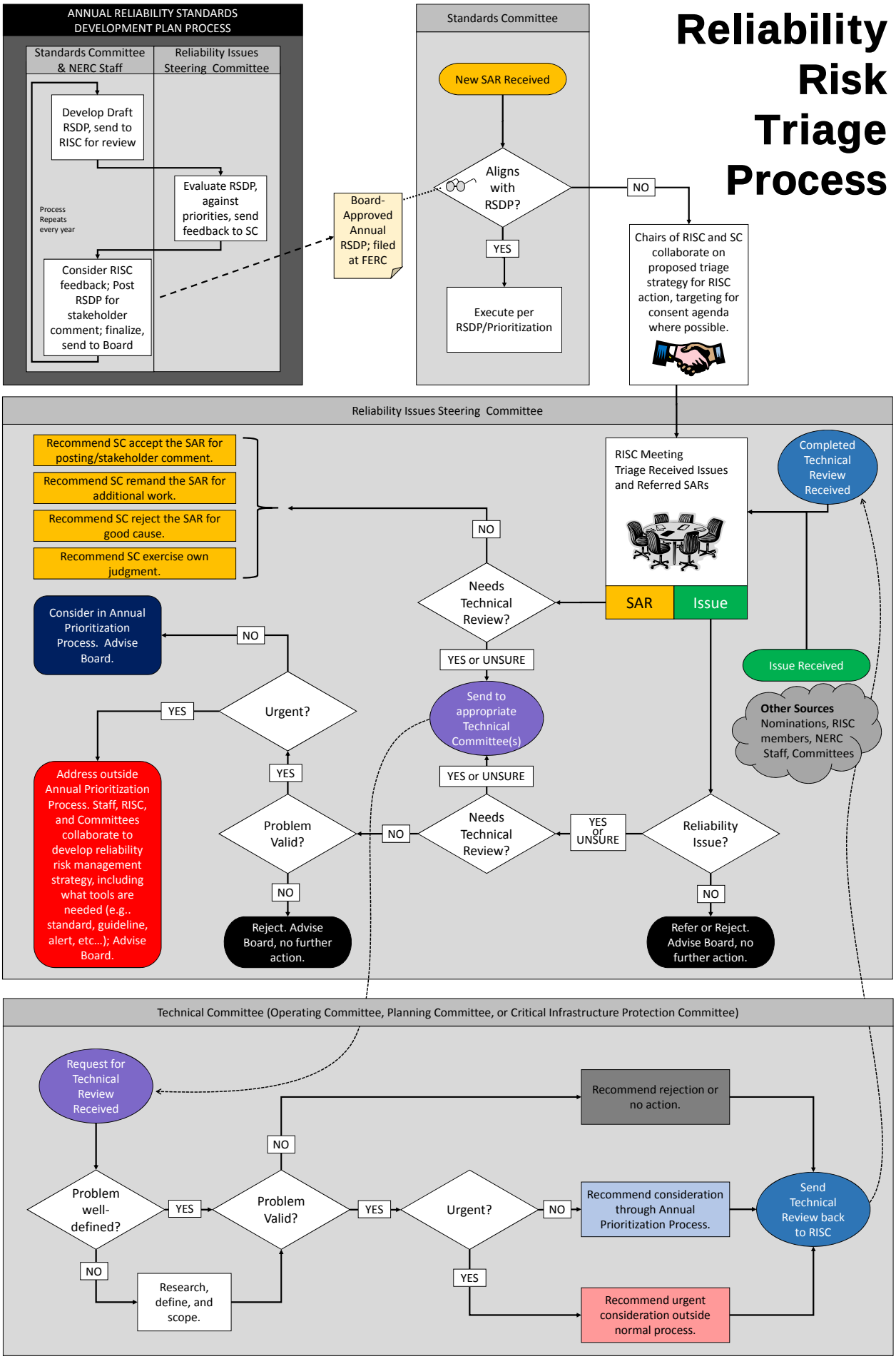
1. That it will review and provide recommendations on draft RSDPs, including recommendations on the need and prioritization for Standard projects (the same as it did in 2013);
2. That any Standard project that is identified in a Board of Trustees approved RSDP, the Standard project will not be reviewed by RISC when a SAR is drafted, posted, etc;
3. That if a SAR is submitted for a Standard project not identified in the approved RSDP, the Chair of the SC will request the SC's to endorse to invoke the following provision in Section 4.1 of the Standards processes Manual so that RISC may decide whether to review and make recommendations on the SAR:

   > SAR Delay action on the SAR pending one of the following: (i) development of a technical justification for the proposed project; or (ii) consultation with another NERC Committee to determine if there is another approach to addressing the issue raised in the SAR.

   If the SC endorses RISC review of a SAR, the Chair of the SC shall request the Chair of RISC to place it on RISC's next agenda for review and recommendations, which will likely include RISC requesting NERC technical committee input prior to RISC recommendations on the SAR.
4. How a new reliability problem statement on reliability issue can be presented to RISC via the technical committees or nominations.

The attached RISC diagram will be placed in the RISC handbook and used by RISC to guide the committee when presented with a SAR or a new problem statement on reliability issue.

Reliability Risk Triage Process



Process flow for new SARs, Nominations, Issues and problems identified by the technical committees during the course of their regular activities. Note that exceptions will be handled on an as-needed basis.

Update: Reaching Quorum for Standards Ballots

Action

Informational update only

In light of the recent challenges in reaching quorum at the end of the ballot period, the Standards Committee Process Subcommittee (SCPS) and NERC staff have been "exploring options to create and maintain an effective ballot pool and strategies to address situations where a quorum is not reached by the time a ballot period is scheduled to close." November 2013 SC Agenda item 13 (a) iii. Those efforts are ongoing. A report is being prepared for the June SC meeting detailing what NERC has done to date to address quorum issues, steps that are being executed for projects in the current standard balloting system and enhancements contained in the new standard balloting system that have the potential to improve reaching quorum. In the interim, the chair and vice chair of the Standards Committee (SC) have been assisting NERC Staff and sending emails asking voters who have not yet voted to vote. Also, NERC Staff will explore with the SCPS (and then the SC) the practicability and appropriateness of having voters voluntarily notify NERC when they join the ballot pool that in the event they fail to vote by the voting deadline that their vote should be recorded as an abstention.

Standards Committee Project Management Oversight Subcommittee (PMOS) Update

Action

None requested. Update Only.

Background

The PMOS met in person on April 17, 2014. The following items were discussed.

1. Per previous Standards Committee (SC) discussions, NERC Staff has added a column to the Project Tracking Spreadsheet to indicate whether a project is "consistent with the direction" of the Independent Experts Report. NERC Staff has populated the new column for each of the projects on the spreadsheet.
2. The PMOS Liaisons present provided a brief update on progress of assigned projects.
3. The role of the PMOS liaisons in participating in a Standard Drafting Team's response to stakeholder comments was discussed. The PMOS decided not to change or expand the liaison role for now.
4. Changes to the PMOS charter to conform to proposed changes to the Standards Committee Process Subcommittee (SCPS) charter were discussed. Any potential changes were put on hold pending further conversations between SC Leadership and the SCPS.
5. The SC Chair updated PMOS on the RISC Triage Diagram and will provide further updates at this SC meeting.
6. Finally, a schedule for future meetings was set: PMOS will meet at Xcel Energy in Denver, CO from 8 a.m. to 12 p.m. MST on June 10, 2014 and will meet at Bonneville Power Administration in Portland, OR from 8 a.m. to 12 p.m. PST on September 30, 2014.

Agenda Item 10b
Standards Committee
May 14, 2014

Standards Committee Process Subcommittee Membership

Action

Approve recommended slate of additional members.

Background

The Standards Committee Process Subcommittee (SCPS) has identified a need for new members. A solicitation for nominations was sent to the registered ballot body and the standards and NERC roster distribution lists. The SCPS Chair, Vice Chair, and NERC staff member reviewed the nominations and developed a slate of recommended additions to the roster. Both the current roster and the recommended additions are provided as supporting meeting documents. Two of the recommended additions are current Standards Committee (SC) members. They will provide the benefit of insight into SC views and direction. Two of the recommended additions are active SC and SCPS observers. These two members are familiar with the current work of the SC and SCPS, and have evidenced their ability to dedicate the time required to be active participants. The final recommended addition provides a fresh perspective due to not being an active SC or SCPS member or observer, and has also received positive recommendations from previous Standard Drafting Team work and Regional involvement.

Agenda Item 11
Standards Committee
May 14, 2014

Standards Committee Communications Updates and Activities

Action
Information only.

Background
Mallory Huggins of NERC Staff and Scott Miller will provide an update on NERC and Standards Committee communication activities in the last month, including plans for upcoming standards webinars and workshops.

NERC Legal and Regulatory Filings - Standards

RECENT FILINGS

DATE	PROJECT/DESCRIPTION
March 7, 2014	Petition of NERC for Approval of Proposed Reliability Standard PER-005-2 and Retirement of Reliability Standard PER-005-1. Docket No. RD14-7
March 10, 2014	Doc-Less Motion to Intervene in Docket No. RD14-6-000
March 12, 2014	Petition of NERC for Approval of Interpretation of Regional Reliability Standard TOP-007-WECC-1. Docket Nos. RM09-14 and RD14-8
March 18, 2014	Request of NERC for Extension of Time to File Revisions to the Violation Risk Factors Assigned to Reliability Standards CIP-006-5, Requirement R3 and CIP-004-5, Requirement R4. Docket No. RM13-5
March 24, 2014	Comments of NERC in Response to Notice of Proposed Rulemaking EOP-010-1 (Geomagnetic Disturbance Operations). Docket No. RM14-1
March 31, 2014	NERC Standards Report, Status and Timetable for Processing Regulatory Directives. Docket No. RR09-6
April 1, 2014	TOP/IRO Quarterly Status Report. Docket No. RM13-12, RM13-14, RM3-15
April 2, 2014	Petition of NERC for Approval of Reliability Standard BAL-001-2 (Real Power Balancing Control Performance). Docket No. RM14-10

UPCOMING FILING DATES

DATE	PROJECT/DESCRIPTION
May 31, 2014	Quarterly Nova Scotia filing
May 31, 2014	Quarterly filing regarding timeframe to restore power to the auxiliary systems of nuclear power plants

PROJECTED FILINGS

STATUS	PROJECT/DESCRIPTION
Scheduled for BOT, May 2014 Projected Filing Date: May 2014	Petition for Approval of COM-002-4
Scheduled for BOT, May 2014	Petition for Approval of Proposed Reliability Standard MOD-031-1

STATUS	PROJECT/DESCRIPTION
Projected Filing Date: Mid-May 2014	
Scheduled for BOT, May 2014 Projected Filing Date: Late-May 2014	Petition for Approval of Proposed Reliability Standards VAR-001-4 and VAR-002-3
Scheduled for BOT, May 2014 Projected Filing Date: June 5, 2014	Petition for Approval of Physical Security Standard

Standards Committee Expectations

Approved by Standards Committee January 12, 2012

Background

Standards Committee (SC) members are elected by members of their segment of the Registered Ballot Body, to help the SC fulfill its purpose. According to the Standards Committee Charter, the SC's purpose is:

> *In compliance with the NERC Reliability Standards Development Procedure, the Standards Committee manages the NERC standards development process for the North American-wide reliability standards with the support of the NERC staff to achieve broad bulk power system reliability goals for the industry. The Standards Committee protects the integrity and credibility of the standards development process.*

The purpose of this document is to outline the key considerations that each member of the SC must make in fulfilling his or her duties. Each member is accountable to the members of the Segment that elected them, other members of the SC, and the NERC Board of Trustees for carrying out their responsibilities in accordance with this document.

Expectations of Standards Committee Members

1. SC Members represent their segment, not their organization or personal views. Each member is expected to identify and use mechanisms for being in contact with members of the segment in order to maintain a current perspective of the views, concerns, and input from that segment. NERC can provide mechanisms to support communications if an SC member requests such assistance.

2. SC Members base their decisions on what is best for reliability and must consider not only what is best for their segment, but also what is in the best interest of the broader industry and reliability.

3. SC Members should make every effort to attend scheduled meetings, and when not available are required to identify and brief a proxy from the same segment. Standards Committee business cannot be conducted in the absence of a quorum, and it is essential that each Standards Committee make a commitment to being present.

4. SC Members should not leverage or attempt to leverage their position on the SC to influence the outcome of standards projects.

5. The role of the Standards Committee is to manage the standards process and the quality of the output, not the technical content of standards.

Standards Committee Meeting Dates and Locations for 2014

Face-to-face meetings are typically conducted from 1-5 p.m. on Tuesday and 8 a.m.-12 p.m. on Wednesday, except for the March 2014 face-to-face meeting, which will be held from 1-5 p.m. on Wednesday and 8 a.m.-12 p.m. on Thursday due to space availability. Also, the January 2014 meeting will be a half-day face-to-face meeting. Conference calls are held each month on a Wednesday from 1-5 p.m. Eastern where the SC does not have a face-to-face meeting. The time for face-to-face meetings is based on the 'local' time zone. The time specified for all conference calls is based on the Eastern time zone.

- January 15, 2014 – Atlanta, GA from 1-5 p.m.
- February 12, 2014 – conference call from 1-5 p.m.
- March 12-13, 2014 – Atlanta, GA (1-5 p.m. March 12; 8 a.m.-12 p.m. March 13) **(Wed.-Thurs.)**
- April 9, 2014 – conference call from 1-5 p.m.
- May 14, 2014 – conference call from 1-5 p.m.
- June 10-11, 2014 – Denver, CO (1-5 p.m. June 10; 8 a.m.-12 p.m. June 11)
- July 16, 2014 – conference call from 1-5 p.m.
- August 20, 2014 – conference call from 1-5 p.m.
- September 30, 2014- October 1, 2014 – Portland, OR (1-5 p.m. September 30; 8 a.m.-12 p.m. October 1)
- October 22, 2014 – conference call from 1-5 p.m.
- November 19, 2014 – conference call from 1-5 p.m.
- December 9-10, 2014 – Atlanta, GA (1-5 p.m. December 9; 8 a.m.-12 p.m. December 10)

The Standards Committee has two subcommittees (Project Management and Oversight Committee (PMOS) and Process Subcommittee (SCPS)) which will schedule face-to-face meetings in Atlanta and Portland and conference calls as they deem necessary. They may choose to meet the morning (8 a.m.-12 p.m.) of the first day of the Standards Committee's face-to-face meetings.

Standards Committee
2014 Segment Representatives

Segment and Term	Representative	Organization
Chairman **2014-15**	Brian Murphy Manager, NERC Reliability Standards	NextEra Energy, Inc.
Vice-chairman **2014-15**	Scott Miller Manager Regulatory Policy	MEAG Power
Segment 1-2013-14	Lou Oberski Managing Director, NERC Compliance Policy	Dominion Resources Services, Inc.
Segment 1-2014-15	Laura Lee Manager of ERO Support and Event Analysis, System Operations	Duke Energy
Segment 2-2013-14	Charles Yeung Executive Director Interregional Affairs	Southwest Power Pool
Segment 2-2014-15	Ben Li Consultant	Independent Electric System Operator
Segment 3-2013-14	Jennifer Sterling Director, Exelon NERC Compliance Program	Exelon
Segment 3-2014-15	Ron Parsons General Manager of Transmission Interconnections and Operations	Alabama Power Company
Segment 4-2013-14	Joseph Tarantino Regulatory Compliance Coordinator	Sacramento Municipal Utility District
Segment 4-2014-15	Frank Gaffney Assistant General Manager of and Officer of Regulatory Compliance	Florida Municipal Power Authority
Segment 5-2013-14	Gary Kruempel Compliance Director, Energy Supply	MidAmerican Energy Company

Segment and Term	Representative	Organization
Segment 5-2014-15	Randy Crissman Vice President – Technical Compliance	New York Power Authority
Segment 6-2013-14	Brenda Hampton Regulatory Policy	Energy Future Holdings – Luminant Energy Company LLC
Segment 6-2014-15	Andrew Gallo Director, Reliability Compliance	City of Austin dba Austin Energy
Segment 7-2013-14	John A. Anderson President & CEO	Electricity Consumers Resource Council
Segment 7-2014-15	Frank McElvain Senior Consulting Manager	Siemens Energy, Inc.
Segment 8-2013-14	Robert Blohm Managing Director	Keen Resources Asia Ltd.
Segment 8-2014-15	Frederick Plett Utility Analyst	Massachusetts Attorney General
Segment 9-2014	Klaus Lambeck Chief Facilities, Siting and Environmental Analysis	Public Utilities Commission of Ohio/the Ohio Power Siting Board
Segment 9-2014-15	Jason Woodruff Electrical Engineer	Public Utilities Commission of Nevada
Segment 10-2013-14	Steve Rueckert Director of Standards	Western Electricity Coordinating Council
Segment 10-2014-15	Guy Zito Assistant Vice President of Standards	Northeast Power Coordinating Council

Parliamentary Procedures

Based on Robert's Rules of Order, Newly Revised, 10th Edition, plus "Organization and Procedures Manual for the NERC Standing Committees"

Motions

Unless noted otherwise, all procedures require a "second" to enable discussion.

When you want to…	Procedure	Debatable	Comments
Raise an issue for discussion	Move	Yes	The main action that begins a debate.
Revise a Motion currently under discussion	Amend	Yes	Takes precedence over discussion of main motion. Motions to amend an amendment are allowed, but not any further. The amendment must be germane to the main motion, and can not reverse the intent of the main motion.
Reconsider a Motion already approved	Reconsider	Yes	Allowed only by member who voted on the prevailing side of the original motion.
End debate	Call for the Question *or* End Debate	Yes	If the Chair senses that the committee is ready to vote, he may say "if there are no objections, we will now vote on the Motion." Otherwise, this motion is debatable and subject to 2/3 majority approval.
Record each member's vote on a Motion	Request a Roll Call Vote	No	Takes precedence over main motion. No debate allowed, but the members must approve by 2/3 majority.
Postpone discussion until later in the meeting	Lay on the Table	Yes	Takes precedence over main motion. Used only to postpone discussion until later in the meeting.
Postpone discussion until a future date	Postpone until	Yes	Takes precedence over main motion. Debatable only regarding the date (and time) at which to bring the Motion back for further discussion.
Remove the motion for any further consideration	Postpone indefinitely	Yes	Takes precedence over main motion. Debate can extend to the discussion of the main motion. If approved, it effectively "kills" the motion. Useful for disposing of a badly chosen motion that can not be adopted or rejected without undesirable consequences.
Request a review of procedure	Point of order	No	Second not required. The Chair or secretary shall review the parliamentary procedure used during the discussion of the Motion.

Notes on Motions

Seconds. A Motion must have a second to ensure that at least two members wish to discuss the issue. The "seconder" is not recorded in the minutes. Neither are motions that do not receive a second.

Announcement by the Chair. The Chair should announce the Motion before debate begins. This ensures that the wording is understood by the membership. Once the Motion is announced and seconded, the Committee "owns" the motion, and must deal with it according to parliamentary procedure.

Voting

Voting Method	When Used	How Recorded in Minutes
Unanimous Consent	When the Chair senses that the Committee is substantially in agreement, and the Motion needed little or no debate. No actual vote is taken.	The minutes show "by unanimous consent."
Vote by Voice	The standard practice.	The minutes show Approved or Not Approved (or Failed).
Vote by Show of Hands (tally)	To record the number of votes on each side when an issue has engendered substantial debate or appears to be divisive. Also used when a Voice Vote is inconclusive. (The Chair should ask for a Vote by Show of Hands when requested by a member).	The minutes show both vote totals, and then Approved or Not Approved (or Failed).
Vote by Roll Call	To record each member's vote. Each member is called upon by the Secretary,, and the member indicates either "Yes," "No," or "Present" if abstaining.	The minutes will include the list of members, how each voted or abstained, and the vote totals. Those members for which a "Yes," "No," or "Present" is not shown are considered absent for the vote.

Notes on Voting

(Recommendations from DMB, not necessarily Mr. Robert)

Abstentions. When a member abstains, he is not voting on the Motion, and his abstention is not counted in determining the results of the vote. The Chair should not ask for a tally of those who abstained.

Determining the results. The results of the vote (other than Unanimous Consent) are determined by dividing the votes in favor by the total votes cast. Abstentions are not counted in the vote and shall not be assumed to be on either side.

"Unanimous Approval." Can only be determined by a Roll Call vote because the other methods do not determine whether every member attending the meeting was actually present when the vote was taken, or whether there were abstentions.

Majorities. Robert's Rules use a simple majority (one more than half) as the default for most motions. NERC uses 2/3 majority for all motions.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda

Standards Committee Process Subcommittee

June 10, 2014 | 8:00 a.m.–12:00 p.m. MT
June 11, 2014 | 1:00–5:00 p.m. MT

Xcel Energy
1800 Larimer Street
Denver, CO 80202

Conference Dial-in Information:
Phone: 1-866-740-1260 | Access Code: 9214643 | Security Code: 070452

Administrative

1. **Introductions and Chair's Remarks**
2. **NERC Antitrust Compliance Guidelines and Public Announcement***
3. **Approval of Meeting Notes from May 22, 2014 Conference Call***
4. **Review Team Roster***
5. **Review of Agenda and Objectives**

Agenda Items

1. **SCPS Activities***
   a. Consolidate SC Resource Documents – **G. Zito and M. Benson**
   b. Cost Effectiveness Analysis Process (CEAP) – **G. Zito**
   c. Charter Revisions* – **B. Li and S. Miller**
   d. Modifications to Quality Review (QR) Process* – **K. Porterfield**
   e. Review of Standards Processes and Procedures*– **P. Heidrich**
   f. Consensus Building for SAR Development* – **B. Li**
   g. Process to Improve the Effectiveness of Managing Ballot Pools* – **L. Lee**
4. **SCPS Work Plan*** – **B. Li and L. Lee**
5. **Communication with Industry – L. Lee**
6. **Items for Next Standards Committee Meeting** – **L. Lee and E. Chanzes**

7. **Review of Actions/Assignments – E. Chanzes**
8. **Future Meetings**
   a. Meetings in coordination with the Standards Committee:

      September 30–October 1, 2014 (8:00 a.m.–12:00 p.m.|1:00–5:00 p.m.) Portland
      December 9–10, 2014 (8:00 a.m.–12:00 p.m.|1:00–5:00 p.m.) Atlanta

   b. Interim Meetings
9. **Adjourn**

*Background materials are included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Public Announcements

REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

For face-to-face meeting, with dial-in capability:
Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Notes
Standards Committee Process Subcommittee

May 22, 2014 | 11:00 a.m.–1:00 p.m. ET

Conference Call with ReadyTalk Web Access

Administrative

1. **Introductions and Chair's Remarks**
   L. Lee brought the meeting to order on Thursday, May 22, 2014 at 11:02 a.m. ET. She welcomed the attendees and thanked them for their participation.

2. **NERC Antitrust Compliance Guidelines and Public Announcement**
   E. Chanzes reviewed the NERC Antitrust Compliance Guidelines and announced that the meeting was public.

3. **Approval of Meeting Notes from April 23, 2014 Conference Call**
   With the correction that the Standards Committee (SC) endorsed the Cost Effectiveness Analysis Process (CEAP) report for posting rather than approved the report for posting (Agenda item 2a), the meeting notes from the April 23, 2014 conference call were approved.

Agenda Items

1. **Update on Solicitation for New Members – L. Lee**
   L. Lee welcomed the five newly added members to the Standards Committee Process Subcommittee (SCPS), provided a brief overview of the subcommittee's processes and procedures, and asked new members to let a task group lead know if he or she is interested in being a part of that task group. L. Lee explained that these new members' terms would be for the 2014–2015 calendar years even though they were not added until mid-year. E. Chanzes noted that she would be adding each member's terms to the roster, and L. Lee asked all members to let her and E. Chanzes know if they plan to serve less than a two-year term.

   E. Chanzes will add each member's terms to the current SCPS roster.

2. **SCPS Activities**

   a. **Consolidate SC Resource Documents – G. Zito**
   G. Zito provided a brief history of this project for new members and reported that M. Benson has completed work on a "Resource Package" that will accompany the Drafting Team Reference Manual. This will be circulated to the SCPS for review prior to submitting the package to the SC for their July meeting.

   G. Zito will review the completed Resource Package and circulate to the SCPS for review.

   b. **Process to Improve the Effectiveness of Managing Ballot Pools – L. Lee**
   L. Lee provided a brief history on this project for the new members and reported that she has been working on an informational report to provide the SC for their June meeting. This report will explain the SCPS's current status on this task with respect to work with NERC staff to identify and communicate current NERC strategies for addressing issues with ballots achieving quorum. This includes what's been done to address issues in the past, what's being done currently, and anticipated improvements resulting from the roll-out of the new Standards Balloting System (SBS). The report will also include data points on recent ballots that failed to achieve quorum, and it will explain that the SCPS will be working with NERC staff to evaluate the results of the SBS enhancements and continued interim steps.

   L. Lee will finalize and circulate the informational report to the SCPS and submit for the June SC meeting.

   c. **Consensus Building and SAR Development – B. Li**
   B. Li provided a brief history on this task and reported that the task group met with NERC staff and agreed to the current scope doc with minor changes. The SCPS reviewed and agreed that the scope document was ready to submit to the SC for endorsement.

   B. Li will submit the scope document for the June SC meeting.

   d. **Review of Standards Processes and Procedures – J. Tarantino**
   J. Tarantino provided a brief history on this task and explained that the task group met with NERC staff and came to the conclusion that the SCPS should wait to fully launch this effort until active projects and Standards Process Manual (SPM) revisions have further matured. In the interim, informal outreach could be conducted to continue to identify standard development process issues. Looking forward, the plan would be to form a formal outreach plan to gather input on the standards development process during the first quarter of 2015, and then outreach would be implemented during the second quarter. This will hopefully converge with a more "steady state" of standards projects. It was also noted that NERC staff is in agreement with the scope document if there is the timing adjustment.

The SCPS agreed to provide the scope document with information about the new time frame to the SC for endorsement.

J. Tarantino will submit the scope document for the June SC meeting.

e. **Modify SC Quality Review (QR) Process – K. Porterfield (Added to agenda during meeting)**
The status of the work on the QR process was raised and added to the agenda. K. Porterfield and L. Lee explained that the SCPS had come to consensus during the April 23 call to move forward with submitting the task group's agreed-upon approach with NERC staff to the SC for endorsement. The proposal is that the NERC Coordination QR document can replace the QR process/template, provided that NERC staff commits to communicating the steps that were taken for QR prior to an initial posting. L. Lee explained that she is still working with B. Murphy to determine the best SC meeting for the discussion. Some SCPS members who had not been in attendance during the April 23 call requested to add this topic to the June SCPS meeting agenda for further discussion.

f. **CEAP Pilot – G. Zito (Added to agenda during meeting)**
G. Zito requested to provide an update on this task and it was added to the agenda. He noted that he had met with G. Cauley and M. Lauby about reworking the CEAP guidelines as necessary to move forward with applying CEAP to standards projects in 2014. He noted that the CEAP team is meeting at FRCC June 3–4 and that he would update the SCPS on the outcomes during the June SCPS meeting.

3. **Periodic Review Template – L. Lee (Added to agenda during meeting)**

A. Pusztai raised this topic and L. Lee requested that it be added to the agenda. L. Lee provided background, explaining that the "Enhanced Periodic Review" that was recently authorized for posting by the SC was a result of the development of a NERC company metric, which includes a focus on a periodic review after the end of 2015 to address quality and content issues related to the steady state of Reliability Standards. At its March meeting, the SC appointed the SC, SCPS, and PMOS chairs and NERC staff to develop the attributes of an enhanced quality and content periodic review. The result was the approach that was approved by the SC at its May meeting to be posted for stakeholder comment, which converges the existing five-year review process (now referred to as the periodic review) with an assessment of quality.

A. Pusztai noted that his concern was whether this process should have gone through the SCPS prior to going to the SC to authorize posting. It was explained that the Enhanced Periodic Review approach is a part of the 2015–2017 Reliability Standards Development Plan (RSDP), which follows the process of development by NERC staff, authorization by the SC to post for stakeholder comments, and then SC approval.

5. **Communication with Industry – L. Lee**
   L. Lee noted that the task group for the ballot pool management task should engage with NERC staff about further communications with industry once the report is delivered to the SC in June.

6. **Items Slated for Presentation at Next Standards Committee Meeting – L. Lee and E. Chanzes**

   Update on Ballot Pool Management efforts **(L. Lee)**
   Endorse Consensus Building for SAR Development scope **(B. Li)**
   Endorse Review of Standards Processes and Procedures scope **(J. Tarantino to provide materials; L. Lee to provide SC report)**

7. **Review of Actions/Assignments** – E. Chanzes

   Administrative

   Add membership terms to roster **(E. Chanzes)**
   Inform task group leads if interested in being part of task's group **(New Members)**

   Task-specific

   QR Process: Discuss with B. Murphy about which upcoming SC meeting to submit; Follow up with S. Miller about including QR review information on the project tracking spreadsheet **(L. Lee)**

   Consolidate SC Resource Documents: Circulate resource package to SCPS for review **(G. Zito)**

   Process to Improve the Effectiveness of Balloting: Finalize report/one-pager and submit for June SC meeting **(L. Lee)**

   Consensus Building for SAR Development: Submit scope document and one-pager for June SC meeting **(B. Li)**

   Review Standards Development Processes and Procedures: Submit scope document and one-pager for June SC meeting **(J. Tarantino)**

8. **Future Meetings**

   a. Meetings in coordination with Standards Committee:

      June 10–11, 2014 (8:00 a.m.–12:00 p.m.|1:00–5:00 p.m.) Denver
      September 30–October 1, 2014 (8:00 a.m.–12:00 p.m.|1:00–5:00 p.m.) Portland

December 9–10, 2014 (8:00 a.m.–12:00 p.m.|1:00–5:00 p.m.) Atlanta

b. Interim Meetings
A future interim conference call will be discussed during the June SCPS meeting.

9. **Adjourn**

L. Lee thanked members for their participation and adjourned the meeting.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2014 Roster

Standards Committee Process Subcommittee

Term	Participant	Entity
2013–14	Laura Lee (Chair)	Duke Energy
2013–14	Peter Heidrich (Vice Chair)	Florida Reliability Coordinating Council
2014–15	Brian Buckley	Tampa Electric Co.
2014–15	Randy Crissman	New York Power Authority
2014–15	Brenda Hampton	Energy Future Holdings (Luminant)
2014–15	Lorissa Jones	Bonneville Power Administration
2014–15	P.S. (Ben) Li	Ben Li Associates, Inc.
2013–14	Linn Oelker	LGE&E and KU
2014–15	Keith Porterfield	Georgia Systems Operations Corporation
2013–14	Andrew Pusztai	American Transmission Company
2013–14	Robert Rhodes	Southwest Power Pool, Inc.
2013–14	Steve Rueckert	Western Electricity Coordinating Council
2014–15	Ed Skiba	MISO
2014–15	Joe Tarantino	Sacramento Municipal Utilities District
2013–14	Guy V. Zito	Northeast Power Coordinating Council, Inc.
N/A	Monica Benson (NERC Standards Advisor)	NERC
N/A	Erika Chanzes (NERC Standards Advisor)	NERC
N/A	Stacey Tyrewalla (NERC Legal Advisor)	NERC

Version	Date	Description
1.0	02/13/14	Initial posting
2.0	05/19/14	Added B. Buckley, R. Crissman, B. Hampton, L. Jones, and E. Skiba. Removed B. Walker (NERC).
3.0	06/03/14	Added terms

Standards Committee Process Subcommittee

Activity Status Overview – June 2014

Projects Approaching Close	Status	Team Lead and Members
Consolidate SC Resource Documents **(Phase 1 of Updating the Drafting Team Guidelines Completed)** **(This task also satisfies Task #5 from the 2014–2016 SC Strategic Work Plan)**	**Task Initiated: July 2012** **Current Target Completion: April 2014 SC Meeting (Complete) and July 2014 SC Meeting** The SC approved a finalized list of documents for retirement at the April 9 SC meeting, and the documents have been archived. Since, M. Benson has compiled a "Resource Package" that accompanies the Drafting Team Reference Manual. This will be circulated to the SCPS for review prior submitting for the July SC meeting.	**Guy Zito**; gzito@npcc.org Linn Oelker; linn.oelker@lge-ku.com Monica Benson (NERC); monica.benson@nerc.net
Modify SC Quality Review Process	**Task Initiated: October 2012; Revisited December 2013** **Current Target Completion: July SC meeting** During its April 23 call, the SCPS reviewed the write-up by the task group that proposes that the NERC Coordination QR document can replace the QR process/template, provided that NERC staff commits to communicating the steps that were taken for QR prior to an initial posting. The SCPS agreed that the next step is to take this proposal to the SC. S. Miller will also loop in PMOS about adding QR to the project tracking spreadsheet. L. Lee is following up on these steps.	**Keith Porterfield**; keith.porterfield@gasoc.com Andy Pusztai; apusztai@atcllc.com Ed Skiba; eskiba@misoenergy.org Pete Heidrich; pheidrich@frcc.com Guy Zito; gzito@npcc.org Brenda Hampton; Brenda.Hampton@energyfutureholdings.com Brian Murphy; Brian.J.Murphy@fpl.com Steve Noess (NERC); steven.noess@nerc.net Erika Chanzes (NERC); erika.chanzes@nerc.net Stacey Tyrewala (NERC); stacey.tyrewala@nerc.net
Develop Work Plan **(Task #6 from 2013–2015 SC Strategic Work Plan)**	**Task Initiated: December 2013** **Current Target Completion: July 2014 SC Meeting** The SCPS has fleshed out activities that did not have full consensus with NERC staff and will finalize the Work Plan during the June SCPS meeting to bring to the July SC meeting. In addition, work on the 2015 Work Plan will be added to the 2014 Work Plan.	**Ben Li**; ben@benli.ca Erika Chanzes (NERC); erika.chanzes@nerc.net

Active Projects	Status	Team Lead and Members
Charter Revisions	**Task Initiated: December 2013** **Current Target Completion: TBD** B. Li has drafted revisions to the SCPS Charter to include a communication piece, the role of the SCPS in training, and officer elections. Per S. Miller's effort to align the SCPS and PMOS Charters, he has been researching how other NERC subcommittee charters are handled. This information and a proposal is currently being shared with the SCPS chairs and B. Li, and will be further discussed with the entire SCPS, PMOS, and NERC staff.	**Ben Li;** ben@benli.ca Guy Zito; gzito@npcc.org Pete Heidrich; pheidrich@frcc.com Scott Miller; smiller@meagpower.org Erika Chanzes (NERC); erika.chanzes@nerc.net
CEAP Pilot **(Initial project pilots completed)**	**Task Initiated: April 2012** **Current Target Completion: December 2014 SC Meeting** The finalized Disturbance Monitoring CEAP report was endorsed by the SC for posting during the April SC meeting. The CEAP team is meeting at FRCC June 3–4 to discuss project selection criteria and how to best apply CEAP moving forward.	**Guy Zito**; gzito@npcc.org Pete Heidrich; pheidrich@frcc.com Andy Pusztai; apusztai@atcllc.com Steven Rueckert; steve@wecc.biz Laura Hussey (laura.hussey@nerc.net) is now NERC staff support. Additional committee resources and NERC resources needed.
Consensus Building for SAR Development	**Task Initiated: October 2012; Re-scoped March 2014** **Current Target Completion: Early 2015** The task group met with NERC staff and agreed on the scope with minor changes. The SCPS agreed to the scope as well during the May 22 SCPS call, and B. Li has submitted the scope document and one-pager for the SC to endorse at the June SC meeting.	**Ben Li;** ben@benli.ca Pete Heidrich; pheidrich@frcc.com Steven Rueckert; steve@wecc.biz Guy Zito; gzito@npcc.org Erika Chanzes (NERC); erika.chanzes@nerc.net

Ongoing Projects / On the Horizon	Status	Team Lead and Members
Develop a Process to Improve the Effectiveness of Balloting	**Task Initiated: December 2013** **Current Target Completion: Ongoing / TBD** L. Lee has composed and provided an informational report to the SC for the June SC meeting to include NERC strategies for addressing issues with achieving quorum (what's been done in the past and is being done currently, and SBS improvements). It also includes a proposal for how the SCPS will be working to evaluate the results of the SBS enhancements and continued interim steps.	**Laura Lee**; Laura.Lee@duke-energy.com Robert Rhodes; rrhodes@spp.org Pete Heidrich; pheidrich@frcc.com Steve Rueckert; steve@wecc.biz Brian Buckley; bsbuckley@tecoenergy.com Stacey Tyrewala (NERC); stacey.tyrewala@nerc.net Monica Benson (NERC); monica.benson@nerc.net
Improve Standards Development Processes and Procedures **(Task #2 from the 2013–2015 SC Strategic Work Plan)**	**Task Initiated: January 2013; On hold until early 2015** **Current Target Completion: TBD** During the May 22 SCPS call, J. Tarantino explained that the task group came to the conclusion that the SCPS should wait on this task until active projects and SPM revisions have further matured. In the interim, informal outreach will be conducted to continue to identify standard development process issues. Any identified issues should be communicated to J. Tarantino, L. Lee, and E. Chanzes to keep record of and respond to. A formal outreach plan to gather input on the standards development process will be formed during the first quarter of 2015 and implemented during the second quarter. This will hopefully converge with a more "steady state" of standards projects. The SCPS and NERC staff agreed to this plan with the current scope document. The scope document has been submitted to the SC for endorsement at their June meeting.	**Joe Tarantino**; joseph.tarantino@smud.org Brenda Hampton; Brenda.Hampton@energyfutureholdings.com Fred Plett; frederick.plett@state.ma.us Pete Heidrich; pheidrich@frcc.com Ed Skiba; eskiba@misoenergy.org Guy Zito; Guy Zito; gzito@npcc.org Erika Chanzes (NERC); erika.chanzes@nerc.net Stacey Tyrewala (NERC); stacey.tyrewala@nerc.net Jordan Mallory (NERC); Jordan.mallory@nerc.net

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Item 1C
Attachment A

Standards Committee Process Subcommittee

Scope

Purpose

The purpose of the Standards Committee Process Subcommittee (SCPS) is to develop, maintain and document processes and guidelines to aid the Standards Committee, Standards Drafting Teams, NERC staff and industry in developing clear, effective and enforceable Reliability Standards. It also works to ensure that the documents provide transparency to the industry to ensure understanding of the standard development process and to promote the efficient use of industry technical subject matter expertise.

The SCPS takes direction from the Standards Committee and collects information from all Standards Committee members to identify needed process improvements and modifications.

Activities

1. Ensure effectiveness of standard process documents and references.

2. Maintain a list of all the documents it has responsibility for and establishes a review cycle for each of the standards process documents, and conducts reviews of the documents at least once every three years.

3. Propose key subjects on standards development process documents and references, and coordinate with NERC staff to ensure effective communication of these subjects to the industry.

4. Provide technical support to NERC's Standard Development training activities.

5. Establish and maintain a work plan presenting individual tasks to Standards Committee for acceptance prior to active development.

6. Consensus proposals and recommendations will be presented to the Standards Committee for information or approval. When the SCPS cannot reach a consensus, majority and minority opinions may be presented to the Standards Committee for it to make the final decision.

Membership

1. SCPS membership and participation is open to SC members, observers and all interested parties.

2. Nominations for new members will be requested as needed.

Commented [A1]: New proposed language – Scott Miller

Commented [A2]: Reworded – Scott Miller

Commented [A3]: Reworded -- Scott Miller

3. The SCPS Chair and Vice Chair will provide the Standards Committee with a recommended slate of members for approval as needed.

4. The SC chair and vice chair may participate and support the SCPS as non-members.

5. Members will serve staggered two year terms with no term limits.

6. The SCPS size will be determined by the workload needs of the subcommittee.

7. A NERC staff member will be assigned as the non-voting Subcommittee Coordinator

Commented [A4]: Reworded – Scott Miller

Officers

The subcommittee chair and vice chair are appointed by the chair of the NERC Standards Committee for one two-year term. The vice chair should be available to succeed to the chair.

Commented [A5]: This is the primary approach used by the other Standing committee subgroups. – Scott Miller

OR

- The SCPS will have a Chair and Vice Chair that are elected by the SCPS and approved by the Standards Committee.
- At least one officer must also be a member of the SC.
- Officers will serve 2 year terms with no limits on terms.
- Officers shall recommend the members of the SCPS for approval by the SC
- Officers will prepare meeting agendas and manage SCPS meetings

Officer Selection

Prior to the annual election of SCPS members in odd numbered years, the members of the SCPS shall select a chair and vice chair from among its membership by majority vote of the members of the SCPS. A nominating committee consisting of three (3) members of existing SCPS members shall be formed to solicit nominations for chair and vice chair no less than 30 days prior to the election.

The SCPS officer election shall be conducted at the 3rd quarter SCPS meeting. The nominating committee shall provide to the SCPS members the qualifications of the chair and vice chair nominees proposed. Also, at the time of the election, the Subcommittee can accept nominations from the floor. Following the election, the successful candidates shall be presented to the SC for approval.

Commented [A6]: As currently proposed by B. Li in the new SCPS Scope – Scott Miller

Reporting

1. The SCPS reports and is accountable to the Standards Committee and this Scope is subject to Standards Committee approval.

2. The SCPS will report on its activities at regularly scheduled Standards Committee meetings and calls and between meetings as requested.

Commented [A7]: Reworked and reworded based on the other Standing Committee Scope language – Scott Miller

Meetings

1. The SCPS will generally follow the approach used by the Standards Committee.

2. Four to six open meetings per year, or as needed. Emphasis will be given to conference calls and web-based meetings.

Commented [A8]: This is specifically stated in other standing committee Scope – Scott Miller

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Item 1c
Attachment B

Project Management and Oversight Subcommittee

Scope

Approved by the Standards Committee December 12, 2013

Purpose

The Project Management and Oversight Subcommittee (Subcommittee) works closely with NERC staff and the standards drafting teams (SDTs) to aggressively manage the timely development and maintenance of a comprehensive set of world-class, results-based Reliability Standards. The Subcommittee reports to the full Standards Committee (SC).

Activities

The Subcommittee shall have, at a minimum, the following duties:

1) Work closely with NERC staff, and the SDTs to establish milestones and deadlines for all SC work activities relating to reliability standard development, up to and including BOT approval;

   a) Assist NERC Staff and SDTs with the development of an initial project schedule for approval by the SC as referenced in Standard Processes Manual Section 4.4.1; and

   b) Actively monitor and assist NERC staff in the oversight of SDT milestones and deadlines; and extend or expedite milestones and deadlines, as appropriate; and

   c) Work with NERC staff to develop and refine project management tools; such as dashboards, project charting for tracking projects and communicating the status of projects including the reasons for and plans to address any schedule deviations; and

   d) Track the status of all existing and pending Reliability Standards, including when a Reliability Standard is considered completed (i.e., is Results-based, and has had P81 concepts applied).

2) Work with NERC staff to develop preliminary project timelines to set the expectation prior to the solicitation of SDT so that prospective members of an SDT can understand and

commit to meeting the project timeline, including milestones, at the time of their nomination and appointment.

3) Support all SAR drafting teams and SDTs by providing any specialized resources as may be needed to resolve issues and increase productivity and quality as needed to reach consensus and/or meet its milestones and deadlines;

   a) Assign PMOS liaisons for each active Standard development project who will provide oversight and support and maintain regular contact with the SDT Chair and NERC Standard Developer;

   b) Facilitate SAR drafting teams and SDTs' use of stakeholder technical experts and NERC technical, standing and regional committees for consultation, comments and endorsement, as needed; and

   c) Work with the SC Chair, Vice Chair and NERC standards developer to ensure SAR drafting teams and SDTs use informal methods to actively gain consensus during both the informal development period, as well as during the formal project development period. These informal methods may include, but are not limited to, outreach to individual industry experts and trade associations, webinars and workshops.

Membership

1. Subcommittee membership is open to SC members and other interested parties.
2. The SC Chair and Vice Chair will participate in and support the Subcommittee as non-members.
3. Subcommittee members will serve two-year terms with no term limits.
4. Nominations for new members, will be requested at least every two years, or as needed to add or replace members.
5. Subcommittee members shall be selected by the Subcommittee Officers.
6. The Subcommittee size will be determined by the workload and needs of the Subcommittee.
7. A NERC staff member will be assigned as the non-voting Subcommittee Coordinator

Commented [A1]: Reworded – Scott Miller

Officers

1. The subcommittee chair and vice chair are appointed by the chair of the NERC Standards Committee for one two-year term. The vice chair should be available to succeed to the chair.

OR

The subcommittee chair and vice chare are elected by the NERC Standards Committee for one two-year term.

2. The Subcommittee Chair or Vice Chair will set the agenda and preside over the meetings and calls.

Reporting

1. The Subcommittee is accountable to the full SC and will report jointly with NERC staff on the status of all SDT activities and any issues at regularly scheduled SC meetings and calls.
2. The Subcommittee is accountable to the full SC and will report jointly with NERC staff on the status of all SDT activities and any issues at regularly scheduled SC meetings and calls.

Meetings

1. The SCPS will generally follow the approach used by the Standards Committee.
2. Four to six open meetings per year, or as needed. Emphasis will be given to conference calls and web-based meetings.
3. Members of the Subcommittee may not send a proxy.
4. Subcommittee meetings are open to any and all observers.

Commented [A2]: This is the primary approach used by the other Standing committee subgroups. – Scott Miller

Commented [A3]: This is the method currently used to select the PMOS chair and vice chair. – Scott Miller

Commented [A4]: This is specifically stated in other standing committee Scope – Scott Miller

NERC Quality Review

[SUGGESTED SC ACTION -- FOR SCPS CONSIDERATION AND DISCUSSION]

Action

Endorse the NERC Coordinating Quality Review document, accompanied by a commitment by NERC staff to communicate to the Standards Committee (SC) the Quality Review (QR) steps taken prior to each draft Reliability Standard's initial formal posting. These items would replace the NERC Reliability Standards Quality Review Process that was approved by the SC but has not yet been implemented.

Background

Following SC approval in September 2013 of the SC Process Subcommittee (SCPS)-proposed NERC Reliability Standards Quality Review Process and Revised Template for Quality Review of NERC Reliability Standard or Interpretation documents, NERC staff expressed concern regarding the ERO operational governance provisions stipulated in the process document. Since, the SCPS, the SC Chair and Vice Chair, members of PMOS, and NERC staff have engaged in discussion to reach consensus on the documentation of NERC QR attributes and procedures.

As a result, NERC staff drafted an informational document titled "Coordinating Quality Review," which outlines several attributes that NERC standards staff currently use in executing its obligation under the NERC Standards Process Manual (SPM) to coordinate QR of draft Reliability Standards. All parties agreed that this document is consistent with the principles relating to QR established in the SC Charter, the SPM, and the Revised Template for Quality Review of NERC Reliability Standard or Interpretation. It is noted that the Coordinating Quality Review document references the template as an excellent tool to facilitate a review.

To account for the needs and limitations of the respective groups, discussions led to a compromise between the SCPS and NERC staff that identifies the Coordinating Quality Review document as an appropriate replacement to the process document with respect to the fact that it accurately qualifies what QR should consist of but does not mandate NERC operational procedures. It was also agreed that this document should be coupled with a commitment from NERC staff to communicate to the SC what specific QR steps were conducted for a draft Reliability Standard when it is submitted to the SC for approval of its initial posting.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Item 1D
Attachment B

Coordinating Quality Review

March 1, 2014

This informational document outlines several attributes that NERC Reliability Standards Staff ("Standards Staff") currently use in executing its obligation under the NERC Standards Processes Manual[1] ("SPM") to coordinate Quality Review ("QR") of draft Reliability Standards.

As specified in section 3.5 of the SPM, "NERC Reliability Standards Staff works to ensure the integrity of the Reliability Standards processes and *consistency of quality and completeness* of the Reliability Standards." (Emphasis added). Section 4.6 of the SPM addresses "Quality Review," and it specifies that "NERC Reliability Standards Staff shall *coordinate a quality review* of the Reliability Standard, implementation plan, and VRFs and VSLs *in parallel with the development* of the Reliability Standard and implementation plan, to assess whether the documents are within the scope of the associated SAR, whether the Reliability Standard is clear and enforceable as written, and whether the Reliability Standard meets the criteria specified in NERC's Benchmarks for Excellent Standards and criteria for governmental approval of Reliability Standards." (Emphasis added).

Standards Staff continues to work collaboratively with stakeholders and Standards Committee ("SC") [2] in our equal interest to ensure the highest level of quality. Specifically, the following attributes guide Standards Staff in its coordination of QR:

1. QR is part of the fabric of standards development activities, from project inception through completion, with a focus on quality.
2. QR must be flexible; it must support and not detract from, hinder, or delay the development process.
3. QR input provides important feedback to drafting teams and will be made available to them for consideration in a timely manner before posting.
4. Each NERC Director of Standards Development will work with their associated Standards Developers to coordinate a collaborative QR. The QR scope will consider the facts, circumstances, and complexity associated with each project. This may include group calls, meetings, or email reviews with industry participants.

[1] http://www.nerc.com/pa/Stand/Documents/Appendix_3A_StandardsProcessesManual.pdf

[2] The SC charter similarly acknowledges the importance of quality in accomplishing these common goals. For example, an SC duty under the charter is to establish quality assurance and quality control processes, recognizing the important role of the SC under the SPM in accepting the work of drafting teams.

5. Each project has a primary and secondary standards developer, increasing support for QR throughout the standards development process. Standards Staff also coordinates input from NERC Technical, Compliance, Legal, and Enforcement staffs, further enhancing QR.
6. The template for use in QRs created by the SC Process Subcommittee is an excellent tool for assessing the attributes of quality, and Standards Staff will continue review the items from this template in coordinating QR.
7. Outside input (a.k.a. using "fresh eyes") from individuals not directly connected to the drafting team is important, and Standards Staff is committed to continuing to use and incorporate such input.
8. QR will seek diversity of perspectives, to include NERC, regional, or industry technical, compliance, enforcement, and/or legal expertise.
9. The SC Project Management Oversight Subcommittee ("PMOS") has assigned a liaison for each standard development project. Standards Staff and drafting teams work closely with the PMOS liaison as an additional source of input to support QR.
10. QR efforts will include consideration of Paragraph 81 criteria and assessment of the content and quality criteria from the 2013 Independent Experts Review Panel[3].
11. Standards Staff is committed to ensuring that any QR process considers the full spectrum of quality. Key topics include, but are not limited to, the following:
    a. Does the requirement (and any associated attachments) meet results-based criteria? Namely, does it identify "Who" (functional entity), under what conditions (if any), shall perform what action (including the word "shall"), to achieve what particular result or outcome (that reduces a stated risk to the reliability of the bulk power system)?
    b. Is the requirement stated with sufficient detail and in a clear and concise manner without using ambiguous words or unnecessary explanatory information?
    c. Does the standard satisfy applicable regulatory directives?
    d. If a specific performance can't be identified, is the acceptable performance qualified and bounded by measurable conditions/parameters?
    e. Quality of Measures.
    f. VRF and VSL consistency with guidelines.
    g. Consistency of the standard with the Standard Authorization Request (SAR).
    h. Resolution of relevant Interpretations or Compliance Application Notices (CANs).
    i. Consistency with the Ten Benchmarks of Excellent Reliability Standards[4].

[3] http://www.nerc.com/pa/Stand/Standards%20Development%20Plan%20Library/Standards_Independent_Experts_Review_Project_Report.pdf

[4] http://www.nerc.com/files/10_Benchmarks_of_Excellent_Reliability_Standards.pdf

Standards Committee Strategic Work Plan 2013-2015, Task No. 2: Review of the Standards Processes and Procedures

Action
Endorse.

Background
Task No. 2: Review of the Standards Processes and Procedures:
Implement revisions needed to NERC's Rules of Procedure/SMP and SC processes and procedures to enhance SC and SDT accountability to timely deliver high quality Reliability Standards and execute the Strategic Plan, including the completion of Standards Process Input Group (SPIG) recommendations. All revisions, creation or elimination of processes and procedures provisions shall be presented to the SC for adoption, prior to presenting to the NERC Board of Trustees (BOT) for approval.

Steps Taken to Date:
Two questionnaires were sent seeking feedback in the early part of 2013. The first questionnaire was sent to standards drafting teams to determine areas for improvement in the standard development process. Although a few suggestions were made regarding legal representation on the standard drafting teams, there were no substantive improvements identified for process improvement.

A second questionnaire was sent to a broader audience which focused on asking for a "single biggest issue" with all aspects of the standard development process. This also concluded with no centralized issue to be identified.

Future Plans for Action:
The Task #2 Team noted a limited number of NERC Projects that have been through the revision of the current Standard Process Manual; those that were completed under the new manual were either informal development or were expedited due to FERC directives (MODs, VARs, PER-005, GMD, and CIP-014). The task team felt that evaluating additional projects which undergo formal development with the current Process Manual would allow a more comprehensive review. Additionally, it was noted that polling industry at this time would be deemed problematic due to the number of Project postings.

The recommendation of the task group was unanimous; "keep the scoping document but postpone any actions". The group noted that an outreach plan other than a survey should be considered. The task team also makes the following suggestions: 1) standing committees be solicited for outreach options, and 2) include outreach for this task as an agenda topic during compliance workshops.

A proposed starting time for Task #2 is second quarter of 2015.

Date: May 22, 2014

Scope of NERC SCPS Project
Consensus Building for Standard Authorization Request (SAR) Development

Need for Project:

To develop a process which will facilitate the effective and efficient development of technical information and building of industry consensus leading to the Standards Committee's acceptance/approval of the SAR for proposed standard projects.

Project Scope Statement:

The objective of this task is to develop a new or revised process which will improve the effectiveness and efficiency of consensus building tasks for standard projects starting at or before the initial project proposal stage and continuing to the acceptance/approval of the SAR by the Standards Committee.

A standard project can be initiated by any one of the following means:

a. *Recommendation by the Reliability Issues Steering Committee (RISC) to address an emerging reliability risk/issue;*
b. *Compliance with, or a response to, directives by regulatory authorities or the NERC Board of Trustees;*
c. *A review/revision or need identified in the Standards Committee's Reliability Standards Development Plan (RSDP);*
d. *A request by industry participants through the submission of a SAR;*
e. *Input by a stakeholder into the Single Portal for a potential reliability related issue.*

This project will require a comprehensive review of the existing SAR and Informal development processes and proposing changes- , where appropriate, to improve effectiveness and efficiency in consensus building activities leading to the posting and acceptance/approval of the SAR. The project also will have to be fully coordinated with the RISC, PMOS and other SC activities and SCPS projects. The project is to be conducted in 2 stages.

<u>Stage 1</u> (March 2014 to September 2014)

Develop a revised process that covers the following key activities:

- *Collection of technical information needed to support the proposal for a standard project;*
- *Informal outreach and consensus building on the need and scope of the project;*
- *Drafting/revising the SAR to achieve clarity with sufficient technical information that supports the proposed purpose and scope of project;*
- *Posting of SAR and responding to public comments, and revising SAR to address industry comments;*
- *Consider conducting a Cost Impact Analysis (CIA) as outlined in the NERC Cost Effective Analysis Process Phase 1 to determine potential cost impacts of potential proposed solutions;*

- *Recommending acceptance/approval/rejection of the SAR to the SC with due consideration given to industry input.*

The role of the RISC throughout these activities should be considered and clearly stated as appropriate.

Stage 2 (Latter Part of 2014 to Early 2015)

Revise the Standard Processes Manual to incorporate pertinent elements of the revised process.

Resources:

A small team comprising of 4-5 SCPS members, 1-2 PMOS members and 1-2 NERC Standards and NERC Legal staff.

Stage 1 is expected to start in March 2014 ending September 2014; Stage 2 is expected to start in the latter part of 2014 in conjunction with other SPM changes following the completion of another SCPS task to improve the effectiveness and efficiency of standards development, including balloting.

Addressing Failure to Achieve Quorum in Balloting Standards

Action
Informational update only

Background
Development or modification of a Reliability Standard requires industry balloting of the new Standard or modification. Per the current Standards Process Manual ballot pool approval requires a quorum, which is established by at least 75% of the members of a ballot pool submitting a response in addition to a two-thirds majority of the weighted Segments votes being affirmative. Several ballots have recently experienced failure to achieve the required quorum by the end of the specified voting window, necessitating extension of the voting window. In light of the recent challenges in reaching quorum at the end of the announced voting window, the Standards Committee Process Subcommittee (SCPS) and NERC staff have been "exploring options to create and maintain an effective ballot pool and strategies to address situations where a quorum is not reached by the time a ballot period is scheduled to close." November 2013 SC Agenda item 13 (a) iii. This effort has coincided with development and implementation of the new Standards Balloting System (SBS). This update contains steps taken to date to facilitate reaching quorum in a timely manner, actions being taken on ballots using the original (current) balloting system, enhancements and features of the new Standards Balloting System that are anticipated to improve the reaching quorum, and future plans for analysis and action.

Steps Taken to Date
NERC Standards Information staff has taken the following actions in 2012 and 2013 to address identified challenges to gaining quorum for ballots.

1. The Registered Ballot Body (RBB) was reviewed for members with no activity on their voting records for one year or longer. Members were sent a letter, emailed and/or called. Non-responsive members were removed from the RBB. 41 members were contacted, with seven RBB members removed and nine proxy pool members removed. This review will be performed annually.
2. Segment 8 of the RBB (Small Electricity Users) was reviewed to ensure members were accurately registered.
3. A review of the RBB's Segment representation, as directed in the Appendix 3D Registered Ballot Body Criteria of the NERC Rules of Procedure was performed. Based on the registration responses, the RBB was reviewed and updated.
4. Members of ballot pools who are no longer able to vote due to company mergers were removed from ballot pools and from the RBB.
5. A comparison between RBB and ballot pools to remove members in older ballot pools that are no longer voting members was initiated.

Actions Currently Being Taken
Several actions are being taken with the current ballot pools to encourage reaching a quorum before the voting window closes. Some of these are interim measures necessary at least until projects are transitioned to the new SBS, at which time longer term management can be evaluated.

1. The cleanup of ballot pools mentioned above is continuing prior to the ballot start date. This includes consideration of the effects of company mergers and the comparison of ballot pool membership to the RBB.

2. A contractor has been working with Standards Information staff to perform queries on ballot pools from September 2013 to March 2014 for further analysis. A preliminary query was performed on Segment 10 (Regional Entities) and is being used to refine the specifications for future queries. NERC is developing the capability to perform the queries and will be using the results along with the SCPS members to inform future strategies.
3. Analysis of ballot pools that have been extended is being performed by NERC Standards Information staff. A table containing the balloted projects in 2014 is included.
4. NERC Standards Information staff is communicating to industry voters the importance of abstaining when ballot pools are joined and they do not intend to vote in a particular ballot. These communications included a "Balloting 101" email and reminders at the Standards and Compliance Workshop.
5. An annual review of the RBB's Segment representation will be performed.
6. Reminders are being sent to individuals who have not voted and/or others in their company near the end of a voting window if quorum has not been achieved. Standards Committee leadership has also been assisting with contacting ballot pool members and the Trades to encourage voting.

Potential Improvements in new Software Balloting System (SBS)

Certain enhancements and features that have been built into the new SBS are anticipated to generate improvement in reaching quorum, both during initialization of the system and on an ongoing basis. Examples include:

1. New registration will be required for accessing voting in the new system, improving the cleanup of the RBB.
2. Proxies can be designated until the close of the ballot voting window making voting more accessible. Currently proxy designation can only be accomplished during ballot pool formation.
3. The "My Ballot Activity" section provides a single page view to join, vote and designate proxies, making managing voting activities easier.
4. The Replacement Voter feature allows a voter representing a segment to exit the RBB and be replaced by a new voter who can assume voting activities in the ballot pools.

Future Plans for Analysis and Action

The SCPS and NERC Standards Information staff will monitor the results of both the management strategies being implemented and the enhancements contained in the new SBS. NERC Standards Information staff will also continue the analysis already initiated into the causes of difficulties in achieving quorum in ballot pools. Based on the information gathered, the SCPS and NERC Standards Information staff will evaluate whether additional measures are necessary. An initial list of strategies for consideration has been developed to serve as a starting point if the problem persists. This list is for consideration only and has not been evaluated for practicality or effectiveness.

Suggestions/Ideas

Consider changes to proxy process – allow for multiple proxies, associate proxies with RBB Registered Entity rather than each individual standard.

Ballot pool (or ballot body) members who demonstrate poor voting performance should be replaced if they miss a defined number of votes.

Put an expiration date on a ballot pool – if the pool expires it will have to be "reinitialized", or ballot pool members could be asked to confirm their intent to remain in the pool.

Look at lowering the quorum % to address lack of quorum due to "poor performance".

Allow multiple individuals from a Registered Entity to join the RBB according to their specialty and then only allow one to join the ballot pool (for example an operations person or a CIP person).

Draft agreement for RBB Members defining responsibilities.

Have voters voluntarily notify NERC when they join the ballot pool that in the event they fail to vote by the voting deadline that their vote should be recorded as an abstention.

Analysis of Issues Achieving a Quorum (Jan 1-May 22, 2014)

Project Name and Number	Standard	Ballot Type	Ballot Start Date	Ballot End Date	# of Days Extended
Project 2007-02 - Operating Personnel Communications Protocols	COM-002-4	Additional Ballot	01/22/14	02/04/14	2
Project 2008-12 - Coordinate Interchange Standards	Definitions	Additional Ballot	01/16/14	01/29/14	2
Project 2008-12 - Coordinate Interchange Standards	INT-004-3 and INT-010-2	Additional Ballot	01/10/14	01/22/14	0
Project 2010-01 - Training	PER-005-2	Additional Ballot	01/08/14	01/21/14	1
Project 2010-02 - Connecting Facilities to the Grid	FAC-001-2 and FAC-002-2	Initial Ballot	05/06/14	05/16/14	1
Project 2010-03 - Modeling Data (MOD B)	MOD-033-1	Additional Ballot	01/10/14	01/22/14	1
Project 2010-04 - Demand Data (MOD C)	MOD-031-1	Additional Ballot	04/01/14	04/14/14	2
Project 2010-05.1 - Protection System: Phase 1 (Misoperations)	PRC-004-3	Additional Ballot	02/21/14	03/11/14	6
Project 2012-13 - NUC - Nuclear Plant Interface Coordination	NUC-001-3	Initial Ballot	05/13/14	05/22/14	0
Project 2013-04 - Voltage and Reactive Control	VAR-002-3	Additional Ballot	04/04/14	04/16/14	2
Project 2014-04 - Physical Security	CIP-014-1	Initial Ballot	04/20/14	04/24/14	0

DRAFT SCPS 2014 Work Plan				
Task	**Scope of Task**	**Task Initiated**	**Target Completion**	**Status/Remarks**
1. Modification to SC Quality Review Process Document	Staff has suggested changes to the QR process document that was approved by the Standards Committee at its September 2013 meeting. The SCPS will review and implement the proposed changes, and seek the SC's approval of the revised QR process document to enable implementation of the QR process. **Placeholder for Link to Scope Document**	October 2012	May 2014 SC Meeting	Ongoing. A small team including reps from SCPS, PMOS and NERC staff to meet to collaborate on perspectives and develop a scope document to move forward with implementation.
2. Improving Consensus Building at the SAR stage	A draft document was developed in mid 2013. The document to be revised/refined pending finalization of the informal outreach process so that the improved SAR development process considers all activities leading to the formal development and posting of SARs for projects that are on or to be added to the RSDP. **Placeholder for Link to Scope Document**	October 2012 (Task revisited jointly with PMOS starting March 2014)	June 2014 SC Meeting	Task to be combined with consensus building proposal (currently led by PMOS)
3. Consolidate SC Resource Documents	There exist a number of resource documents some of which are being used by the Standards Committees and drafting teams while others are either not used or out of date. The SCPS thus will: a. Propose a list of documents to be retired, and	July 2012	April 2014 SC Meeting	Ongoing

DRAFT SCPS 2014 Work Plan				
Task	**Scope of Task**	**Task Initiated**	**Target Completion**	**Status/Remarks**
	b. Consolidate the remaining documents to arrive at a single or a set of standards resource documents that would serve to assist the SC and SDTs in discharging their respective tasks. c. Add in version control and template remaining documents **Placeholder for Link to Scope Document**		June 2014 SC Meeting June 2014 SC Meeting	
4. Improve standards development process (Assignment resulting from 2013 Strategic Work Plan – Task #2)	a. Review effectiveness of the revised Standard Processes Manual approved by the FERC in June 2013, and identify areas/changes that can further improve the efficiency and quality of standard development; b. Propose changes to the SPM as necessary, post for comments and finalize changes for balloting and BoT adoption. **Placeholder for Link to Scope Document**	January 2013	June SC Meeting December 2014 SC Meeting	Ongoing
5. CEAP Pilot Project	Conduct CEAP pilots: a. CEAP Subteam is conducting the CEA portion of the CEAP on the second project of the pilot. The Team will develop a report for the SC and the Industry. b. The CEAP Subteam will propose a list of	April 2012	March 2014 SC Meeting March 2014	Ongoing

DRAFT SCPS 2014 Work Plan				
Task	**Scope of Task**	**Task Initiated**	**Target Completion**	**Status/Remarks**
	standards development projects to conduct the CEAP on for 2014 and bring these to the SC and industry for approval and comment. c. Upon completion of the pilot, the current CEAP guideline document will be revised accordingly to reflect lessons learned during the pilot and to address potential "benefits" of standard projects. **Placeholder for Link to Scope Document**		SC Meeting December 2014 SC Meeting	
6. Managing FERC Remands of Interpretations	Develop a process to manage FERC remands of interpretations such that the original request for interpretation will be duly addressed. **Placeholder for Link to Scope Document**	June 2013	June 2014 SC Meeting	Ongoing
7. Process to improve the effectiveness of balloting	Develop a process aiming at: a. Maintain an effective ballot pool b. Managing situations where a quorum is not reached by the end of a ballot such that balloting can be conducted in the most effective and efficient manner. **Placeholder for Link to Scope Document**	December 2013	June 2014 SC Meeting September 2014 SC Meeting	Ongoing
8. Review SCPS Charter	Review current charter, and coordinate revisions with PMOS for consistent approach.	December 2013	April 2014 SC Meeting	Ongoing

DRAFT SCPS 2014 Work Plan				
Task	**Scope of Task**	**Task Initiated**	**Target Completion**	**Status/Remarks**
	Placeholder for Link to Scope Document			

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Project Management and Oversight Subcommittee (PMOS)

April 17, 2014 | 11:00 a.m. – 2:00 p.m. Eastern

NERC
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326

NERC Antitrust Compliance Guidelines and Public Announcement
Agenda Items

1. **Project Tracking Spreadsheet**
   a. NERC Staff update on addition of IERP column
      i. NERC Staff has begun populating the IERP column and it is posted on nerc.com.
2. **Project Liaisons Updates**
   a. The PMOS liaisons provided a brief update on progress of assigned projects.
3. **Discussion on PMOS Role in SDTs' Responses to Comments**
   a. The PMOS members attending the meeting agreed to maintain current PMOS liaison interaction.
   b. The PMOS liaisons will continue their roles in monitoring Response to Comments as well as participating in QR sessions.
4. **Review the SCPS Charter changes for possible PMOS Charter revisions**
   a. The PMOS members did not make any revisions at this time until further SCPS discussions.
5. **Review the RISC Triage Diagram**
   a. The SC Chair updated PMOS on the RISC Triage Diagram and will provide further updates at the next SC meeting.
6. **2014 Meeting Dates Beyond July**
   a. Removed the May 30, 2014 and July 2, 2014 conference calls from the NERC Standards Calendar and sent cancellation notices to the PMOS team
   b. June 10, 2014- 8:00a.m. - 12:00p.m. MT in Denver (Xcel) (in-person)
   c. September 30, 2014- 8:00a.m. - 12:00p.m. PT in Portland (BPA) (in-person)
7. **Adjourn**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Agenda
Project Management and Oversight Subcommittee (PMOS)

June 10, 2014 | 8:00 a.m. – 12:00 p.m. Mountain

Xcel Energy
1800 Larimer Street
Denver, CO 80202

Meeting Dial-in Information:
Phone: 1-866-740-1260 | Meeting Code: 1463851 | Security Code: 0610

Click Here: Webinar Access Link

NERC Antitrust Compliance Guidelines and Public Announcement

Agenda Items

1. **Project Tracking Spreadsheet Review**
   a. Discussion on Project Schedules
2. **Project Liaisons Updates**
   a. Provide brief update on progress of assigned projects
3. **Review Draft PMOS Scope to Attach to SC Charter**
4. **2014 Meeting Dates Beyond October**
5. **Adjourn**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Member Representatives Committee

May 6, 2014 | 1:00–5:00 p.m. Eastern

Hyatt Regency Philadelphia at Penn's Landing
201 South Columbus Blvd
Philadelphia, PA 19106
215-928-1234

Introductions and Chair's Remarks

NERC Antitrust Compliance Guidelines and Public Announcement*

Consent Agenda

1. **Minutes* — Approve**
   a. April 9, 2014 Conference Call
   b. February 5, 2014 Meeting
2. **Future Meetings***

Regular Agenda

3. **Recommended Slate of Stakeholder-based Members to the Reliability Issues Steering Committee (RISC)* — Endorse**
4. **Request for MRC Members to Serve on the Board of Trustees Nominating Committee***
5. **Responses to the Board's Request for Policy Input***
   a. Reliability Standard Audit Worksheet (RSAW) Review and Revision Process
   b. Risk-Based Registration Initiative
   c. Potential Alternative Funding Mechanism to Support Expanded Cyber Security Information Sharing and Capabilities
6. **Additional Policy Discussion from Board Committee Meetings***
   a. Finance and Audit Committee
   b. Compliance Committee
      i. Reliability Assurance Initiative (RAI) Update
   c. Standards Oversight and Technology Committee

i. Critical Infrastructure Protection (CIP) Version 5 Response to FERC Directives and Implementation Update

ii. Stage 2 Geomagnetic Disturbance (GMD) Standard

iii. Physical Security Standard

iv. TOP/IRO Response Update

v. ERO Enterprise IT Applications

d. Other

7. **2015 Business Plan and Budget***
8. **2014 Long-Term Reliability Assessment: Development Plan and MRC Input***
9. **Essential Reliability Services Whitepaper***
10. **Five-Year Performance Assessment***
11. **Regulatory Update***

***Background materials include**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda Item 1a

Draft Minutes
Member Representatives Committee Pre-Meeting Informational Session Conference Call and Webinar

April 9, 2014 | 11:00 a.m. Eastern

Introductions and Chair's Remarks

Chair John Anderson, with vice chair Sylvain Clermont present, convened a duly-noticed open meeting by conference call and webinar of the North American Electric Reliability Corporation (NERC) Member Representatives Committee (MRC) on April 9, 2014 at 11:02 a.m., Eastern. The meeting provided the MRC and other stakeholders an opportunity to preview proposed agenda topics for the MRC Board of Trustees (Board) and Board committee meetings scheduled to be held May 6-7, 2014 in Philadelphia, PA. The meeting announcement, agenda, and list of attendees are attached as **Exhibits A, B, and C**, respectively.

NERC Antitrust Compliance Guidelines and Public Meeting Notice

Kristin Iwanechko, committee secretary, directed the participants' attention to the NERC Antitrust Compliance Guidelines and the public meeting notice included in the agenda.

Schedule of Quarterly NERC Meetings and Conference Calls

The draft schedule of events for the upcoming meetings in Philadelphia was included in the agenda package for today's meeting. The MRC meeting is scheduled to begin at 1:00 p.m. on May 6.

Policy Input Reminder

Mr. Anderson announced that the Board's request for policy input is scheduled to be released today and responses are due by Tuesday, April 29 to Kristin Iwanechko, committee secretary. The topics included in the policy input letter are:

- Reliability Standard Audit Worksheet (RSAW) review and revision process;
- Risk-based registration assessment; and
- Potential alternative funding mechanism to support expanded cyber security information sharing and capabilities.

Review of Proposed Board and Board Committees' Meeting Agenda Items

Mark Rossi noted that the preliminary agenda items for the Board of Trustees and Board committee meetings scheduled for May 6-7 in Philadelphia are identified in the slide presentation included in the agenda package for today's call (**Exhibit D**). He also noted that the Board is considering scheduling a meeting on April 23 to understand the plan for the physical security standard and the potential path to closure for the standard by the June 5, 2014 filing deadline. Mr. Anderson encouraged MRC members to review all agenda materials for the Board and Board committee meetings, once posted and available

on April 21, and attend as many of these meetings as possible, in advance of the MRC's meeting on May 6.

Review of Proposed MRC Agenda Items for May 6

Mr. Anderson noted that the preliminary MRC agenda items for the upcoming May 6 meeting in Philadelphia are identified in the slide presentation included in the agenda package for today's call (**Exhibit D**). Topics include:

- Endorsement of a recommended slate of members for the Reliability Issues Steering Committee;
- Request for MRC members to serve on the Board nominating committee;
- Discussion of the responses submitted to the policy input request from the Board;
- Additional discussion of the issues presented at the Board committee meetings on May 6;
- Discussion on the 2015 business plan and budget;
- Plan for the 2014 long-term reliability assessment and emerging issues;
- Whitepaper for the Essential Reliability Services Task Force; and
- Update on the five-year performance assessment.

Informational Items

NERC staff provided updates on the following topics: Reliability Assurance Initiative (RAI) progress; critical infrastructure protection (CIP) version 5 implementation study; physical security standard project; 2015 business plan and budget and stakeholder input tracking; operating personnel communication protocols standard development; definition of bulk electric system; and the ERO Enterprise operating model.

Proxy Reminder

Proxy notifications for the May 6 meetings must be submitted in writing to Kristin Iwanechko, committee secretary.

Meeting Adjourned

There being no further business, the call was terminated at 12:42 p.m., Eastern.

Submitted by,

Kristin Iwanechko
Secretary

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda Item 1b

Draft Minutes
Member Representatives Committee

February 5, 2014 | 1:00–5:00 p.m. Mountain

Arizona Grand Resort & Spa
8000 S. Arizona Grand Parkway
Phoenix, AZ 85044
602-659-6356

Outgoing Chair Carol Chinn, with incoming Chair John Anderson and incoming Vice Chair Sylvain Clermont present, called to order the North American Electric Reliability Corporation (NERC) Member Representatives Committee (MRC) meeting on February 5, 2014, at 1:00 p.m., Mountain. The meeting announcement, agenda, and list of attendees are attached as **Exhibits A**, **B** and **C**, respectively.

Introductions and Chair's Remarks

Mr. Anderson welcomed attendees and acknowledged the attendance of FERC staff, the NERC Board of Trustees (Board), Ken Quesnelle of the Canadian Association of Members of Public Utility Tribunals, and State Commissioners Asim Haque and David Clark. Mr. Anderson recognized the MRC responses to the January 8, 2013 policy input request from Fred Gorbet, chairman of the Board. He reminded attendees that full presentations were conducted at the committee meetings and will not be repeated during the MRC meeting.

NERC Antitrust Compliance Guidelines and Public Announcement

Kristin Iwanechko, committee secretary, called attention to the NERC antitrust compliance guidelines and the public meeting notice. Any questions should be addressed to NERC's general counsel, Charles Berardesco.

Ms. Iwanechko declared a quorum present with the following recognized proxies:

- Barry Lawson for Michael L. Smith – Cooperative Utility
- Ayesha Sabouba for Lam Chung – Federal/Provincial
- Martin Huang for Mike Penstone – Federal/Provincial
- Marion Lucas for Thomas Gianneschi – Large End-Use Electricity Customer
- Charles Acquard for Lawrence Nordell – Small End-Use Electricity Customer
- Asim Haque for Todd A. Snitchler – State Government

Minutes

The MRC approved, on a motion by Scott Helyer and seconded by Bruce Campbell, the draft minutes of its January 8, 2014 conference call and the draft minutes of its November 6, 2013 meeting in Atlanta (**Exhibits D** and **E**, respectively).

Election, Board of Trustees

Dave Goulding, chair of the Board's Nominating Committee, provided a report and recommendation for the election of four Board members for the class of 2017. The MRC approved, on a motion by Steve Whitley and seconded by Bill Gallagher, the re-election of Paul Barber, Janice Case, Fred Gorbet, and Roy Thilly for the class of 2017.

Mr. Goulding also noted that there have been questions regarding whether there should be more specific criteria for the nomination of Board members. Any comments should be provided to the next nominating committee.

Request for MRC Members to Serve on Nominating Committee for RISC Membership

Bob Schaffeld, chair of the Reliability Issues Steering Committee (RISC), noted that the RISC charter states that the Board and MRC would form a nominating committee to solicit a pool of candidates for membership in the RISC, and recommend a slate of members to the RISC for the Board's approval at the May meeting. Mr. Anderson asked for volunteers from the MRC interested in serving on the nominating committee or as a member of the RISC.

Mr. Schaffeld also noted that he would be asking the Board to approve the RISC's review of its charter and MRC input would be requested through the charter review process.

ERO Enterprise Three-Year Strategic Plan and 2014 Performance Metrics

Mr. Anderson reminded the MRC of the discussion on this item during the Corporate Governance and Human Resources Committee (CGHRC). Gerry Cauley, president and chief executive officer of NERC, noted that the metrics are an effort to define quantitative and measurable performance measures for the organization that will help drive the desired performance and outcomes. He highlighted the following takeaways on the metrics from the morning discussion and suggested to bring revised metrics to the CGHRC for approval during its March conference call:

1. The metric on Bulk Power System (BPS) outages should be better quantified.
2. The first metric should be reconciled with the comments submitted by the Standards Committee, and supported by many others, in response to the policy input letter.
3. The list of metrics regarding specific reliability risk initiatives should be revised to have more tangible and quantifiable outcomes.

Mr. Cauley suggested that the strategic plan be approved at the February meeting, recognizing that it will continue to be worked on based on inputs received. He recognized the collaborative effort with the Regional Executives and noted that it is an improvement from past strategic plans. He also proposed to create an accountability matrix to identify how comments are being considered and

addressed, and present the matrix at the May meetings. Mr. Cauley recognized that one of the challenges is showing clear prioritization and cost efficiencies.

Attendees shared comments related to this update:

- Many noted that a well-defined de-registration process should be identified in the strategic plan.
- Some MRC members are concerned over the interchangeable use of Bulk Power System and Bulk Electric System and requested that all instances in the strategic plan refer to the same term.
- An MRC member asked about the meaning of 'threshold' and 'target' and what is the unacceptable level. Mr. Cauley clarified that not meeting the threshold is the unacceptable level and partial credit is given for anything between threshold and target.
- NERC is urged to ensure transparency of the accountability matrix with industry.

2015 Business Plan and Budget Schedule

Mike Walker, senior vice president and chief financial and administrative officer at NERC, reported that a concerted effort is being made early in the process in coordination with the Regional Entities to draft the Business Plans and Budgets in a way to show a better linkage between the activities being undertaken to the strategic plan and the priorities set forth in the plan. He noted that there is a discussion on roles and responsibilities between NERC and the regions, with a clearer allocation of resources to accomplish the items set forth in the plan. There will also be a very clear focus on costs at the regional and NERC levels and a focus on forecasting capabilities.

Further, Mr. Walker highlighted the following changes to the schedule:

- More opportunities for input prior to posting the initial draft.
- Posting will be delayed to May 16, 2014, to provide more time for review and provide a complete picture so stakeholders are in a better position to provide informed feedback.
- Increased the time provided for comment on the initial draft to 45 days.

Many MRC members believe this schedule is a significant improvement from past schedules.

Responses to the Board's Request for Policy Input

Mr. Anderson acknowledged the MRC's responses to Fred Gorbet's January 8, 2014 letter requesting policy input on the operating personnel communication protocols standard development, 2014-2017 ERO Enterprise Strategic Plan and 2015 Business Plan and Budget Schedule, and critical infrastructure protection (CIP) Version 5 Order 791 Response Plan. The discussion on the 2014-2017 ERO Enterprise Strategic Plan and 2015 Business Plan and Budget Schedule took place during the previous agenda item. The following comments on the other two policy input topics are not all inclusive, but provide the general tenor and scope of the discussion:

Operating Personnel Communication Protocols Standard Development

- Some MRC members recommended that the applicability of COM-002-4 to the Distribution Provider function be restricted the same way as in the Version 4 and 5 Critical Infrastructure Protection standards.
- Fred Gorbet reiterated that this standard has been an important issue for the Board and they are pleased with the current status of the standard. He noted that if the standard drafting team determines that changes are needed in response to comments, the process should run its course.

Critical Infrastructure Protection (CIP) Version 5 Order 791 Response Plan

- MRC members recognized that the Reliability Assurance Initiative (RAI) is intended to be broad enough to cover all Reliability Standards, but one member suggested that there may be an opportunity with the CIP Version 5 standards to have a practical test on how RAI would be applied in place of the "identify, assess, and correct" language.
- Gerry Cauley noted that NERC recognizes the need for clarity and certainty on the transition and the need to demonstrate what success looks like with respect to RAI.
- Some MRC members are concerned that there will not be a clear enough understanding of RAI by the time the CIP standards are balloted.
- In response to questions from MRC members, it was clarified that the reference to the C2M2 model is meant only as a possible tool for industry to use and is not required for compliance.

Additional Policy Discussion from Board Committee Meetings

Attendees shared comments in response to the discussions from the Board committee meetings:

Finance and Audit Committee

- MRC members support the 2015 Business Plan and Budget schedule.
- A tentative meeting is scheduled with the MRC Business Plan and Budget Input Group in April and the group welcomes any comments in advance of that meeting.

Standards Oversight and Technology Committee

- MRC members suggested developing a process for revisions to Reliability Standard Audit Worksheets (RSAW) to be posted for industry comment and if adverse comments are submitted, the RSAW could be submitted to a Board committee for review.
- A small sub-group was formed with representation from the MRC, NERC staff, and the NERC Board to develop a proposal for an RSAW revision process to be presented at the May meetings. The scope of the sub-group is for revisions made, after a standard has been approved, to RSAWs that were posted concurrently with the standard.

- MRC members asked that the sub-group consider the effective date of RSAW changes and whether they would be applied retroactively or prospectively.
- Some MRC members are concerned that standards may be interpreted differently amongst industry and suggested that the sub-group could evaluate options to address those types of questions.

Corporate Governance and Human Resources Committee

- For the MRC Assessment of Board of Trustees Effectiveness, an MRC member suggested having the ability to review or edit comments prior to submitting in future surveys.

Compliance Committee

- A great deal of progress has been made on RAI, but it may be useful to provide a case study and to define some of the commonly used terms.
- MRC members raised questions about whether the controls would be entity specific and changed over time. They also raised questions about the timing of the FFT triage process.

Risk-based Registration Assessment Project

Mr. Cauley provided some history on the development of the current registration criteria, noting that the current registration framework does not differentiate between entities that present different levels of risk. He noted that, overall, the desire is to get the scope of work and programs so they can be efficiently applied to get reliability benefit without creating excess burden. The objective of this initiative is to gain clarity on whether there is a better design that will allow scope to be tailored based on risk and to benefit reliability.

This initiative was introduced at the January MRC Informational Session. A survey was distributed to industry with responses due by February 28, 2014. The near-term objective is to develop a whitepaper to be presented at the May meeting, which would identify the issues and lay out a potential framework. At the November meetings, a final proposal and transition plan would be presented.

Attendees shared comments related to this update:

- Industry strongly supports this initiative and how to address smaller entities that have minimal, if any, impact on the BPS in order to determine actual vulnerability. It was recommended to define minimal impact.
- Some suggested changes to the compliance registry document include consistent use of BES, BPS, or greater than 100 kV, define terms that may be interpreted differently across the regions, and include a formal de-registration process.
- NERC is recommended to review the applicability in all Reliability Standards to ensure appropriate applicability.

- NERC is encouraged to ensure that this initiative does not become too complex and tie up too many resources.
- A suggestion was made to do a search on whether there are good risk models used in other industries that could be used with this initiative.

Definition of BES Implementation Discussion

Tom Burgess provided a brief overview of this item, specifically the three-step process of applying the definition, considering inclusions, and considering exclusions, and processes for making exception requests and self-notifications. He noted that it is a bright-line approach and the goal is to have a stable foundation of understanding what the BES elements are to know standard applicability, compliance, and other functions that are important to ensure reliability. NERC staff is working towards making several reference documents available in a common location to address questions that have been raised and to assist industry in the implementation.

Mr. Burgess noted that questions were raised during the MRC informational session regarding dispersed generation individual units and large end-use customers. He noted that a Standard Authorization Request has been received that is directed at helping to provide long term certainty around the applicability of standards in the dispersed generation setting. With respect to large end-use customers, additional information was provided about how the 50kV threshold came about and what the implications are in terms of considering either industrial facilities or other situations where there are radials connected by systems that are below 100 kV.

The transition from work underway to deployment and implementation will be completed by July 1, 2014. NERC staff is conducting significant outreach and will make information available on processes and tools to reach consistent and uniform determinations on BES elements. NERC and ERO staff will receive training to ensure there is a common perspective, and Registered Entities will receive training to provide a good understanding of how to use the various reference materials and tools. NERC staff expects to complete most of the training for ERO staff in March and expects to begin training for industry in April.

Mr. Burgess reminded industry that the new definition becomes effective on July 1, 2014, and newly identified elements need to be in compliance by July 1, 2016.

Attendees shared comments related to this update:

- NERC is urged to be very clear on the expectations of the process for reporting self-determinations, including the expectations of the Regional Entities. Further, clarification is needed regarding the compliance status of an element that a Registered Entity submits as an exclusion where the Regional Entity disagrees with that determination.
- Clarification was given that notifications are required for any newly identified elements as a result of the new definition. For situations where more information is needed about particular application of the definition, there are specific provisions in the various processes to handle

these and it is expected that Regional Entities will work with the Registered Entities to resolve questions.

- There are some entities that don't know NERC and may have facilities that will get swept in with the bright-line definition. If any of these entities become registered, applicability begins at the time of registration and not retroactively.
- Some stakeholders asked for clarity on when the two-year "clock" begins. Mr. Burgess clarified that the two-year clock begins on July 1, 2014, for newly identified elements.
- There may be situations where an element that was previously classified as a BES element is determined to be excluded under the new definition and there is a question regarding how granular the support for the excluded element would need to be. This information will be included in the reference documents and in the various training sessions.
- An MRC member noted that dispersed power producing resources are not determined to be BES unless they aggregate to over 75 MW.

Five-Year Performance Assessment Update

Rebecca Michael, associate general counsel at NERC, reported that with respect to the instant survey the number of responses doubled as compared to responses for the previous performance assessment report. For this second performance assessment report, the survey was issued first and there will be an opportunity for industry to provide comments on the report, which will be due in April. The draft report will be reviewed at the May MRC and Board meetings with the final report expected to be filed with FERC in July. Ms. Michael reported on the highest and lowest average scores with respect to various areas, the lowest averages for enforcement, registration and certification, reliability assessments, and critical infrastructure protection. She highlighted nine overarching themes that will be addressed in the report.

Regulatory Update

Charles Berardesco, senior vice president and general counsel at NERC, invited questions or comments regarding the regulatory report which highlights Canadian affairs as well as past and future significant FERC filings.

Future Meetings

The following are future dates for the MRC Pre-Meeting and Informational Sessions:

- July 16, 2014
- October 15, 2014

The following are future NERC Board and MRC meeting dates and locations:

- May 6-7, 2014 – Philadelphia, PA
- August 13-14, 2014 – Vancouver, Canada
- November 12-13, 2014 – Atlanta, GA

- February 11-12, 2015 – San Diego, CA
- May 6-7, 2015 – Pentagon City, VA
- August 12-13, 2015 – Toronto, Canada
- November 4-5, 2015 – Atlanta, GA

Adjournment

There being no further business, the meeting terminated at 4:36 p.m., Mountain.

Submitted by,

Kristin Iwanechko
Secretary

Agenda Item 2
MRC Meeting
May 6, 2014

Future Meetings

Action
Information

Summary
The following are the future meeting dates for 2014 and 2015. The dates for the 2014 Pre-Meeting and Informational Sessions conducted via conference call and webinar are also included below.

2014 Dates

July 16	Pre-Meeting and Informational Session
August 13-14	Vancouver, Canada
October 15	Pre-Meeting and Informational Session
November 12-13	Atlanta, GA

2015 Dates

February 11-12	San Diego, CA
May 6-7	Pentagon City, VA
August 12-13	Toronto, Canada
November 4-5	Atlanta, GA

Agenda Item 3
MRC Meeting
May 6, 2014

Recommended Slate of Stakeholder-based Members to the Reliability Issues Steering Committee

Action

Endorse slate of stakeholder-based members to serve on the Reliability Issues Steering Committee (RISC) for two-year terms.

Summary

The RISC charter states "In advance of their annual May meetings, the NERC Board and the MRC will form a nominating committee to solicit a pool of candidates… [a]t its May meeting each year, the MRC shall review and recommend to the Board a slate of stakeholder-based members to the RISC."

Pursuant to this language, a RISC nominating committee was formed, consisting of Sylvain Clermont, vice chair of the MRC; Gerry Cauley, president and CEO of NERC; Ken Peterson, chair of the Standards Oversight and Technology Committee; and Bob Schaffeld, chair of the RISC. Nominations were solicited in March 2014. The nominating committee reviewed a number of candidates and evaluated them based on general experience and qualifications, as well as diversity within the context of the entire membership of the RISC. The nominating committee recommends MRC endorsement of the following slate of stakeholder-based members to serve on the RISC for two-year terms ending May 2016.

Name	Title and Company
Daniel Froetscher, At-Large Member	Senior Vice President, Transmission, Distribution, and Customers, Arizona Public Service Company
Ray Gorman, At-Large Member	Chairman, New Brunswick Energy and Utilities Board
Scot Hathaway, At-Large Member	Vice President – Transmission, Dominion Virginia Power
Duane Highley, At-Large Member	President and CEO, Arkansas Electric Cooperative
Nabil Hitti, MRC Member	Vice President, Transmission Network Operations, National Grid
Steve Whitley, At-Large Member	President and CEO, New York ISO

Agenda Item 4
MRC Meeting
May 6, 2014

Request for MRC Members to Serve on the Board of Trustees Nominating Committee

Action

Request for MRC member volunteers to serve on the nominating committee for 2014.

Background

On May 6, 2014, Chair Anderson will ask the MRC for volunteers to serve on the Board of Trustees Nominating Committee (BOTNC) for 2014. The BOTNC will recommend nominees for election/re-election to the NERC Board of Trustees (Board) at the Member Representatives Committee meeting in February 2015. Janice Case will chair the BOTNC for 2014.

Agenda Item 5
MRC Meeting
May 6, 2014

Responses to the Board's Request for Policy Input

Action
Discussion

Background
The policy input letter is issued by the Chair of the NERC Board of Trustees (Board) four weeks in advance of the quarterly meetings and includes relevant materials necessary to inform discussion. Written input from the MRC and stakeholders is due one week before the meetings and is then revisited during a dedicated discussion time on the MRC's agenda, in the presence of the Board.

Status
On May 6, 2014, the MRC can expect to participate in further discussion of the responses received to the policy input request that was distributed on April 9, 2014.

Deadline for submitting policy input responses is **April 29, 2014** and should be sent to Kristin.Iwanechko@nerc.net

In addition to the information provided in the policy input letter on the Risk-Based Registration initiative, a supplemental update is also enclosed.

Enclosed Attachments
1. Risk-Based Registration Initiative Supplemental Update
2. April 9, 2014 Board's Letter Requesting Policy Input

Agenda Item 5
Attachment 1
MRC Meeting
May 6, 2014

Risk-Based Registration Initiative Supplemental Update

Action
Information

Background
NERC launched the Risk-Based Registration (RBR) initiative in 2014 to ensure that a common approach to identifying and evaluating risks to reliability is used consistently throughout the ERO Enterprise. NERC has always included risk evaluation as part of its programs, procedures and policies, and over the last seven years, the risk evaluation has become more formalized and mature. This initiative will address industry registration and reduced industry compliance burden, while supporting NERC and Regional Entities to: 1) identify who should be registered and who should not be registered - according to their risk to reliability; and 2) refine the criteria needed to make decisions to register and a basis to determine the appropriate sub-lists of applicable Reliability Standard requirements.

Summary
The registration program is the key to what triggers mandatory compliance by an entity with Reliability Standard requirements and associated compliance monitoring and enforcement activities. NERC believes that the ultimate end-state vision for the registration program should be to ensure the right entities are subject to the right set of applicable Reliability Standards, using a consistent approach to risk assessment and registration across the ERO Enterprise.

Formation of Advisory Group
In 2014, NERC established a RBR Advisory Group (RBRAG) to provide input and advice on the RBR design and implementation plan. The RBRAG is comprised of representatives from NERC staff, Regional Entity staff, and Federal Energy Regulatory Commission staff, along with U.S. and Canadian industry representatives.

Status Update
The RBRAG has met for two full-group discussion and planning meetings. During the in-person meeting on March 28, 2014, the RBRAG agreed that some functions should remain untouched, while others required enhancement. RBRAG divided into working sub-groups, each group focused on specific registered functions, to review potential elimination or threshold enhancements. These sub-groups met during the first week of April 2014, in order to frame problems, outline possible solutions, and refine the criteria needed to make decisions to register for those functions. Based on the proposals developed during the sub-group meetings, the RBRAG developed a draft white paper of proposed enhancements to the NERC Registration program. The draft white paper was included in the NERC request to the Member Representatives Committee (MRC) for policy input.

After discussion during the MRC Informational Session and at the MRC meeting in May, a draft design and implementation plan will be posted for public comment. Taking into account public

comments on these two documents, the RBRAG will complete enhancement of the design and implementation plan by mid-July, will post these documents for MRC policy input and present the products for discussion at the Board of Trustees Compliance Committee (BOTCC) and MRC meetings in August.

The design will incorporate evaluation of the risks and benefits provided by a given entity to ensure reliability, and will identify a corresponding properly tailored set of NERC Reliability Standard requirements for certain functional categories, as warranted. The design will also include an implementation plan supporting a 2016 or sooner launch, along with business practice and IT requirements, with the possibility of early adoption options. These options result in addressing industry burden, while preserving reliability of the Bulk Power System. The second stage will address any remaining non-design issues or issues requiring a longer lead-time.

Existing flexibility in the application of threshold criteria, the Functional Model categories and scaled sets of applicable Reliability Standards may provide opportunities for accelerated reform within the existing NERC Rules of Procedure (ROP). However, possible modifications to the ROP are being assessed and will be pursued as necessary.

The final versions of registration criteria, implementation plan, and any necessary ROP changes will be presented to the BOTCC and MRC in November with an anticipated filing date at the end of that month.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Fred W. Gorbet, Chair
Board of Trustees

Attachment 2

April 9, 2014

Mr. John A. Anderson, Chair
NERC Member Representatives Committee
c/o Electricity Consumers Resource Council
1111 19th Street, NW
Suite 700
Washington, DC 20036

Re: May 2014 Policy Input to NERC Board of Trustees

Dear John:

I would like to invite the Member Representatives Committee (MRC) to provide policy input on three issues of particular interest to the Board of Trustees (Board) as it prepares for the meetings on May 6-7, 2014, in Philadelphia, PA. We recognize many of those on the MRC are involved with numerous important NERC activities, including the development of the physical security standard, and would appreciate your thoughts on these additional matters of importance. Enclosed with this request is additional background information to help MRC members solicit inputs from their respective sectors. The three issues are:

Item 1: Reliability Standard Audit Worksheet (RSAW) Review and Revision Process
At the February MRC meeting, there was a discussion about developing a review and approval process for changes to RSAWs to ensure that a change does not materially change the scope or intent of a standard. A working group was formed with representation from the MRC, NERC staff, and the Board to develop a proposal to be presented at the May meetings. The working group developed a proposed process to vet proposed changes to an RSAW that is already in place for an existing standard (*see,* **Attachment A**). **The MRC is encouraged to provide feedback on the proposed process and, specifically, whether it addresses the concerns raised during the February meetings.**

Item 2: Risk-Based Registration Assessment
The April 9, 2014 MRC Informational Session agenda materials include an update on the Risk-Based Registration (RBR) Initiative launched in 2014 (*see* Agenda Item 4b). The RBR Initiative is assessing the current registration criteria and practices to ensure the right entities are subject to the right set of applicable Reliability Standards, using a consistent and common approach to risk assessment and registration across the ERO Enterprise. NERC has established a RBR Advisory Group (RBRAG) to provide input and advice for the RBR design and implementation plan. The RBRAG is comprised of representatives from NERC staff, Regional Entity staff, and Federal Energy Regulatory Commission staff, along with U.S.

and Canadian industry representatives. A whitepaper has been developed by the RBRAG to identify issues that need to be addressed in the ultimate design. **At this formative stage in the project, the MRC is encouraged to provide feedback on the draft whitepaper** (*see,* **Attachment B**), **specifically around the following questions:**

1. **The whitepaper sets out several objectives for this initiative. Do you agree with these objectives and are there any other considerations you would suggest?**
2. **Is the use of multiple thresholds, as discussed in the whitepaper, a prudent approach to determining whether an entity should be registered and do you believe this may cause any unintended consequences?**
3. **Are there any other considerations not identified in the whitepaper that you believe need to be factored into this initiative?**

The RBR design and implementation plan are targeted to be posted in late May 2014 for public comment. Further, based on the current plan, the Registration program redesign and implementation plan will be discussed at the MRC and Board committee meetings in May and August 2014, and approved at the Board's November 2014 meeting.

Item 3: Potential Alternative Funding Mechanism to Support Expanded Cyber Security Information Sharing and Capabilities

The Electricity Sector Information Sharing and Analysis Center (ES-ISAC) was formed in 1998 when the Secretary of Energy requested that NERC serve as the ISAC for the electricity sub-sector. ES-ISAC's primary function is the rapid and secure sharing of information with the electric industry and governmental entities regarding real and potential cyber-related threats to the electricity sector, as well as methods and tools to avoid or mitigate the potential impact from these threats.

During the final stages in the preparation of NERC's 2014 budget, a new opportunity was identified which would allow ES-ISAC to further improve its information sharing capability by participation alongside industry in a voluntary private sector funded cyber security communication and information sharing network. This project is known as the "Cyber Federated Model" (CFM) and "Cyber Risk Information Sharing Program" (CRISP), the purpose of which is to deliver a highly secure information sharing network utilized to identify, track and deploy fixes to emerging cyber security threats. It was initially funded by the Department of Energy, has been successfully piloted by several large investor owned utilities and is in the process of being transitioned to private-sector funding. NERC deferred a decision to participate in this program pending further investigation of the program structure and costs. Over the past six months NERC conducted further due diligence regarding both the structure and costs and believes there is merit in considering participation as part of NERC's upcoming draft 2015 business plan and budget. The primary value to NERC stakeholders of having ES-ISAC participation in CFM and CRISP is the ability to share additional timely information on threats and vulnerabilities with a broader segment of industry that is not directly participating in the program and therefore would not have access to this information. Issues and

trends discovered through CFM and CRISP participation would be shared without attribution. However, in light of the costs of participation in the program, which involves investments in hardware, additional secure communications capabilities and increased analytical resources and services, NERC is interested in exploring the potential for obtaining voluntarily direct funding from industry as a special project in order to mitigate assessment impacts from program participation. This would represent a new funding approach to a special reliability project which is designed to benefit the entire sector. **The Board requests input on this alternative funding approach.**

As a reminder, the full agenda packages for the Board, Board committees and MRC meetings will be available on April 21, 2014. I encourage the MRC to review the agenda materials for the May meetings, once available, and offer any additional input that is meaningful and timely to industry and stakeholders.

Written comments should be sent to Kristin Iwanechko, MRC Secretary (Kristin.Iwanechko@nerc.net) by **April 29, 2014** for the Board to review in advance of the meetings scheduled for Philadelphia.

Sincerely,

Fred W. Gorbet, Chair
NERC Board of Trustees

cc: NERC Board of Trustees
Member Representatives Committee

Reliability Standard Audit Worksheet (RSAW) Review and Revision Process

Objectives

There are several key principles that must be balanced in constructing the RSAW review process:

1. The RSAW is intended to be a tool to assist the ERO in conducting its audit field work and to enable a consistent approach throughout the ERO Enterprise.
2. The ERO is committed to making RSAWs publicly available to industry as part of the standards balloting process to provide a level of transparency about the compliance expectations for the standard.
3. The ERO must have the latitude to modify RSAWs as experience is gained in the field over time.
4. The purpose of the RSAW review process is to ensure that any proposed change to an RSAW does not effectuate a material change in the scope or intent of a standard.

Proposed Process

A simple process to achieve these objectives would be as follows. The process will be used to vet proposed changes to an RSAW that is already in place for an existing standard.

1. NERC will post any substantive revision to an RSAW for industry comment for a period of at least 15 business days before it becomes effective. The posting will state whether the changes are intended to apply to current open audits or only to audits commencing on or after the effective date. Comments should focus on whether industry believes the proposed changes to the RSAW are a material change in the scope of the standard, a technical error or a concern regarding the effective date.
2. NERC, along with the Regions, will review the comments and may propose additional revisions to the RSAW to address industry comments. If revisions are made, NERC will re-post the RSAW for industry comment for an additional 15 business days.
3. NERC will forward any remaining comments not accepted, along with its rationale, to the Chair of the Standards Oversight and Technology Committee (SOTC). The Chair of the SOTC will decide whether a review by the full SOTC is necessary and will take into consideration the following:
    a. Whether a technical error or inaccuracy is identified in the proposed change;
    b. the proposed change incorrectly expands what is required by the standard's requirements; or
    c. the effective date for the proposed changes increase compliance requirements retroactively.

4. The Chair of the SOTC will take one of the following actions:
    a. No action required. The RSAW will go into effect on its proposed effective date.
    b. Forward the proposed RSAW revisions for review by the full SOTC. The proposed revisions to the RSAW will not go into effect.
5. The SOTC will perform a similar review for any RSAW referred to it. NERC will implement the SOTC's findings as to whether additional changes to the RSAW are required or if the RSAW may go into effect as drafted.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

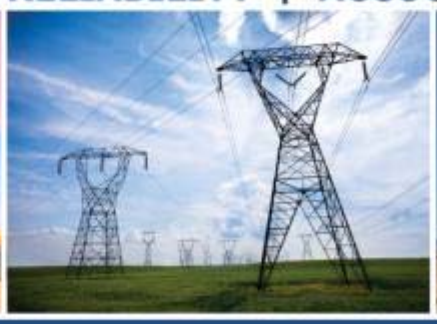
Attachment B

Risk-Based Registration

Draft White Paper

April 9, 2014

RELIABILITY | ACCOUNTABILITY



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface ii
Executive Summary 1
Introduction 3
Background 3
Purpose 3
Formation of an advisory group 4
Recommendations 5
Clarify terms and improve current procedures 5
Materiality 5
BES references 5
De-registration 5
NERC oversight and guidance on registration practices 5
One-time attestations 5
Establish a centralized review process 7
Entity risk assessment in a common registration form 7
New BES Definition as model and anchor for risk-based registration 9
Functional registration category elimination if not material to reliability 9
Synchronize threshold revisions with BES Definition and align with risk 8
Reliability Standards/compliance and monitoring/risk-based criteria 8
Status quo for other functional registration categories 8
Task forces for risk criteria and Reliability Standard applicability classes 8
Issues that require a longer time horizon 9
Appendix A – Risk-Based Registration Threshold Reviews ..... A-A
Purchasing-Selling Entity (PSE) ..... A-A
Interchange Authority/Interchange Coordinator (used interchangeably) (IA) ..... A-B
Distribution Provider (DP) A-4
Load-Serving Entity (LSE) A-9
Transmission Owner (TO) A-13
Transmission Operator (TOP) A-17
Generator Owner (GO) A-19
Generator Operator (GOP) A-22
Appendix B – Current State of Registration Program B-1
NERC's Role B-1
Regional Entity's Role B-1
Functional Model B-2
Thresholds B-2
Reliability Standard Applicability B-3
Registration Types B-3
Multi-Regional Registered Entity (MRRE) B-4
Appendix C – BES Definition C-1

Preface

This document sets forth recommendations for proposed enhancements to the North American Electric Reliability Corporation (NERC) Registration program for discussion purposes. Proposed changes to the NERC Statement of Registry Criteria[1] as outlined herein will not result in an automatic change to such functional categories in the Functional Model.[2]

Pursuant to the Energy Policy Act of 2005, NERC and the Federal Energy Regulatory Commission (FERC or Commission) have jurisdiction over users, owners and operators of the Bulk Power System (BPS). Section 215 of the Federal Power Act (FPA) defines BPS as the:

A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

B) electric energy from generation facilities needed to maintain transmission system reliability.

The term does not include facilities used in the local distribution of electric energy.

To date, FERC has not directly defined the limits of its jurisdiction under Section 215 of the FPA. However, FERC has recognized that users, owners and operators of the BPS are users, owners and operators of the Bulk Electric System (BES).[3] FERC recently approved NERC's new BES Definition.[4] Users, owners and operators of the BES are subject to compliance with NERC Reliability Standards. NERC's Registration program identifies specific entities that are responsible for compliance with NERC Reliability Standards.

Nothing in this document limits the jurisdictional authority of NERC and FERC pursuant to the Energy Policy Act of 2005 and Section 215 of the FPA.

[1] NERC Rules of Procedure at Appendix 5B, *NERC Statement of Registry Criteria* (Registry Criteria), available at http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_5B_RegistrationCriteria_20121220.pdf.

[2] The Implementation Plan associated with this effort will address issues related to the Functional Model.

[3] The term BES does not include facilities used in the local distribution of electric energy.

[4] *See* Appendix C hereto.

Executive Summary

NERC has launched the Risk-Based Registration (RBR) Initiative to ensure that the right entities are subject to the right set of applicable Reliability Standards, using a consistent approach to risk assessment and registration across the Electric Reliability Organization (ERO) Enterprise. The goal is to develop enhanced Registry Criteria, including the use of thresholds and specific Reliability Standards applicability, where appropriate, to better align compliance obligations with material risk to the BES reliability. The proposed enhancements reduce unnecessary burdens by all involved, while preserving BES reliability, and avoid causing or exacerbating instability, uncontrolled separation, or cascading failures. All reliability stakeholders should benefit from RBR.

NERC has established a Risk-Based Registration Advisory Group (RBRAG) to provide input and advice for the RBR design and implementation plan. This white paper is a starting point for discussion and includes input from the RBRAG. Conceptually, there appears to be general agreement on the need to have: (i) clearly defined terms, criteria and procedures that are risk-based and ensure reliability of the BES, (ii) refined thresholds, where warranted, based on sound technical analysis and support, and (iii) reduced Reliability Standard applicability, where warranted, based on sound technical analysis and support.

Taking into account experience to date and current practices, the white paper explores possible options for reform of the NERC Registration program. Other options may exist. The instant options would:

- eliminate up to two functional categories that may not be material to BES reliability;
- revise the thresholds for registration of two functions to better align with risk;
- for selected functions, move away from a "one-size-fits-all" approach by using risk-based criteria to define classes of Registered Entities for application of a properly scoped subset of applicable Reliability Standard requirements;
- develop a consistent approach to determining materiality and fine-tuning registration determinations to include or exclude entities where generally applicable thresholds do not accurately reflect the BES reliability risk posed by a particular entity, along with enhanced ERO-wide processes and procedures for registration and de-registration; and
- identify associated business practices and IT requirements.

There are several possible options, three of which were explored by the RBRAG, to facilitate the implementation of the RBR. These options may be used together or separately. These approaches need more discussion and analysis to consider the most effective and efficient way forward:

1. The Compliance Monitoring and Enforcement Program (CMEP) approach involves establishing that certain requirements do not apply to a Registered Entity, based on uniform characteristics.
2. A Materiality approach involves using the existing thresholds, at their current levels or revised as appropriate, but providing more specificity on the risk-based criteria an entity would use to demonstrate that it no longer needs to be registered for a given function.
3. Revising Reliability Standards is another option. Under the Reliability Standards approach, Reliability Standard requirement applicability classes refer to applying subsets of Reliability Standard requirements to subcategories of certain functions of Registered Entities, and not developing a custom tailoring of applicability for each individual registered entity.

This white paper also includes several "straw" proposals for RBR reforms to the Registry Criteria and Reliability Standard applicability for consideration and further evaluation. Technical analyses in accordance with Section 215 of the FPA will be required to identify any reliability implications or gaps resulting from these proposals. The new

BES Definition also will be central to the analysis to be conducted. Jurisdictional issues are presented by tariff, interconnection agreement and NAESB standard options, and reliance on these is not a substitute for the technical analysis to be conducted. An industry survey will be used to identify issues to be considered as part of the technical analysis.

Feedback on the concepts outlined within the white paper will help inform the ultimate RBR design and related implementation plan. The draft RBR design and implementation plan will be posted in May 2014 for public comment. Based on the current plan, the Registration program redesign and implementation plan will be discussed at the Member Representatives Committee's (MRC's) and NERC Board of Trustees' (Board's) committee meetings in May and August 2014, followed by approval at the Board's November 2014 meeting. The schedule allows for modifications to the NERC Rules of Procedure, as needed, in the third quarter of 2014. NERC requests that stakeholders consider the following questions as they develop comments on the white paper and provide input on the end-state Registration program reform and redesign.

- Have all RBR design elements been covered? If not, what are the other elements?
- Which options should be considered to best facilitate RBR implementation?
- Have appropriate modifications to the functions requiring registration and thresholds for Registry Criteria been identified for further examination? How should they be revised to achieve the risk-based objective while being complete, clear, not unduly complex, and repeatable?
- How should classes of Reliability Standard requirement applicability be set to achieve the risk-based objective, while being complete, clear, not unduly complex, and repeatable? Is the initial identification of Reliability Standard applicability for the lesser risk class appropriate to ensure BES reliability? Please explain.
- Are there other registration reforms that should be considered? If so, please elaborate.
- Are there additional detailed facts and circumstances that influence risk that support an entity's risk assessment in determinations that are above or below the thresholds?
- What technical studies should be completed to justify the threshold changes objectively?

Introduction

Background

NERC launched the RBR Initiative in early 2014, following on the heels of reform in the Reliability Standards program, as well as the Compliance Monitoring and Enforcement programs. The purpose of the Registration program is to identify those entities that are responsible for compliance with the FERC-approved Reliability Standards. NERC's Registration program is set forth in Section 500 of the NERC Rules of Procedure,[5] as well as Appendices 5A and 5B. Notably, NERC registers entities, not facilities. Approximately 1,900[6] entities are registered on NERC's Compliance Registry (NCR) for approximately 4,800 functions.

Pursuant to the NERC Rules of Procedure and its appendices, the Regional Entities identify candidates for registration. In addition, Regional Entities review and evaluate entity registration requests and changes and make recommendations to NERC when a request or change may affect the NCR.

Users, owners and operators of the BPS are required to register, and NERC and the Regional Entities may identify additional entities that should be registered. An entity may be registered in one or more appropriate functional categories and is responsible for complying with the Reliability Standards applicable to the functional categories in which it is registered.[7] If an entity is not listed on the NCR, it is not legally required to comply with Reliability Standards.[8]

The significant experience of NERC and the Regional Entities to date in implementing the Registration program will help inform enhancements to the Registration program.[9]

Purpose

NERC has launched the RBR Initiative to ensure that entities are properly registered and subject to the right set of applicable Reliability Standards to ensure reliability of the BPS. The RBR initiative uses a consistent approach to risk assessment and registration across the ERO Enterprise. The goal is to develop revised Registry Criteria and Reliability Standard applicability, where appropriate, to better align compliance obligations with risk to BES reliability. These enhancements are designed to reduce unnecessary burdens on all involved, while preserving BES reliability and avoid causing or exacerbating instability, uncontrolled separation, or cascading failures.

The goals of the NERC RBR Initiative are twofold. The first is to develop and deploy a sustainable Registration program design that incorporates evaluation of the reliability risks and benefits provided by an entity to ensure reliability, and where appropriate, define classes of Registered Entities for application of a properly scoped set of Reliability Standard requirements. The second goal lays a foundation for the first goal by creating an implementation plan that supports a 2016 or sooner launch, along with business practices and IT requirements, with the possibility of early adoption options that can address undue industry burden, while also preserving reliability.

---

[5] *See* http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20140130.pdf

[6] The number of unique Registered Entities is 1,652, and they are responsible for 4,427 registered functions. Because some Registered Entities are in multiple footprints, the total number of Registered Entities is 1,921, and they are responsible for 4,784 registered functions. This white paper will use 1,900 Registered Entities.

[7] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242 at P 96, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

[8] Order No. 693 at P 97.

[9] *See* Appendix B for additional discussion of the current NERC Registration program, Functions, Functional Model, Regional Entity roles, and Thresholds.

The white paper will be released for public comment as part of the NERC request for MRC's policy input in April 2014. Further, based on the current plan, the Registration program redesign and implementation plan will be discussed at the MRC and Board committee meetings in May and August 2014, and will be approved at the Board's committee meeting in November 2014.

Benefits of deploying an RBR program include:

- aligning entity registration and compliance burden to its risks and contributions to BPS reliability;
- reducing the industry burden associated with registration, while sustaining continued BPS reliability;
- improving use of NERC, Regional Entity , and Registered Entity resources;
- providing feedback to Reliability Standards development to enhance the applicability of currently enforceable and future Reliability Standards; and
- increasing consistency in registration across the eight Regional Entities by developing a common and repeatable approach, along with improving registration and de-registration procedures.

In addition, coordination of this effort will enhance the ERO's ability to:

- evaluate risks to reliability for use across the ERO Enterprise; and
- align changes to the Registry Criteria with other NERC activities and the BES Definition.

RBR will include the use of consistent terminology, a common approach to criteria application, appropriate oversight and improved procedures.

Formation of an advisory group

In 2014, NERC established the RBRAG to provide input and advice for the RBR design and implementation plan. The RBRAG is comprised of representatives from NERC staff, Regional Entity staff and FERC staff, along with United States and Canadian industry representatives. This white paper was developed with input from the RBRAG, industry responses to a focused survey, and assessment of information about the current Registration program attributes.

Recommendations

Clarify terms and improve current procedures

Materiality

The issue of materiality arises in evaluating whether to register an entity that does not meet the criteria or to determine not to register an entity that meets the criteria. Further, materiality assessments can come into play in connection with assigning Registered Entities to appropriate classes of Reliability Standard applicability (discussed in more detail below). Thus, RBR recommends a consistent approach to assessing materiality.

The RBR design should take into account risk assessment considerations across the ERO Enterprise. Generally, the ERO risk assessment involves a review of individual and aggregate system-wide risks and considerations that include the inherent or structural risk to reliability of the BPS, as anchored in the new BES Definition.

BES references

The proposed changes include revising references from BPS to BES in specific threshold criteria; however, such changes would not apply when discussing NERC and FERC jurisdiction over the BPS. Moreover, flexibility to register entities that do not meet threshold criteria will be retained in the Registry Criteria, in recognition of the jurisdiction of NERC and FERC over users, owners and operators of the BPS.

General terms

As part of the RBR effort, NERC will ensure the terms used in the Registry Criteria are clear and defined.

De-registration

An entity seeking to modify its current registration, including de-registration for a particular function, must inform its applicable Regional Entity. The Regional Entity will evaluate the request and notify NERC of any resulting registration changes. The new BES Definition has raised general questions on the procedures and associated timelines for pursuing de-registration of a given function. RBR includes better visibility, clarity, instruction and feedback in this process, as well as additional, improved registration and de-registration procedures and timelines.

NERC oversight and guidance on registration practices

NERC retains responsibility and oversight to ensure that a Regional Entity implements the Registration program in a consistent manner. Towards this end, the RBR redesign should ensure that NERC is periodically performing programmatic reviews of the Regional Entities' registration activities to ensure uniformity in due process and consistency in application. This will include development of controls to ensure consistency.

Possible improvements to the program include, but are not limited to:

- sampling and auditing of Regional Entity application of RBR classes and individual entity application;
- using surveys to reach out to Registered Entities as a means of identifying that a given entity is registered for the proper functions;
- using ongoing outreach to Registered Entities on registration issues; and
- mapping entities within each Regional Entity footprint to ensure awareness of entities that may have a material impact on BEPS reliability.

One-time attestations

As the CMEP is currently implemented, a Registered Entity may be subject to a requirement that is nominally applicable based on functional entity registration, but inapplicable based on specific facts (e.g., a coordinated functional registration agreement, entity does not own that type of equipment, etc.), must attest (with full documentation and citations), at every contact with ERO compliance, that the requirement is still inapplicable. To

reduce undue administrative burdens on the many entities subject to compliance with particular requirements that are inapplicable to them, two improvements can be implemented in the short-term.

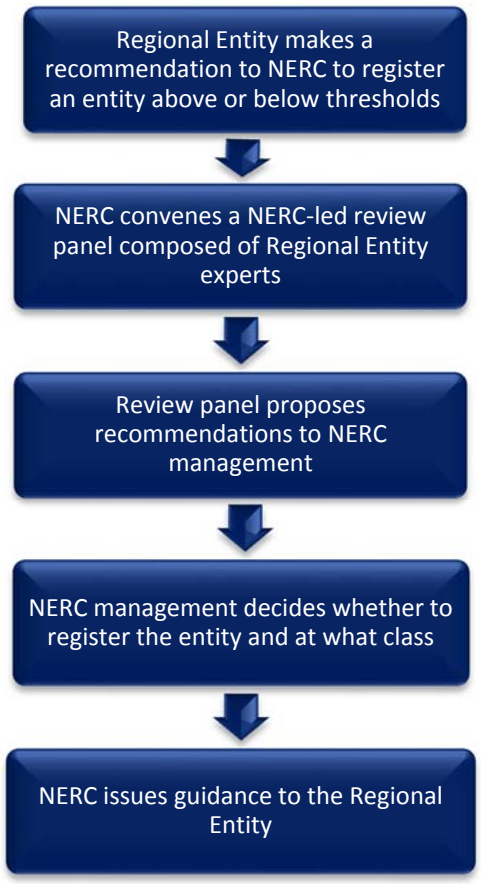
First, with respect to self-certifications and other compliance monitoring activities, Registered Entities should be permitted to record a one-time attestation of "Not applicable" to a given Reliability Standard requirement where there is an existing physical or technical limitation, or the requirement is not applicable for another reason, unless circumstances materially change requiring the need for the registered entity to notify the appropriate Regional Entity. For example, if the registered entity does not own or operate underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) assets, it should simply use the "Not applicable" designation. The Regional Entity will then carry forward this declaration from year-to-year, without requiring the registered entity to repeat the attestation each year. NERC or the Regional Entity would have the ability to audit to verify the recordation is correct, on an as needed basis, but this should be infrequent. In addition, NERC and the Regional Entities should allow Multi-Regional Registered Entities (MRRE) to use a single, one time attestation, updated as needed to reflect material changes, which would apply to all of its registration and compliance monitoring activities across North America, regardless of the Regional Entity footprint in which it operates. In such a case, NERC and the Regional Entities would have the opportunity to audit to verify the single attestation is true and correct.

Establish a centralized review process

NERC intends to establish a centralized, NERC-led review process to address questions or issues that arise with respect to threshold application, materiality, or Reliability Standard requirement applicability. This process will include a panel comprised of a NERC lead with Regional Entity participants. The review panel will vet the issues and provide recommendations to NERC. Once a decision is made, it will be shared throughout the ERO Enterprise. The RBRAG expects this to result in consistency across the ERO Enterprise with respect to threshold, materiality, or applicable Reliability Standard class determinations. In addition, improved procedures, with defined timelines, would be established for registration and de-registration, as well as Reliability Standard applicability class determinations and associated appeals.

The flow diagram (Figure 1) provides a high-level view of some of the steps that might be incorporated into the final RBR design. The goal is to provide a foundation for consistent decision-making and application of the criteria and thresholds.

Figure 1: Flow chart of High-Level Review



Entity risk assessment in a common registration form

The Registration and Certification Functional Group is currently developing a common registration form to help drive consistency in registration. The common registration form is pending consideration as part of the ERO Enterprise applications. The RBR provides an opportunity to finalize and implement the common registration form for use by NERC, Regional Entities, and Registered Entities. The use of a common form will facilitate uniformity in the information being collected from registration candidates regardless of where they are located in North America. The common form is intended is to capture, without undue complexity, key factors relevant to an assessment of an entity's inherent risk. Inherent risk is a function of an entity's various registrations and other relevant factors like its system design, configuration, size, etc.).

The RBR redesign must necessarily address potential impacts on business processes and tools needed to support RBR both within the ERO Enterprise and in industry. RBR recommends exploring use of a single, web-based design. In the interim, changes to the portals and various electronic forms used by NERC and the Regional Entities will need to be adapted to take into account Reliability Standard applicability classes. This will affect compliance monitoring and enforcement activities and will need to be addressed as part of the implementation plan.

In addition, entity risk assessments should take into account information from "neighbor" surveys that Regional Entities issue to Reliability Coordinators (RCs) as part of certification and other activities to ensure coordination with adjacent entities. This survey approach also may increase awareness and tracking by NERC, Regional Entities and RCs of entities within each RC's footprint and help identify needed revisions to an entity's registration.

New BES Definition as model and anchor for risk-based registration

The new BES Definition goes into effect on July 1, 2014 and includes processes for self-determined exclusions and inclusions, as well as exception requests to add elements to, or remove elements from, the BES on a case-by-case basis. The new BES Definition and exception process may resolve, to some extent, the treatment of facilities that are not necessary for the reliable operation of the BPS. However, the revised BES Definition does not eliminate NERC flexibility to decide that registration is not warranted in particular cases, or to restrict the applicability of standards to entities owning or operating limited BES Facilities, where appropriate.

The BES Definition is important to the RBR for two reasons. First, the structure of the BES Definition, approved by FERC, may prove to be a useful model for the RBR. It begins with a bright-line threshold that identifies most facilities that are part of the BES, and then layers on clear exclusions and inclusions that address the most common configurations not adequately captured by the bright-line threshold. Combined, the bright-line, exclusions, and inclusions address the vast majority of elements that should be part of the BES, but elements can be included or excluded from the BES through a case-by-case exception process. The reformed registration process should similarly include revised thresholds, with a case-by-case process to adjust registration (by inclusion or exclusion) where warranted based on a materiality determination that takes into account circumstances not captured by the revised thresholds.

Second, the new BES Definition serves as an anchor for Registry Criteria. While the statutory term BPS sets the outer limit of NERC authority, it has not been defined. Now that the BES is clearly defined, the term can be used to determine on a consistent basis the entities that warrant registration and assess material impact on reliability. For this reason, the straw proposals included as Appendix A for revising Registry Criteria incorporate the BES Definition.

Functional registration category elimination if not material to reliability

NERC reviewed information from various sources to determine if any of the functional categories could be eliminated as part of the RBR redesign. Three have been identified: 1) Regional Reliability Organizations,[10] 2) Purchasing-Selling Entities (PSEs), and 3) Interchange Authorities (IAs). As described in the Appendix A, based on an initial evaluation of risk to BES reliability, elimination of the PSE as a functional registration, which includes some 446 entities, appears promising, although further examination is required. In the event a particular function is determined not to be material to reliability going forward, NERC will evaluate the associated Reliability Standard requirements to determine if accountability for those requirements should be assigned to another function, or

[10] Currently, NERC is eliminating references to Regional Reliability Organization in the NERC Reliability Standards. As a result, the RBR redesign will not include this term.

consider elimination of the requirement with assessment with NERC's Standards Committee, similar to the Paragraph 81 effort.

Synchronize threshold revisions with BES Definition and align with risk

Another approach is to modify current registration thresholds for certain functions. Entities have contended that the current thresholds are too low and sweep in a large number of entities that pose little or no risk to reliability. In addition, the current Registry Criteria reference the BPS, rather than the new BES Definition, creating a lack of clarity and potential for inefficiency and confusion that has no place in a risk-based approach to registration.

Appendix A includes several straw proposals to revise the Registry Criteria for Distribution Provider (DP), Load-Serving Entity (LSE), Transmission Owners and Transmission Operators (TOs and TOPs), and Generator Owners and Generator Operators (GOs and GOPs), to more clearly anchor them in the new BES Definition. In addition, the straw proposals for DP, LSE, and TO/TOP include potential revisions to the registration thresholds to better align with risk. The revised thresholds would be subject to a case-by-case process (modeled after the BES exceptions process) to allow for registration of entities that do not meet the threshold criteria or de-registration of entities that satisfy those thresholds, based on a determination of materiality.

Reliability Standards / compliance and monitoring / risk-based criteria

There are several possible options, three of which were explored by the RBRAG, to facilitate the implementation of the RBR. These options may be used together or separately. These approaches need more discussion and analysis to consider the most effective and efficient way forward.

One option, a CMEP approach, involves establishing that certain requirements do not apply to a Registered Entity, based on uniform characteristics. A matrix could be added to the CMEP that adopts many of the Reliability Standard applicability classes set forth in Appendix A to this white paper. For example, for TOPs, the matrix would indicate the core requirements that apply no matter the uniform characteristics. In addition, the matrix would indicate that certain other requirements, such as load shedding requirements, only apply if the TOP is connected to load.

Another option, a materiality approach, involves using the existing thresholds, at their current levels or revised as appropriate, but providing more specificity on the risk-based criteria that an entity would use to demonstrate that it no longer needs to be registered for a given function. There are many smaller entities that do not believe they should be registered under the current criteria; however, at present, there are no uniform risk-based criteria in place for them to justify how and why they should be de-registered, as well as a timely commitment to address registration concerns. Large TOPs and/or the RC in the region should have an opportunity for input on deregistration decisions. The procedures for submitting a deregistration request also should be part of this RBR effort.

Revising Reliability Standards is another option. Under the Reliability Standards approach, Reliability Standard requirement applicability classes refer to applying subsets of Reliability Standard requirements to subcategories of certain functions of Registered Entities, and not developing a custom tailoring of applicability for each individual registered entity. The intent is to restrict the requirements applicable to Registered Entities that satisfy specified risk-based criteria to ensure the right entities are identified for compliance with appropriate Reliability Standard requirements, and avoid burdening such entities with compliance obligations disproportionate to their risk to BES reliability. Tailoring Reliability Standard obligations has been successfully implemented in both the registration appeal context and Project 2010-07: Generator Requirements at the Transmission Interface (the GO/TO project). In addition, historically, some Regional Entities have addressed the challenges of Reliability Standard applicability to entities through their compliance monitoring activities, such as adjusting the scope of audits. These experiences will help inform RBR efforts.

All three possible approaches set forth above can be further informed by the initial evaluation in Appendix A and additional technical analysis to be conducted. The straw proposals identify a category of entities that own or operate BES Facilities, but that also warrant application of a more limited set of requirements than the more typical TO/TOP and GO/GOP. The proposals suggest a starting point for evaluating the subset of Reliability Standards to be to applicable entities that fall within that lesser risk category. In addition, Appendix A identifies targeting requirements to entities that fall below the revised DP and LSE thresholds, but that are necessary participants in a BES protection program (e.g., UFLS or UVLS).

Particularly under the CMEP and the Reliability Standards approach, described above, once Reliability Standard applicability classes are established and applicable Reliability Standard requirement compliance obligations are aligned with the classes, a number of implementation approaches are available. Under the CMEP approach, a standardized compliance matrix can be maintained to identify which Reliability Standard requirements apply to a given class. Entities registered to the functions with Reliability Standard class applicability will be formally assigned to the appropriate class. Class assignment should be subject to a process that enables the entity to challenge inappropriate application of the criteria, as well as a process (modeled after the BES Exception Process) to assign outliers to the appropriate class, based on an individualized risk assessment and technical justification.

Under the Reliability Standards approach, class compliance responsibility may be reflected within the Applicability section of a given Reliability Standard. Alternatively, as in the GO/TO project, a class approach may be implemented through limited changes in the Reliability Standard applicability, along with associated registration modifications. The latter approach may be suitable to DPs with limited BES transmission facilities, eliminating the need to register such entities as TOs or TOPs. Either of these approaches will require modification of Reliability Standards through the Standards Development Process.

Status quo for other functional registration categories

As discussed above, recommendations for changes apply to eight of the fifteen functional categories, including PSEs, IAs, DPs, LSEs, GOs, GOPs, TOs and TOPs. At this time, there are no proposed recommendations with respect to the following seven functional categories:

> Balancing Authorities (BAs), Planning Authorities (PAs)/Planning Coordinators (PCs), Reliability Coordinators (RCs), Transmission Planners (TPs), Resource Planners (RPs), Reserve Sharing Groups (RSGs) and Transmission Service Provider (TSPs).

Task forces for risk criteria and Reliability Standard applicability classes

As part of RBR, NERC plans to form task forces to develop risk criteria to apply to: (i) entities that meet the thresholds but seek to make a case that they should not be registered because they do not have a material impact on reliability; and (ii) entities that do not meet the thresholds but the Regional Entity, NERC or a reliability entity, such as a BA, RC or TOP, asserts such entities need to be registered and subject to some or all of applicable Reliability Standard requirements.

In addition, NERC plans to form a task force, modeled on the GOTO Task Force, to identify a common set of Reliability Standards that need to be applied to BES resources owned and operated by certain TO/TOPs and GO/GOPs, as discussed in greater detail in Appendix A. This task force will also assess the merits of alternative approaches to targeting registration, standards applicability, and compliance monitoring and enforcement to entity risk.

The resulting analysis can then be used as the basis for establishing appropriate registration categories and making appropriate classes of Reliability Standard applicability.

Issues that require a longer time horizon

Possible rule changes have been identified with respect to the NERC Rules of Procedure Section 500, Appendix 5A, and Appendix 5B to implement risk-based registration. For example, the opportunities for change include modification of the Registry Criteria, and improving procedures, Reliability Standard requirement applicability classes, determinations and associated appeals. Other changes are appropriate to memorialize practices in place today because of FERC orders, and to implement other improvements to these sections. As also noted above, to the extent classes of applicable Reliability Standards are adopted for certain functions, long-term implementation is best achieved through modification of Reliability Standards through the Standards Development Process.

While these efforts can be launched, and interim implementation steps can be taken, as part of Phase 1, completion of these more formalized implementation efforts will likely extend into Phase 2. More details such as scope, outreach, and timing will be addressed in the RBR implementation plan.

Another longer-term related issue is ensuring that Standard Drafting Teams develop standard applicability language for new or revised standards that provides for the most granular applicability language possible.

Appendix A – Risk-Based Registration Threshold Reviews

Purchasing-Selling Entity (PSE)

Current Definition and/or Threshold in Statement of Compliance Registry Criteria

Definition

The entity that purchases, or sells, and takes title to, energy, capacity, and Interconnected Operations Services. The Purchasing-Selling Entity may be affiliated or unaffiliated merchants and may or may not own generating Facilities.

Threshold

N/A

Functional Model Description

The PSE arranges for and takes title to energy products (capacity, energy and reliability-related services) that it secures from a resource for delivery to a Load-Serving Entity. The Purchasing-Selling Entity also arranges for transmission service with the Transmission Service Provider that provide transmission service to the Load-Serving Entity under a tariff or market rule. The Purchasing-Selling Entity initiates a bilateral Interchange between Balancing Authority Areas by submitting a Request for Interchange to the Interchange Coordinator.

Proposed Elimination

Recommend that the functional category of PSE be eliminated as part of the RBR effort. For all Reliability Standards that apply to PSEs, this function should be removed through the Standards Development Process.

Proposed Revised Threshold

N/A- Proposed Function for Elimination

Proposed Critical Sub-function(s)

Dynamic Transfers could be a critical sub-function. However, a survey should be conducted to determine how many entities still use Dynamic Transfers.

Analysis and Support for Proposed Action

There are 447 unique entities registered as a PSE. Five (5) FERC-approved Reliability Standard Requirements currently apply to PSEs. Those standards and requirements are:

- INT-001-3, Requirement R1
- INT-004-2, Requirement R2
- IRO-001-1.1, Requirement R8
- IRO-005-3.1a, Requirement R10
- TOP-005-2a, Requirement R3

With regard to violations, there have only been 40 instances of PSE noncompliance out of 29,545 total instances of noncompliance. The NERC and Regional CMEP efforts have recently begun to utilize more self-certifications (rather than audits) for entities registered only as PSEs, and only one PSE standard is currently listed on Compliance's 2014 Actively Monitored List, IRO-005-3.1a. In addition, only one requirement listed above has a High Violation Risk Factor (VRF), IRO-001-1.1, Requirement R8, which states as follows:

> Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling

> Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.

IRO-001-1 will eventually be replaced by a new set of IRO standards, together with revised Transmission Operator (TOP) standards.[11] The proposed standard IRO-001-3, which will replace IRO-001-1, has removed applicability for the PSE functions. Further, the Independent Experts Review Panel (IERP) recommended INT-004 standards for potential retirement reasoning that a NAESB guideline exists in the *Electronic Tagging Functional Specification* document.

The remaining standards have a Lower VRF. In reviewing the remaining standards that still apply to PSEs, the Standards Development Process would need to address removing PSEs from individual requirements and must determine if there is a suitable replacement entity or if a business practice/process can be transferred to North American Energy Standards Board (NAESB). Technical analyses in accordance with Section 215 of the FPA will be required to identify any reliability implications so that no reliability gaps are created. As a result, this initial assessment of risk could be revised based on further analysis. An industry survey also will be used to identify issues to be considered as part of the technical analysis.

Finally, Dynamic Transfers may not apply to organized markets. RTO/ISOs usually only dispatch generation in their operational jurisdiction, but this will need to be confirmed as part of the survey to determine if Dynamic Transfers are a critical sub-function. In addition, PSEs do not have the authority to initiate a curtailment on a transaction due to a reliability event, and PSEs do not have the authority to reload transactions or the ability to release a limit.

Interchange Authority / Interchange Coordinator (used interchangeably) (IA)

Current Definition and/or Threshold in Statement of Compliance Registry Criteria

Definition

The responsible entity that authorizes implementation of valid and balanced Interchange Schedules between Balancing Authority Areas, and ensures communication of Interchange information for reliability assessment purposes.

Threshold

N/A

Functional Model Description

The Interchange Coordinator collects approvals or denials for Arranged Interchange from Balancing Authorities and Transmission Service Providers and verifies the validity of the source and sink. The NERC Tag Authority provides this service assigned to the Sink Balancing Authority.

The Interchange Coordinator provides the Balancing Authority with the individual bilateral Arranged Interchange. The Balancing Authority must track the individual Interchange Schedules in case one or more of them are curtailed by the Reliability Coordinator or by the Balancing Authority in those cases where a generator or load is interrupted.

[11] However, both sets of proposed standard were subject to a recent FERC NOPR recommending a remand. A standard development project is ongoing to address the NOPR's proposed remand. FERC did not take issue with the elimination of PSEs in IRO-001-1.

The Balancing Authority then creates a "net" interchange total for use in its energy management system as well as a "net" interchange for each neighboring Balancing Authority. The net Interchange Schedule for each neighboring Balancing Authority is used by the Receiving Balancing Authority for checkout with the neighboring Balancing Authorities.

All bilateral Interchange Transactions that cross a Balancing Authority Area boundary are coordinated through the Interchange Coordinator.

While the approval/denial process may utilize tools (such as computer software and communication protocols), the Model envisages that the Interchange function will be assigned to an actual organization. A Balancing Authority may serve as its own Interchange Coordinator or have this service provided by a separate organization.

Assessing ramping capability and connectivity. The Balancing Authority approves/denies the capability to ramp the Arranged Interchange in or out and notifies the Interchange Coordinator. The connectivity of adjacent Balancing Authorities is also verified by the Balancing Authorities before responding to the Interchange Coordinator.

Ensuring balanced, valid Interchange Transactions. The Interchange Coordinator also ensures that the resulting Confirmed Interchange Transactions is balanced and valid prior to physical delivery. This means:

- The source MW must be equal to the sink MW (plus losses if they are "self-provided"), and
- All reliability entities involved in the Arranged Interchange are currently in the NERC registry.

Only when it receives approvals from the Transmission Service Providers and Balancing Authorities, does the Interchange Coordinator direct the Balancing Authorities to implement the Transaction. If any of these entities — Transmission Service Providers, or Balancing Authorities — does not approve the Arranged Transaction, then the Interchange Coordinator does not authorize the Transaction to become Confirmed Interchange.

Curtailments. The Interchange Coordinator coordinates curtailments of Confirmed Interchange ordered by the Reliability Coordinator by notifying the Balancing Authorities, Transmission Service Providers, and Purchasing-Selling Entities. The Interchange Coordinators also communicates and coordinates the resulting modified Arranged Interchange that result from the curtailments.

Proposed Elimination

The functional category of IA has been identified for potential elimination as part of the RBR effort. The industry must be surveyed to determine if a reliability gap will be created by removing the IA function from the Registry Criteria. Most notably, the industry must answer whether the Balancing Authority (BA) function and applicable requirements are sufficient for ensuring reliability. In eliminating the IA, the BA will not take over all of the IA standards and requirements. The industry must provide whether the existing BA function and existing BA requirements are sufficient for maintaining reliability after the IA has been removed. Industry feedback should provide particular attention to how a BA would balance generation, manage load and schedules, avoid unscheduled transfers, and the ability of the BA to implement congestion management.

Proposed Revised Threshold

N/A

Proposed Critical Sub-function(s)

N/A

Analysis and Support for Proposed Action

There are currently forty-one (41) uniquely registered IAs. Of those forty-one entities, only one (1), Peak Reliability, is not also registered as a BA. Currently, the following families of Reliability Standards apply to IAs:

- CIP
- INT-005-3
- INT-007-1
- INT-008-3
- IRO-010-1a

However, NERC recently submitted a filing that recommended the retirement of INT-005-3, INT-007-1, and INT-008-3.[12] That leaves only one non-CIP requirement that would apply to IAs: IRO-010-1a, Requirement R3. Although the changes have not been adopted, the latest recommendations from the IRO Five-Year Review Team are to remove IAs from the applicability of IRO-010-1a.[13] Although the IERP did not recommend deletion of IRO-010-1a, Requirement R3 due to this being the only data-sharing requirement, the IERP did state this requirement could be consolidated with a TOP requirement.

With regard to violations, IAs have had 598 instances of noncompliance out of 29,545 total instances of noncompliance since 2007. A large majority of those violations were CIP violations.

The IA function itself has evolved greatly since the Registry Criteria was first created. Several aspects of the IA function have become automated over time. Also, because most of the IAs are already registered as BAs, it is recommended that BAs serve as the entity ultimately responsible for the historically-IA functions in the Registry Criteria. This would not entail transferring all of the applicable IA requirements to BAs. Instead, the recommendation is to first survey the industry in order to determine if a reliability gap is created by removing IAs and have the BAs maintain reliability through their on-going operations and requirements.

Distribution Provider (DP)

Current Definition and/or Threshold in Statement of Compliance Registry Criteria

Definition

Provides and operates the "wires" between the transmission system and the end-use customer. For those end-use customers who are served at transmission voltages, the Transmission Owner also serves as the Distribution Provider. Thus, the Distribution Provider is not defined by a specific voltage, but rather as performing the distribution function at any voltage.

Threshold

NERC Rules of Procedure (ROP) Appendix 5B at III.b.1 Distribution Provider system serving >25 MW of peak load that is directly connected to the Bulk Power System.

> *[Exclusion: A Distribution Provider will not be registered based on this criterion if responsibilities for compliance with approved NERC Reliability Standards or associated Requirements including*

[12] *See Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standards for Interchange Scheduling and Coordination,* submitted on February 27, 2014 (available at http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20for%20Approval%20of%20INT%20Reliability%20Standards_.pdf).

[13] *See http://www.nerc.com/pa/Stand/Project201209IROReview/IRO-010-2_redline_2013Oct01.pdf.*

reporting have been transferred by written agreement to another entity that has registered for the appropriate function for the transferred responsibilities, such as a Load-Serving Entity, Balancing Authority, Transmission Operator, generation and transmission cooperative, or joint action agency as described in Sections 501 and 507 of the NERC Rules of Procedure.]
or;

ROP Appendix 5B at III.b.2 Distribution Provider is the responsible entity that owns, controls, or operates Facilities that are part of any of the following Protection Systems or programs designed, installed, and operated for the protection of the Bulk Power System:

- a required UFLS program.
- a required UVLS program.
- a required Special Protection System [(SPS)].
- a required transmission Protection System [(TPS)].

[Exclusion: A Distribution Provider will not be registered based on these criteria if responsibilities for compliance with approved NERC Reliability Standards or associated Requirements including reporting have been transferred by written agreement to another entity that has registered for the appropriate function for the transferred responsibilities, such as a Load-Serving Entity, Balancing Authority, Transmission Operator, generation and transmission cooperative, or joint action agency as described in Sections 501 and 507 of the NERC Rules of Procedure.]

Functional Model Description
The Distribution Provider provides the physical connection between the end-use customers and the electric system, including customers served at transmission level voltages. The Distribution Provider is not defined by a specific voltage, but rather as performing the Distribution function at any voltage. One Distribution Provider may be directly connected to another Distribution Provider and not directly connected to the Bulk Electric System.

The Distribution Provider maintains “local” safety and reliability. The Distribution Provider provides the switches and reclosers necessary for emergency action. The Distribution Provider may need to demonstrate load-shedding capability to the Balancing Authority and Transmission Operator.

The same organization may serve as the Distribution Provider and Load-Serving Entity, but they may be separate organizations as well. Unlike the Load-Serving Entity, the Distribution Provider has the facilities or assets (“wires”) and does not take title to any energy. However, while these functions are distinct, in many cases an organization, such as a vertically integrated utility, bundles these functions together.

Proposed Elimination
N/A

Proposed Revised Threshold
Recommend that the peak load threshold in Registry Criteria III.b.1 be increased to 75 MW or 100 MW (or other number as determined based on further analysis) and directly connected to the BES.

Replace Registry Criteria III.b.2 with the following two paragraphs. Using the risk-based criteria, which is to be developed, DPs with peak load between 25 MW and the new peak load threshold and directly connected to the BES generally would not be subject to registration even if they participate in a BES protection program (e.g., UFLS, UVLS, SPS or TPS), unless it has been demonstrated that their participation in such a program is necessary for the reliable operation of the BES. To the extent that they are registered, they should be subject only to a sub-list class

of Reliability Standards, including the relevant protection system Reliability Standards, which is to be determined based on further analysis.

Entities with less than 25 MW peak load, or not directly connected to the BES, generally would not be registered, even if they participate in a BES protection program, except in extraordinary circumstances under the risk-based criteria, which is to be developed. To the extent that they are registered, they should be subject only to a sub-list class of Reliability Standards, including the relevant protection system Reliability Standards, which is to be determined based on further analysis.

Proposed Critical Sub-function(s)

DPs with peak load between 25 MW and the new peak load threshold and directly connected to the BES are subject to registration for participation in a BES protection program if it has been demonstrated that their participation in such a program is necessary for the reliable operation of the BES.

Analysis and Support for Proposed Action

Increase DP threshold to a peak load of 75-100 MW and directly connected to the BES

Consistent with a risk-based approach to registration, the general threshold for DP registration should be modified to 75 MW or 100 MW (or other number as determined based on further analysis) and directly connected to the BES. The new threshold should be accompanied by a risk-based process, like the BES Exception Process, that allows Regional Entities to register entities below the threshold on the basis of a demonstration of material impact on the BES, and allows entities above that threshold to seek relief from registration as a DP where the entity demonstrates lack of a material impact on the BES. Replacing the reference in the threshold with BES (rather than BPS) is consistent with FERC's determination in the SLECA case[14] and a risk-based approach because it would take into account the results of the application of the new BES Definition, including its exception process.

Reliability Standards applicable to DPs fall into the following categories: coordination with higher-level entities when adding new facilities; nuclear plant service; compliance with reliability directives issued by higher-level entities; cybersecurity (in limited circumstances); reporting of certain events; operator training (if the DP has field switching personnel identified as performing unique tasks associated with the Transmission Operator's restoration plan that are outside of their normal tasks); and protection systems (addressed in a separate section below).

Except in very unusual cases, imposing all of these requirements on entities with a peak load below 75 MW-100 MW or not directly connected to the BES may not be necessary from a risk-based perspective. According to data assembled by NERC, there were only 0.21 DP violations per registered DP per year in 2007-2014—far less than the rate for other functions, such as TOP and BA. In addition, a preliminary review of Energy Information Administration (EIA) data—which does not present a complete view of Registered Entities—suggests that DPs with peak load under 75 or 100 MW serve a very small proportion of U.S. load, and that including these entities on the NCR may not be needed to accomplish the primary reliability objectives of standards applicable to DPs, particularly when viewed in the context of the purpose of Reliability Standard, which is to avoid BES instability, uncontrolled separation and cascading outages. Further, an initial analysis of applicable Reliability Standards suggests that a risk-based approach to registration generally would not require registration of small (below 75 MW-100 MW peak load) DPs, although further analysis is warranted:

- FAC-002-1 requires DPs "seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities" to coordinate and cooperate on assessments with their TP and PA. DPs are already required by tariff or interconnection agreement to coordinate with the TO/TOP(s) to which they are

[14] *S. La. Elec. Coop. Ass'n*, 144 FERC ¶ 61,050 (2013).

connected before adding another point of interconnection. There may not be a need for a Reliability Standard to ensure that small DPs do not add new facilities without permission. To the extent that any gap in coverage may exist with respect to such small entities, it may not be material.

- It would be unusual for a DP under 100 MW to have Nuclear Plant Interface Requirements (NPIR) responsibilities. To the extent that there are any such DPs, they could be retained on the NCR (for compliance with NUC-001) through the case-by-case material impact process.
- Other DP requirements focus on compliance with reliability directives. In the unlikely event a small (below 75 MW – 100 MW) DP is issued a reliability directive, it would most likely be to shed load. The Open Access Transmission Tariff (OATT) includes provisions for curtailing transmission service for point to point service (§§ 13.6, 14.7) and network service (§ 33). Furthermore, a small DP's failure to follow a reliability directive is unlikely to have a material impact on BES reliability, because the entity is too small to have such an impact. If, however, a particular DP under 100 MW could materially impact BES reliability by failing to comply with a reliability directive, the entity can be registered through the material impact process.
- As for cybersecurity, CIP-002-5 applies to very few DPs with peak load under 100 MW: those with an SPS, Remedial Action Scheme (RAS), or other transmission Protection System (other than UFLS or UVLS) subject to NERC Reliability Standards, and those that own a "Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started." To the extent a particular small DP's compliance with cybersecurity standards is demonstrated to be necessary to prevent a material risk to BES reliability, that DP can be registered on a case-by-case basis through the risk-based criteria.
- DPs are required to have, and follow, an event reporting plan under EOP-004-2; but the events to be reported, for DPs, are only of damage or threats to a Facility (i.e., a BES Element); automatic shedding of at least 100 MW; and the loss of at least 200 MW of firm load. Most if not all small DPs, in their capacity as DPs, do not own Facilities; and by definition, a DP with a peak load under 100 MW will not shed 100 MW or lose 200 MW of firm load. Making EOP-004-2 inapplicable to small DPs would not result in increased risk to BES reliability.
- Operator training is required by EOP-005-2 only where a DP is identified in a TOP's restoration plan, and the DP has field switching personnel identified as performing unique tasks associated with the TOP's restoration plan that are outside of their normal tasks. The subset of DPs that meet those criteria and are under 100 MW is not expected to be large. To the extent the participation of any such DP in the TOP's restoration plan is shown to be material to BES reliability, however, the DP can be registered through the material impact process.

As discussed above, the registration threshold for DPs could be raised from the present 25 MW peak load to 75 MW or 100 MW without a significant impact on risk to BES reliability. While the EIA data suggests that the proportion of load served by DPs with peak loads under 100 MW is *de minimis* on a continent-wide basis, that data may not provide a complete picture. Because tariff and interconnection agreements arise under Section 205 of the FPA, technical analyses in accordance with Section 215 of the FPA will be required to identify any reliability implications so that no reliability gaps are created. As a result, this initial assessment of risk could be revised based on further analysis. An industry survey also will be used to identify issues to be considered as part of the technical analysis.

Restrict DP registration of below-threshold entities based on UFLS/UVLS/SPS/TPS

DPs with peak load between 25 MW and the revised threshold and directly connected to the BES—i.e., entities below the revised threshold who were previously registered based on the minimum 25 MW size—would not be registered based on their participation in a BES protection program, unless there is a demonstrated reliability

need; to the extent that they are registered, they should be subject only to the relevant protection system reliability standards and such other Reliability Standards as determined to be necessary based on further analysis. Rather, consideration of materiality of risk to BES reliability calls for restricting registration of such entities except where demonstrated necessary in light of unusual circumstances, and in such cases limiting the applicable standards.

In unusual situations (i.e., significant portion of load is served by small DPs), the DPs could be registered on a case-by-case basis based on their material impact on reliability, and made subject only to the relevant system protection standards and such other Reliability Standards as determined to be necessary based on further analysis. Where the Planning Coordinator PC or Regional Entity demonstrates that the participation of a particular directly-connected DP between 25 MW and the revised 75MW or 100MW threshold is necessary to protect BES reliability, the DP should be required to comply only with the relevant system protection standards and such other Reliability Standards as determined to be necessary based on further analysis. Removal of small DPs from compliance with other DP requirements would be unlikely to materially increase the risk to BES reliability. Small entities who are no longer subject to DP registration but wish to remain a part of a BES protection program should be permitted to opt in to compliance with such programs and the applicable Reliability Standards, so that small utilities that need to choose which portions of their load to shed can continue to do so.

Technical analyses in accordance with Section 215 of the FPA will be required to identify any reliability implications so that no reliability gaps are created. As a result, this initial assessment of risk could be revised based on further analysis. An industry survey also will be used to identify issues to be considered as part of the technical analysis.

Load-Serving Entity (LSE)

Current Definition and/or Threshold in Statement of Compliance Registry Criteria

Definition

Secures energy and Transmission Service (and related Interconnected Operations Services) to serve the electrical demand and energy requirements of its end-use customers.

Threshold

NERC Rules of Procedure (ROP) Appendix 5B at III.a.1 Load-Serving Entity peak load is > 25 MW and is directly connected to the Bulk Power (>100 kV) System, or;

ROP Appendix 5B at III.a.2 Load-Serving Entity is designated as the responsible entity for Facilities that are part of a required underfrequency load shedding (UFLS) program designed, installed, and operated for the protection of the Bulk Power System, or;

ROP Appendix 5B at III.a.3 Load-Serving Entity is designated as the responsible entity for Facilities that are part of a required undervoltage load shedding (UVLS) program designed, installed, and operated for the protection of the Bulk Power System.

> *[Exclusion: A Load-Serving Entity will not be registered based on these criteria if responsibilities for compliance with approved NERC Reliability Standards or associated Requirements including reporting have been transferred by written agreement to another entity that has registered for the appropriate function for the transferred responsibilities, such as a Load-Serving Entity, Balancing Authority, Transmission Operator, generation and transmission cooperative or joint action agency as described in Sections 501 and 507 of the NERC Rules of Procedure.]*

ROP Appendix 5B at III.a.4 Distribution Providers registered under the criteria in III.b.1 or III.b.2 will be registered as a Load Serving Entity for all load directly connected to their distribution facilities.

> *[Exclusion: A Distribution Provider will not be registered based on this criterion if responsibilities for compliance with approved NERC Reliability Standards or associated Requirements including reporting have been transferred by written agreement to another entity that has registered for the appropriate function for the transferred responsibilities, such as a Load-Serving Entity, Balancing Authority, Transmission Operator, generation and transmission cooperative, or joint action agency as described in Sections 501 and 507 of the NERC Rules of Procedure.]*

Functional Model Description

The Load-Serving Entity arranges for the provision of energy to its end-use customers, but does not provide distribution services (“wires”). The Load-Serving Entity defined in the Model is not to be confused with or equated to the Load-Serving Entity as defined in any tariff or market rule.

Today, organizations serving as Load-Serving Entities may also be Generation Owners and can self-provide, or have contracts with other Generator Owners for capacity and energy to serve the Load-Serving Entity’s customers, or purchase capacity and energy from non-affiliated Generator Owners through a Purchasing-Selling Entity (or Market Operator), or employ a combination of these three options.

The Load-Serving Entity reports its generation (affiliated and non-affiliated) arrangements to serve load to the Balancing Authority, which forwards this information to the Reliability Coordinator, for day-ahead analysis.

The Load-Serving Entity may contract for reliability-related services through the Market Operator (if the Load-Serving Entity is part of a market or pool) or directly from Generator Owners or loads.

The same organization may serve as the Distribution Provider and Load-Serving Entity, but they may be separate organizations as well. Unlike the Distribution Provider, the Load-Serving Entity, does not have Bulk Electric System assets ("wires") but does take title to energy. However, while these functions are distinct, in many cases an organization, such as a vertically integrated utility, bundles these functions together.

The Functional Model assigns to the Load-Serving Entity the identification of loads for curtailment and the development of load profiles and load forecasts. Please see Section II, 114: Roles in Load Curtailment for more detailed information.

The Load-Serving Entity communicates requests for voluntary curtailment to the appropriate end-use customer loads, thereby ensuring that these loads will, in fact, be curtailed.

Proposed Elimination
N/A

Proposed Revised Threshold
Recommend that the peak load threshold in Registry Criteria III.a.1 be increased to 75 MW or 100 MW (or other number as determined based on further analysis) and directly connected to the BES.

Also, revise that section to reflect the following two paragraphs. Using the risk-based criteria, which is to be developed, LSEs with peak load between 25 MW and the new peak load threshold, and directly connected to the BES, generally would not be subject to registration even if they participate a UVLS program, unless it has been demonstrated that their participation in such a program is necessary for the reliable operation of the BES. To the extent that they are registered, they should be subject only to a sub-list class of Reliability Standards, including the relevant protection system Reliability Standards, which is to be determined based on further analysis.

Entities with less than 25 MW peak load, or not directly connected to the BES, generally would not be registered, even if they participate in a BES protection program, unless there is a demonstrated reliability need. To the extent that they are registered, they should be subject only to a sub-list class of Reliability Standards, which is to be determined based on further analysis.

Proposed Critical Sub-function(s)
LSEs with peak load between 25 MW and the new peak load threshold, and directly connected to the BES, generally would not be registered, even if they participate in a UVLS program, except in extraordinary circumstances under the risk-based criteria, which is to be developed. To the extent that they are registered, they should be subject only to a sub-list class of Reliability Standards, including the relevant protection system Reliability Standards, which is to be determined based on further analysis.

Analysis and Support for Proposed Action
Change the LSE registration threshold to LSEs with peak load of at least 75 MW-100 MW and directly connected to the BES
Consistent with a risk-based approach to registration, the threshold for registration should be increased to 75 MW or 100 MW (or other number as determined based on further analysis) and directly connected to the BES. The new threshold would be accompanied by a risk-based process that enables Regional Entities to register entities below the threshold based on a demonstration of material impact on the BES, and allows entities above that threshold to seek relief from registration as an LSE where the entity demonstrates lack of a material impact on

the BES. Replacing the reference in the threshold with BES (rather than BPS or above 100 kV) is consistent with FERC's determination in the SLECA case and a risk-based approach because it would take into account the results of the application of the new BES Definition, including its exception process.

Reliability Standards applicable to LSEs fall into the following categories: coordination with higher-level entities; nuclear plant service; compliance with reliability directives issued by RCs and TOPs; cybersecurity (under currently-effective version 3, but not under version 5); procedures during Energy Emergencies; Requests for Interchange for intra-BA transfers; operate the BES to the most limiting parameter; provide data and information to higher-level entities; appropriately determining Capacity Benefit Margin (CBM) need, where applicable; coordinate operations with host BA and TSP; and UVLS (addressed in Section B below).

Except in very unusual cases, imposing these requirements on entities with peak load below 75 MW or 100 MW or not directly connected to the BES may not be necessary from a risk-based perspective. According to data assembled by NERC, there were only 0.86 LSE violations per registered LSE per year in 2007-2014—far less than the rate for other functions, such as TOP and BA. In addition, a preliminary review of EIA data—which does not present a complete view of Registered Entities—suggests that LSEs with peak load under 75 MW or 100 MW likely serve a very small proportion of U.S. load. Including these entities on the Compliance Registry is not needed to accomplish the primary reliability objectives of standards applicable to LSEs. Specifically:

- LSEs are subject to FAC-002-1, NUC-001-2.1, and Reliability Standards requiring compliance with reliability directives. The analysis of these issues in the discussion of DP registration applies to LSEs as well.
- LSEs are to be removed from CIP requirements under CIP version 5, which suggests that de-registering a subset of LSEs will not pose a risk to BES reliability.
- Energy-deficient LSEs must follow certain procedures under EOP-002-3.1. However, the amount of energy likely to be needed by an energy-deficient LSE whose *peak* load is under 100 MW is unlikely to pose a reliability risk; moreover, such an LSE could voluntarily follow the EOP-002-3.1 R1-R8 procedures to remedy its deficiency. If those procedures were inadequate and firm load needed to be shed to protect reliability, and the unregistered LSE refused to do so, its transmission provider would have the authority and obligation to do so under the OATT and NAESB Wholesale Electric Quadrant Standard WEQ-008, Transmission Loading Relief (TLR) – Eastern Interconnection.
- INT-011-1 (which is pending before FERC) requires that *"Each Load-Serving Entity that uses Point to Point Transmission Service for intra-Balancing Authority Area transfers shall submit a Request for Interchange unless the information about intra-Balancing Authority transfers is included in congestion management procedure(s) via an alternate method."* The purpose of the standard is "[t]o ensure that transfers within a Balancing Authority Area using Point to Point Transmission Service are communicated and accounted for in congestion management procedures." Intra-BA transfers by LSEs with peak load between 25 and 100 MW are subject to tariff, operating agreement, and interconnection agreement requirements and, in any case, are unlikely to be a significant contributor to congestion.
- LSEs, among other entities, are required to operate the BES to the most limiting parameter. LSEs, as such, do not operate the BES, IRO-005-3.1a should not be applicable to LSEs. Making the requirement inapplicable to LSEs with peak load under 100 MW does not pose a material risk to BES reliability.
- Providing data for modeling and planning purposes is the concern often identified with respect to raising the registration threshold for LSEs. Based on the EIA data available, however, it appears that the aggregate load of LSEs under 75 MW or 100 MW is likely within the margin of error in their regions, provides little technical significance to the models, and is accordingly not needed. In the event that data from such entities is needed to avoid an undue risk to BES reliability in a particular region, however, the necessary LSEs can be registered on a case-by-case basis through the material impact process.

- In regions that use CBM, a registered LSE determining the need for transmission capacity to be set aside as CBM must use one of several studies or other methods of determining needed CBM. The TP must then establish a CBM value to use in its Available Transfer Capability (ATC) calculations that reflects consideration of the LSE's study. Subjecting small LSEs to compliance with the CBM-related reliability standard may not be needed to prevent material impact on the BES. Either small LSEs seeking a CBM set-aside will perform the required studies, or their TP will not set aside any CBM for them.
- Finally, TOP-002-2.1b requires that, to the extent permitted by confidentiality agreements, LSEs coordinate their current-day, next-day, and seasonal operations with their BAs and TSPs—i.e., that they provide load forecasts. To a significant degree, such coordination is achieved through tariff provisions or through an LSE's power supplier. To the extent not covered, such coordination by LSEs under 100 MW is unlikely to be material to BES reliability.

As shown above, the registration threshold for LSEs could be raised from the present 25 MW peak load to 75 MW or 100 MW without a significant impact on risk to BES reliability. While the EIA data suggests that the proportion of load served by LSEs with peak loads under 100 MW is *de minimis* on a continent-wide basis, that data may not provide a complete picture. As noted above, because tariff and interconnection agreements arise under Section 205 of the FPA, technical analyses in accordance with Section 215 of the FPA will be required to identify any reliability implications so that no reliability gaps are created. As a result, this initial assessment of risk could be revised based on further analysis. An industry survey also will be used to identify issues to be considered as part of the technical analysis.

Restrict LSE registration of below-threshold entities based on UFLS/UVLS

LSEs with peak load between 25 MW and the revised threshold and directly connected to the BES generally would not be registered, even if they participate in a UVLS program, unless there is a demonstrated reliability need. To the extent that they are registered, they should be subject only to the relevant protection system reliability standard or such other Reliability Standards as determined necessary based on further analysis. No entity should be registered as an LSE based on its participation in a UFLS program, because UFLS standards no longer apply to LSEs. Rather, consideration of materiality of risk to BES reliability calls for restricting registration of such entities except where demonstrated necessary in light of unusual circumstances, and in such cases limit the applicable standards to those directly pertaining to the relevant protection program.

In unusual situations (i.e., significant portion of load is served by small LSEs), the LSEs could be registered on a case-by-case basis based on their material impact on reliability, and made subject only to the UVLS standard or other Reliability Standards based on further analysis. As a general matter, Registered Entities should be encouraged to avoid requiring small LSEs to own or operate UVLS equipment as a mandatory part of the entities' UVLS programs, because direct participation of such entities is not likely to significantly affect the effectiveness of those programs except in unusual circumstances. Where the PC or Regional Entity demonstrates that the participation of a particular directly connected LSE between 25 MW and the revised MW threshold in a UVLS program is necessary to protect BES reliability, the LSE should be required to comply only with the Reliability Standards relevant to the UVLS program or other Reliability Standards based on further analysis. Removal of such small entities (or entities not directly connected with the BES) from compliance with other LSE requirements would be unlikely to materially increase the risk to BES reliability. Small entities should be permitted to opt in to compliance with such programs and the applicable Reliability Standards, so that small utilities that need to choose which portions of their load to shed can continue to do so.

Technical analyses in accordance with Section 215 of the FPA will be required to identify any reliability implications so that no reliability gaps are created. As a result, this initial assessment of risk could be revised based on further analysis. An industry survey also will be used to identify issues to be considered as part of the technical analysis.

Transmission Owner (TO)

Current Definition and/or Threshold in Statement of Compliance Registry Criteria in Statement of Compliance Registry Criteria

Definition
The entity that owns and maintains transmission Facilities.

Threshold
NERC Rules of Procedure (ROP) Appendix 5B at III.d.1 An entity that owns/operates an integrated transmission Element associated with the Bulk Power System 100 kV and above, or lower voltage as defined by the Regional Entity necessary to provide for the Reliable Operation of the interconnected transmission grid; or

ROP Appendix 5B at III.d.2 An entity that owns/operates a transmission Element below 100 kV associated with a Facility that is included on a critical Facilities list that is defined by the Regional Entity.

> *[Exclusion: A Transmission Owner/Operator will not be registered based on these criteria if responsibilities for compliance with approved NERC Reliability Standards or associated Requirements including reporting have been transferred by written agreement to another entity that has registered for the appropriate function for the transferred responsibilities, such as a Load-Serving Entity, generation and transmission cooperative or joint action agency as described in Sections 501 and 507 of the NERC Rules of Procedure.]*

Functional Model Description
The Transmission Owner owns its transmission facilities and provides for the maintenance of those facilities. It also specifies equipment operating limits, and supplies this information to the Transmission Operator, Reliability Coordinator, and Transmission Planner and Planning Coordinator.

In many cases, the Transmission Owner has contracts or interconnection agreements with generators or other transmission customers that would detail the terms of the interconnection between the owner and customer.

Relationship with the Transmission Operator. The organization serving as Transmission Owner may operate its transmission facilities or arrange for another organization (which may or may not be a Transmission Owner) to operate and/or maintain its transmission facilities.

Proposed Elimination
N/A

Proposed Modification of Registration Criteria
Recommend that section III(d) of the Statement of Compliance Registry Criteria be revised to read:

> *Any owner or operator of one or more Bulk Electric System transmission Elements.*

Proposed Revised Threshold/Classes of Standards Applicability
The detailed registration thresholds located at section III(d) of the Registry Criteria are no longer needed to determine whether the owner or operator of an electric transmission Facility is subject to NERC Reliability Standards. The BES Definition and BES Exception Process set forth in the NERC Rules of Procedure perform the same tests, with greater precision and consistency. However, there is merit to establishing criteria to determine the applicability of Reliability Standards to different classes of TO and TOP entities. The following sub-threshold is proposed for consideration:

An entity that owns/operates only transmission lines operated below 200 kV and/or transformers with low voltage terminals connected at below 200 kV, and whose transmission Facilities do not meet the other criteria in Attachment B to reliability standard PRC-023-2, Relay Loadability.

The intent of establishing criteria to differentiate classes of TO/TOPs is not to remove entities owning and operating BES transmission Facilities from the NCR. Rather, such owners and operators would remain registered and subject to compliance with a subset of TO/TOP standards, but those that do not exceed the threshold set in this process would be subject only to the pre-determined subset of TO/TOP requirements appropriate for entities with limited BES transmission Facilities. The resulting sub-set of applicable TO/TOP standards could be accomplished by a variety of approaches:

Three options are proposed for consideration to implement the revised threshold:

(i) Register the BES Element owner/operator as a DP and where necessary, make corresponding changes to the applicability sections and requirements of Reliability Standards.

(ii) Establish a new Registry function, Local Transmission Owners, with corresponding changes to Reliability Standards.

(iii) Develop and post a standard set of TO and TOP requirements that are determined to be applicable to BES transmission owners that meet the revised Local Transmission Facility threshold described above.

Option (i) is discussed in detail below.

Proposed Critical Sub-function(s)
N/A

Analysis and Support for Proposed Action
Under the revised Statement of Compliance Registry Criteria, an entity is subject to registration as a TO/TOP if it owns/operates "transmission Facilities," i.e., BES Elements used for transmission. Entities will thus be registered only if they own/operate BES transmission Elements, i.e., if their transmission equipment meets the revised BES Definition or has been added through the exceptions process, and has not been *excluded* through the exceptions process.

However, the simple revisions outlined above will not, without more analysis,[15] provide for a rational risk-based registration of BES transmission owners and operators. The current registration criteria for TOs and TOPs assume that all TOs and all TOPs perform similar BES functions and have similar capabilities. For example, a small DP entity that owns a single 115 kV switching station on a BES 115 kV transmission circuit that is part of an integrated transmission network owned and operated by others will normally be registered a TO and TOP, and be responsible for the same requirements as a large vertically integrated utility. A strict reading of the Registry Criteria has led to the result that an entity that owns one 138-kV BES loop being subject to the full set of standard requirements that were written to apply to TOs and TOPs with extensive transmission networks and a wide-area view.

[15] Technical analyses in accordance with Section 215 of the FPA will be required to identify any reliability implications so that no reliability gaps are created. As a result, this initial assessment of risk could be revised based on further analysis. An industry survey also will be used to identify issues to be considered as part of the technical analysis.

The results of these processes result in: (i) time consuming reviews of facts and circumstances required for Registered Entities to attest that specific requirements are not applicable; and/or (ii) unduly burdensome efforts to comply with requirements that are inappropriate to an entity with such limited BES facilities and do not significantly contribute to BES reliability.

Consistent with a risk-based approach to registration, entities that own/operate insignificant BES transmission could be registered as DPs instead of TO/TOPs, and any requirements that must apply to such entities be revised to include such entities in the applicability (hereinafter, "DP/TO registration"). This approach to registration was successful in the GO/TO project, which could be emulated here. As in the GO/TO project, some transmission Facilities that fall below the threshold(s) set for DP registration:

> [a]re more complex and may therefore require individual assessment. The reliability gaps associated with such Facilities should not be addressed simply through application of all standards applicable to Transmission Owners and Transmission Operators, but instead through an assessment of the impact of such a Facility on neighboring transmission Facilities. Such assessment should then be used to determine exactly which Reliability Standards and requirements should apply to that Facility and whether additional entity registration is warranted. This assessment should, at a minimum, be based upon the output of transmission planning and operating studies used by the Reliability Coordinator, Transmission Operator and Transmission Planner in complying with applicable Reliability Standards (specifically, IRO, TOP and TPL).

Order 785 at P 8.

Threshold for DP/TO Registration

The applicability of Requirements R1-R5 of PRC-023-2, which is established by Attachment B to that standard, provides a possible starting point for setting a threshold for DP/TO registration. Based on Attachment B, an entity that owns/operates only transmission lines operated below 200 kV and transformers with low voltage terminals connected at below 200 kV, and whose transmission Facilities do not meet the other criteria in Attachment B, would be registered as a DP. Entities that own other transmission Facilities would be registered as TO/TOP.

Separate consideration should be given to operational responsibility for BES transmission Elements operating at below the threshold.

Standards Applicability

Further analysis is required to determine the TO/TOP standards that should apply to DPs that own/operate only the lower voltage transmission Facilities as defined by PRC-023-2 Attachment B.

Special Considerations for Load-Only Manufacturing Facilities

Because most large manufacturing facilities are served by multiple feeds, this configuration may result in BES classification and therefore a candidate for registration based on the bright-line application of the new BES definition. The following Entity Risk Assessment is proposed to assess whether such a facility poses a material risk to the reliability of the BES. It would normally be applied to candidates for registration as TOs/TOPs because the facility did not qualify for the E1/E3 Exclusions. The key concept underlying the Entity Risk Assessment is that, in the case of these retail loads, BES reliability is assured by the real-time actions of the RC/BA/TOP service providers.

Entity Risk Assessment Applicable to Load-Only Manufacturing Facilities

The following criteria could be applied to load-only manufacturing facilities that become candidates for TO/TOP registration by application of the revised BES Definition, with a rebuttable presumption that the entity should not be so registered if the following criteria are met:

1. No BES behind-the-meter generation at facility.
2. Utility maintains the element (e.g., the interconnecting substation and/or protection equipment under the terms and conditions of the applicable interconnection agreement or tariff).
3. Not an "integrated transmission Element" necessary to provide for the reliable operation of the interconnected transmission grid. Element is embedded in a retail customer facility and serves only a local distribution function.
4. No third-party usage of element under terms and conditions of a FERC-jurisdictional OATT.
5. Wide-area view is not relevant to the facility (e.g., it is a retail load).
6. The following additional factors may be used in support of the above criteria, which include that the organization is not required to participate in SPS (or RAS), UVLS or UFLS programs.

The application of the above criteria would not preclude the ability of the facility's Regional Entity, in consultation with the entity's RC/BA/TOP service providers, to register the facility if the Regional Entity can establish that the facility is material to the reliability of the BES. Such demonstration of materiality shall include a fact-specific analysis reflecting technical judgment.

In the event that such load-only manufacturing facilities are determined to be subject to registration as TO/TOP under this analysis, they could be addressed as a separate subclass such as "Customer Distribution." Review of the TO/TOP Reliability Standards should be undertaken to determine if a sub-list of applicable requirements is appropriate from a risk-based perspective.

Moreover, because tariff and interconnection agreements arise under Section 205 of the FPA, technical analyses in accordance with Section 215 of the FPA will be required to identify any reliability implications so that no reliability gaps are created. The technical analysis should take into the need for coordinating high voltage protection schemes and recognizing dependency by BAs and RPs on reserves, resource adequacy and ancillary services, which are important fundamental aspects needed to support reliability.

As a result, this initial assessment of risk could be revised based on further analysis. An industry survey also will be used to identify issues to be considered as part of the technical analysis.

Transmission Operator (TOP)

Current Definition and/or Threshold in Statement of Compliance Registry Criteria in Statement of Compliance Registry Criteria

Definition

The entity responsible for the reliability of its local transmission system and operates or directs the operations of the transmission Facilities.

Threshold

NERC Rules of Procedure (ROP) Appendix 5B at III.d.1 An entity that owns/operates an integrated transmission Element associated with the Bulk Power System 100 kV and above, or lower voltage as defined by the Regional Entity necessary to provide for the Reliable Operation of the interconnected transmission grid; or

ROP Appendix 5B at III.d.2 An entity that owns/operates a transmission Element below 100 kV associated with a Facility that is included on a critical Facilities list that is defined by the Regional Entity.

> *[Exclusion: A Transmission Owner/Operator will not be registered based on these criteria if responsibilities for compliance with approved NERC Reliability Standards or associated Requirements including reporting have been transferred by written agreement to another entity that has registered for the appropriate function for the transferred responsibilities, such as a Load-Serving Entity, generation and transmission cooperative or joint action agency as described in Sections 501 and 507 of the NERC Rules of Procedure.]*

Functional Model Description

The Transmission Operator operates or directs the operation of transmission facilities, and maintains local-area reliability, that is, the reliability of the system and area for which the Transmission Operator has responsibility. The Transmission Operator achieves this by operating the transmission system within its purview in a manner that maintains proper voltage profiles and System Operating Limits, and honors transmission equipment limits established by the Transmission Owner. The Transmission Operator is under the Reliability Coordinator's direction respecting wide-area reliability considerations, that is, considerations beyond those of the system and area for which the Transmission Operator has responsibility and that include the systems and areas of neighboring Reliability Coordinators. The Transmission Operator, in coordination with the Reliability Coordinator, can take action, such as implementing voltage reductions, to help mitigate an Energy Emergency, and can take action in system restoration.

Note that the Model does not attempt to define what is and is not a transmission facility, versus a generating facility. As discussed in Section II-13, this is assumed to be defined elsewhere by NERC or by governmental authorities.

Maintenance. The Transmission Owner provides the overall maintenance plans and requirements for its equipment, specifying, for example, maintenance periods for its transformers, breakers, and the like. The Transmission Owner then develops or arranges for the development of the detailed maintenance schedules (dates and times) based on the Transmission Owner's maintenance plans and requirements, and provides those schedules to the Reliability Coordinator and others as needed.

The organization serving as Transmission Operator may also physically provide or arrange for transmission maintenance, but it does this under the direction of the Transmission Owner, which is ultimately responsible for maintaining its owned transmission facilities.

Bundled with the Reliability Coordinator or Transmission Owner. A single organization may be the functional entity for multiple Functions. In such a case, the functional entities are said to be "rolled up" or "bundled" into a single organization. An organization may be a Transmission Operator without being a Reliability Coordinator or Transmission Owner. However, in many cases the Transmission Operator is bundled with one of these functional entities.

Bundled with Reliability Coordinator. For example, consider a regional transmission organization (RTO) with several members. The RTO registers with NERC as a Reliability Coordinator and Transmission Operator and is NERC-certified for both. The RTO then delegates/assigns some of the Transmission Operator Tasks to its members.

Bundled with the Transmission Owner. In other situations, the RTO registers with NERC as the Reliability Coordinator, and its members register as Transmission Owners and Transmission Operators. In this case, the Model views the RTO as responsible for complying with Reliability Standards associated with the Reliability Coordinator and would be NERC-certified as such. The RTO members would be responsible for complying with all Reliability Standards associated with the Transmission Operator, and would be NERC-certified as such.

Proposed Elimination
N/A

Proposed Revised Threshold
Yes, see the discussion of registration thresholds, standards applicability and implementation options under Transmission Owner.

Generator Owner (GO)

Current Definition and/or Threshold in Statement of Compliance Registry Criteria in Statement of Compliance Registry Criteria

Definition
Entity that owns and maintains generating units.

Threshold
NERC Rules of Procedure (ROP) Appendix 5B at III.c.1 Individual generating unit > 20 MVA (gross nameplate rating) and is directly connected to the Bulk Power System, or;

ROP Appendix 5B at III.c.2 Generating plant/facility > 75 MVA (gross aggregate nameplate rating) or when the entity has responsibility for any facility consisting of one or more units that are connected to the Bulk Power System at a common bus with total generation above 75 MVA gross nameplate rating, or;

ROP Appendix 5B at III.c.3 Any generator, regardless of size, that is a Blackstart Resource material to and designated as part of a Transmission Operator entity's restoration plan, or;

ROP Appendix 5B at III.c.4 Any generator, regardless of size, that is material to the reliability of the Bulk Power System.

> *[Exclusions: A Generator Owner/Operator will not be registered based on these criteria if responsibilities for compliance with approved NERC Reliability Standards or associated Requirements including reporting have been transferred by written agreement to another entity that has registered for the appropriate function for the transferred responsibilities, such as a Load-Serving Entity, generation and transmission cooperative or joint action agency as described in Sections 501 and 507 of the NERC Rules of Procedure.*
>
> *As a general matter, a customer-owned or operated generator/generation that serves all or part of retail load with electric energy on the customer's side of the retail meter may be excluded as a candidate for Registration based on these criteria if (i) the net capacity provided to the Bulk Power System does not exceed the criteria above or the Regional Entity otherwise determines the generator is not material to the Bulk Power System and (ii) standby, back-up and maintenance power services are provided to the generator or to the retail load pursuant to a binding obligation with another Generator Owner/Operator or under terms approved by the local regulatory authority or the Federal Energy Regulatory Commission, as applicable.]*

Functional Model Description
The Generator Owner owns its generation facilities and provides for the maintenance of those facilities. It also provides verified equipment operating limits and supplies this information to the Generator Operator, Reliability Coordinator, Transmission Planner and Planning Coordinator. In many cases, the Generator Owner has contracts or interconnection agreements with Transmission Owners or Distribution Providers that detail the terms of the interconnection between these parties.

Relationship with the Generator Operator. The organization serving as Generator Owner may operate generation facilities, or arrange for another organization to do so. In addition, the organization serving as Generator Owner may perform maintenance and facility verification, or may arrange with another organization to do so.

Proposed Elimination
N/A

Proposed Modification of Registration Criteria
Recommend section III(c) of the Statement of Compliance Registry Criteria be revised to read:

> *Any owner or operator of one or more Bulk Electric System generating resources*.

Proposed Revised Threshold/Classes of Standards Applicability
The proposal is to establish a small GO/GOP MVA threshold for owners and operators of less than 75 MVA of BES generating units and plants (or other amount agreed upon after further technical analysis), including dispersed power generating resources.

The applicability of MOD-026-1, which is established by the Facilities Applicability section of that standard, could, in conjunction with the risk-based "Verification Conditions" set out in Attachment A to that standard, provide a possible starting point for setting qualification criteria for Small GO/GOP registration. These could include capacity and connection thresholds, as in the Applicability section, as well as consideration of reactive power control, capacity factor, and other appropriate factors, as in Attachment A.

The intent of establishing a small GO/GOP threshold is not to remove any BES generator owners and operators from the registry. Rather, all BES generator owners and operators that meet the BES Definition, as well as the Registry Criteria capacity thresholds (individual units >20 MVA, plant >75 MVA), would remain registered and subject to compliance with applicable GO/GOP standards. For entities that do not exceed the small GO/GOP threshold set in the RBR process, they would be subject only to a defined subset of GO/GOP requirements (discussed below), which is to be determined after further analysis.

The following criteria could be applied to behind-the-meter generation where discretionary sales to the BES may exceed the "net" 75 MVA threshold applicable to behind-the-meter generation under Exclusion E2. These criteria are contingent on the development of a higher risk-based threshold "[X] MVA" as determined through further study:

1. Sales in excess of 75 MVA are energy only but not to exceed [X] MVA.
2. Capacity sales in excess of 75 MVA as requested and directed by the BA, TOP or RC, but not to exceed [X] MVA.
3. Additional factors in support of the above criteria, include that the entity is not a registered TO or TOP (or not otherwise a TO/TOP by virtue of generator tie lines) and does not otherwise affect SOLs or Interconnection Reliability Operating Limits (IROLs).

Proposed Critical Sub-function(s)
The working assumption is that all BES generating resource owners and operators with more than 75 MVA (or other threshold as determined through further study) are providing material amounts of capacity and energy to the BES and that misoperation of such BES resources could have an adverse reliability impact, and should accordingly remain subject to the full set of applicable reliability standards. Owners and operators of Blackstart Resources would also remain subject to full compliance responsibilities.

Analysis and Support for Proposed Action
When the revised BES Definition becomes effective, the Registry Criteria could be simplified to refer to an entity that owns/operates "BES generating units." Entities will thus be registered only if they own/operate BES

generation, i.e., if their generation meets the revised BES Definition or has been added through the exceptions process, and has not been *excluded* through the exceptions process.
The current registration criteria for GOs and GOPs, however, do not distinguish between the owners and operators of a 2,000 MW baseload plant and a 30 MW peaking unit that is primarily used to serve local load centers when market prices are high. Consistent with a risk-based approach to registration, entities that own/operate only insignificant BES generation should be subject only to a subset of GO/GOP standards required to ensure that the interconnection and operation of these resources do not cause or contribute to an adverse reliability impact during normal operations or when contingencies occur on the BES. As the drafting team determined in the MOD-026 Project, it is possible to draw technically sound distinctions among applicable units for modeling and other purposes. The purpose of drawing such distinctions is to lessen undue regulatory burdens on the owners and operators of limited amounts of generating capacity, and better target use of NERC resources on reducing risks to reliable interconnected operations.

As in the GO/TO project, it may be the case that some generators that fall below the threshold(s) set for Small GO/GOP registration are more complex and may therefore require individual assessment.

> The reliability gaps associated with such Facilities should not be addressed simply through application of all standards applicable to [Generator] Owners and [Generator] Operators, but instead through an assessment of the impact of such a Facility on [BES reliability]. Such assessment should then be used to determine exactly which Reliability Standards and requirements should apply to that Facility and whether additional entity registration is warranted. This assessment should, at a minimum, be based upon the output of transmission planning and operating studies used by the Reliability Coordinator, Transmission Operator and Transmission Planner in complying with applicable Reliability Standards (specifically, IRO, TOP and TPL).

Order 785 P 8.

Allowing energy-only sales in excess of 75 MVA would encourage entities with discretionary sales not to withhold power sales to the BES in order to stay below the threshold and avoid registration. Such sales would contribute to market liquidity and could be valuable in emergency situations. The variance would be capped at [X] MVA. Similarly, withholding capacity during high-load or emergency situations (to avoid registration) may have a higher reliability risk profile than exceeding the threshold on a limited basis. Any sales of capacity (such as ancillary services) that exceed the threshold by a behind-the-meter generator at the request of the BA, TOP, or RC should not be grounds for registration. The variance would be capped at [X] MVA.

Standards Applicability
The core standard requirements that need to apply across the board to small GO/GOP generators include those focused on protection systems (PRC) and modeling (MOD). Further analysis is required with respect to other Reliability Standards that should remain applicable, including, but not limited to, EOP-004-2, FAC-008-3, IRO-010, and TOP-006-2.

The task force could identify a common set of Reliability Standards that need to be applied to BES resources owned and operated by small GO/GOPs. This task force could also assess the merits of alternative approaches to targeting registration, standards applicability, and compliance monitoring and enforcement to entity risk. Technical analyses in accordance with Section 215 of the FPA will be required to identify any reliability implications so that no reliability gaps are created. As a result, this initial assessment of risk could be revised based on further analysis. An industry survey also will be used to identify issues to be considered as part of the technical analysis.

The resulting analysis can then be used as the basis for establishing a small GO/GOP registration category and making appropriate revisions to Reliability Standard applicability.

Generator Operator (GOP)

Current Definition and/or Threshold in Statement of Compliance Registry Criteria

Definition

The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services.

Threshold

NERC Rules of Procedure (ROP) Appendix 5B at III.c.1 Individual generating unit > 20 MVA (gross nameplate rating) and is directly connected to the Bulk Power System, or;

ROP Appendix 5B at III.c.2 Generating plant/facility > 75 MVA (gross aggregate nameplate rating) or when the entity has responsibility for any facility consisting of one or more units that are connected to the Bulk Power System at a common bus with total generation above 75 MVA gross nameplate rating, or;

ROP Appendix 5B at III.c.3 Any generator, regardless of size, that is a Blackstart Resource material to and designated as part of a Transmission Operator entity's restoration plan, or;

ROP Appendix 5B at III.c.4 Any generator, regardless of size, that is material to the reliability of the Bulk Power System.

> *[Exclusions: A Generator Owner/Operator will not be registered based on these criteria if responsibilities for compliance with approved NERC Reliability Standards or associated Requirements including reporting have been transferred by written agreement to another entity that has registered for the appropriate function for the transferred responsibilities, such as a Load-Serving Entity, generation and transmission cooperative or joint action agency as described in Sections 501 and 507 of the NERC Rules of Procedure.*
>
> *As a general matter, a customer-owned or operated generator/generation that serves all or part of retail load with electric energy on the customer's side of the retail meter may be excluded as a candidate for Registration based on these criteria if (i) the net capacity provided to the Bulk Power System does not exceed the criteria above or the Regional Entity otherwise determines the generator is not material to the Bulk Power System and (ii) standby, back-up and maintenance power services are provided to the generator or to the retail load pursuant to a binding obligation with another Generator Owner/Operator or under terms approved by the local regulatory authority or the Federal Energy Regulatory Commission, as applicable.]*

Functional Model Description

The Generator Owner may operate its generating facilities or designate a separate organization to perform the Generator Operation Function. The Generator Operator operates, or directs the operation of generation facilities. The Generator Operator supports the needs of the Bulk Electric System up to the limits of the generating facilities in its purview. Ultimately, the Generator Operator's role is to meet generation schedules, manage fuel supplies, and provide frequency support and reactive resources without jeopardizing equipment.

Relationship with the Generator Owner. The organization that serves as Generator Operator may also be the owner of the generation facilities it operates; or it may be a separate organization designated by the Generator Owner to operate the facilities. The Generator Operator receives maintenance and performance verification schedules from the Generator Owner, and develops operating and unit commitment plans based on these schedules.

Relationship with the Transmission Operator. The Generator Operator provides reliability related services through arrangements or by direction from the Transmission Operator for support of the Bulk Electric System. The Generator Operator provides maintenance schedules, generator status, and AVR status to the Transmission Operator. The Generator Operator receives notification of transmission system problems affecting its generator from the Transmission Operator or Reliability Coordinator.

Relationship with the Balancing Authority. The Generator Operator provides unit commitment schedules, generator status, and operating and availability status of generating units to the Balancing Authority.

Relationship with the Reliability Coordinator. The Generator Operator provides annual maintenance plans, and operational data to the Reliability Coordinator. The Generator Operator takes actions based on directives from the Reliability Coordinator for the needs of the Bulk Electric System.

Relationship with Purchasing-Selling-Entity. The Generator Operator receives notice of Arranged Interchange approved by the Purchasing-Selling-Entity.

Proposed Elimination
N/A

Proposed Revised Threshold
Yes, as outlined in the analysis and discussion of Generator Owner. A common technical analysis is required of standards applicable to both functions. An initial review indicates a proportionally *smaller* number of Generator Operator-related requirements would likely be determined to be applicable to small GO/GOP entities than would be the case for Generator Owner-related requirements.

For example, proposed COM-002-2a would require all Small Generator Operators to "have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators [that are] . . . staffed and available for addressing a real-time emergency condition." COM-002-3 would require small GOPs to train staff and be prepared to document the use of three-part communications in communications that are unlikely to take place. Regional Entities would similarly be responsible for ensuring compliance with these requirements.

Appendix B – Current State of Registration Program

NERC's Role

NERC plays several key roles in entity registration. NERC has authority to identify candidates for registration. In addition, NERC reviews registration recommendations and changes to the NCR from Regional Entities. NERC also oversees implementation of the Registration program at the Regional Entities. Finally, NERC is responsible for registering entities, and establishing and maintaining the NCR of the BPS users, owners and operators subject to its Reliability Standards.[16]

Throughout implementation of the Registration program, NERC has provided formal and informal guidance to Regional Entities and industry regarding Registration requirements, roles and responsibilities. This guidance generally has been in response to issues that have arisen in execution of the Registration program, primarily through registration appeals as well as entity sales, mergers, and acquisitions of assets. However, NERC has not defined certain terms used in the Registry Criteria[17] or mandated a set of specific criteria that could result in the addition or removal of an entity from the NCR. NERC also has not prescribed the use of a single web-based portal or common registration form.

In addition, NERC has worked closely with Regional Entity Registration activities and reviewed Registration activities and processes over time, and has recently revised internal oversight processes. As part of this initiative, NERC is reviewing best practices and procedures at the Regional Entities to incorporate them into the proposed design. This white paper identifies a summary of those practices and procedures, as well as possible improvements, such as a common registration form.

Regional Entity's Role

As called for in the NERC Rules of Procedure and its appendices, the Regional Entities identify candidates for registration. In addition, Regional Entities review and evaluate registration requests and changes making recommendations to NERC when a request or change may affect the NCR.

The staffs of the Regional Entities actively participate in NERC-led committees, task forces, and working groups, which facilitate the exchange of information between NERC and the Regional Entities. In addition, the Regional Entities are active participants in the ERO Compliance and Enforcement Management Group (ECEMG) and the Registration and Certification Functional Group (RCFG), both of which are under the oversight of the ERO Executive Management Group, comprised of the chief executive officers of NERC and the eight Regional Entities.

As part of this initiative, the ECEMG was asked to provide a review of the Regional Entity registration practices. A summary of the observations is below:

1. The majority of the Regional Entities use the Registry Criteria to determine materiality. If the entity meets the Registry Criteria, it will be registered and considered material. Some Regional Entities invoke the footnote in Registry Criteria that allows registration of an entity if it is material to the reliability of the BPS, even if it does not meet Registry Criteria.
2. Most Regional Entities have developed internal procedures to implement registration, based on the Registry Criteria. However, some Regional Entities use the Registration Criteria to determine registration candidates and then apply a material or risk "assessment."

[16] *See* http://www.nerc.com/pa/comp/Pages/Registration-and-Certification.aspx.

3. There is no consistency among Regional Entities in defining "materiality." A major objective should be to develop a consistent approach, for use by all Regional Entities, to determine an entity's material impact on BPS reliability.

Functional Model

Users, owners and operators of the BPS are registered by the function they perform, based upon the Functional Model. An entity is registered by function to comply with specific Reliability Standards, because the "Applicability" section of each Reliability Standard is based on the functional approach. However, there are some exceptions (e.g., based on facility characteristics such as radial lines 200 kV and above as called for in FAC-003). Unless an entity is registered for the function to which a Reliability Standard requirement is applicable, it is not responsible for compliance with that requirement.

Fifteen function types are included in the Registry Criteria. These include Balancing Authorities (BAs), DPs, Generator Owners (GOs), Generator Operators (GOPs), Interchange Authorities (IAs), LSEs, Planning Authorities (PAs)/Planning Coordinators (PCs), Purchasing-Selling Entities (PSEs), Reliability Coordinators (RCs), Transmission Planners (TPs), Transmission Owners (TOs), Transmission Operators (TOPs), Resource Planners (RPs), Reserve Sharing Groups (RSGs) and Transmission Service Provider (TSPs). User roles, include but are not limited to, DPs, LSEs, IAs and PSEs. Once registered for a function, entities are generally subject to the full set of Reliability Standards applicable to that function.

Thresholds

NERC's Registration program uses threshold criteria to determine if an entity meets a functional category and qualifies for registration. A user, owner or operator of the BES is considered a user, owner and operator of the BPS. Currently, an entity that meets the threshold criteria is deemed to have a material impact on the reliability of the BPS and thus may be registered, unless a Regional Entity determines otherwise. The NERC Rules of Procedure, and specifically the Registry Criteria in Appendix 5B,[18] provide the flexibility needed to register the appropriate organizations and subject them to applicable Reliability Standard requirements. The Registry Criteria provides for registration of an entity based on a material impact assessment even if it does not satisfy the threshold criteria, and for declining to register an entity that satisfies the threshold criteria based on a determination of lack of material impact. Notwithstanding this flexibility, implementation of the Registration program generally has led to a one-size-fits-all approach for identification of candidates for registration and related Reliability Standard applicability.[19] Inconsistencies in application also appear because terms are not be consistently defined or evaluated in the same way across the Regional Entities.

[18] *See* Registry Criteria at p. 11, "Notes to the above Criteria," Item number 1.

[19] For example, an entity that owns only a single BES 115 kV line or substation cannot specify realistic voltage schedules for generators in accordance with VAR-001 R4 when it is between two neighbors with disparate voltage schedules on their systems; the voltage schedule will be driven by larger neighboring system(s) with a wide-area view and responsibility for BES operations, not the small entity operating limited transmission facilities. Another example is that a small TOP without a wide-area view should not be setting System Operating Limits.

Reliability Standard Applicability

Once registered for a function, an entity is subject to the full set of Reliability Standards applicable to that function. There are a few exceptions, such as a technical or physical limitation (e.g., the entity does not have the asset subject to the Reliability Standard requirement such as SPS, Blackstart units, etc., or has an approved Technical Feasibility Exception, etc.).

However, this approach may result in implementation of the Registration program in a manner that does not take the size and scope of entities, and their role in BES reliability, into account in determinations as to registration and Reliability Standard applicability.

In Order No. 693,[20] and as part of its approval of the revised BES Definition,[21] FERC has encouraged Registered Entities to work with NERC and Regional Entities to determine if a sub-list of Reliability Standard requirements should be applicable to its respective registration. In some limited situations, NERC and the Regional Entities have tailored Reliability Standard requirement applicability for certain functional categories, such that the entity is not automatically subjected to the full scope of standard requirements otherwise applicable to a particular function.[22] This experience has shown that appropriately scoped registration better serves reliability, as it allows entities to increase their focus on their specific reliability and operational obligations, as appropriate to the reliability risk they impose. In addition, NERC's GO/TO project, which led to Order No. 785, "Generator Requirements at the Transmission Interface," demonstrated that this approach can be effective in addressing a class of Registered Entities, as well as on an individual basis.

Registration Types

Once the functional type is identified, there are four categories of entity registration:

1. First, in an Individual Registration scenario, an entity is registered on the NCR for one or more specific functions, and that individual entity accepts full compliance responsibility and accountability regarding Reliability Standard requirements associated with those specific functions.
2. Second, in a Joint Registration Organization (JRO) scenario, an entity registers on behalf of one or more of its members or related entities for one or more functions for which its members or related entities would otherwise be required to register, in accordance with Section 507 of the NERC Rules of Procedure. In this case, the registered entity accepts full compliance responsibility and accountability regarding Reliability Standards associated with those functions.
3. Third, Section 508 of the NERC Rules of Procedure allows two or more entities to register using a Coordinated Functional Registration (CFR). In this case, both entities are registered for one or more applicable function(s) and each is assigned respective responsibility for Reliability Standard requirements applicable to those functions. In a CFR, each registered entity accepts full compliance responsibility and accountability regarding Reliability Standards associated with those functions as listed in the CFR.
4. Finally, entities may be registered as a "concurrent registration" or "co-registration." A concurrent registration may be used when two entities meet the requirements for registration individually and may have an existing arrangement, agreement or contract that assigns responsibility for taking certain reliability actions, but the entities have not entered into a JRO or CFR. In this circumstance, NERC has the ability to register both entities for the same function, and may enforce noncompliance by either or both entities for failure to take the required reliability actions.

---

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

[21] Order Approving Revised Definition, 146 FERC ¶ 61,199 (2014).

[22] *See, e.g., Cedar Creek Wind Energy, LLC*, 139 FERC ¶ 61,214 (2012).

The functional registration of an entity does not preclude it from delegating activities and tasks related to compliance to third parties. In such cases, only the entity that appears on the NCR are held accountable for compliance with applicable Reliability Standards.

Multi-Regional Registered Entity (MRRE)

MRRE is not a formal registration process. NERC and the Regional Entities are separately addressing compliance monitoring and enforcement activities for entities registered in more than one Regional Entity footprint. In some enforcement situations, the Regional Entities have worked together to identify a lead region, such that one of the respective Regional Entities has led enforcement efforts for a given MRRE.

Appendix C – BES Definition

"Bulk Electric System" or "BES" means unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.

Inclusions:

- ***I1*** *- Transformers with the primary terminal and at least one secondary terminal operated at 100 kV or higher unless excluded by application of Exclusion E1 or E3.*
- ***I2*** *- Generating resource(s) including the generator terminals through the high-side of the step-up transformer(s) connected at a voltage of 100 kV or above with:*
  - *a) Gross individual nameplate rating greater than 20 MVA. Or,*
  - *b) Gross plant/facility aggregate nameplate rating greater than 75 MVA.*
- ***I3*** *- Blackstart Resources identified in the Transmission Operator's restoration plan.*
- ***I4*** *- Dispersed power producing resources that aggregate to a total capacity greater than 75 MVA (gross nameplate rating), and that are connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage of 100 kV or above. Thus, the facilities designated as BES are:*
  - *a) The individual resources, and*
  - *b) The system designed primarily for delivering capacity from the point where those resources aggregate to greater than 75 MVA to a common point of connection at a voltage of 100 kV or above.*
- ***I5*** *- Static or dynamic devices (excluding generators) dedicated to supplying or absorbing Reactive Power that are connected at 100 kV or higher, or through a dedicated transformer with a high-side voltage of 100 kV or higher, or through a transformer that is designated in Inclusion I1 unless excluded by application of Exclusion E4.*

Exclusions:

- ***E1*** *- Radial systems: A group of contiguous transmission Elements that emanates from a single point of connection of 100 kV or higher and:*
  - a) *Only serves Load. Or,*
  - b) *Only includes generation resources, not identified in Inclusion I2, I3, or I4, with an aggregate capacity less than or equal to 75 MVA (gross nameplate rating). Or,*
  - c) *Where the radial system serves Load and includes generation resources, not identified in Inclusions I2, I3 or I4, with an aggregate capacity of non-retail generation less than or equal to 75 MVA (gross nameplate rating).*

  Note 1 – A normally open switching device between radial systems, as depicted on prints or one-line diagrams for example, does not affect this exclusion.

  Note 2 – The presence of a contiguous loop, operated at a voltage level of 50 kV or less, between configurations being considered as radial systems, does not affect this exclusion.
- ***E2*** *- A generating unit or multiple generating units on the customer's side of the retail meter that serve all or part of the retail Load with electric energy if: (i) the net capacity provided to the BES does not exceed 75 MVA, and (ii) standby, back-up, and maintenance power services are provided to the generating unit*

or multiple generating units or to the retail Load by a Balancing Authority, or provided pursuant to a binding obligation with a Generator Owner or Generator Operator, or under terms approved by the applicable regulatory authority.

- ***E3*** *- Local networks (LN): A group of contiguous transmission Elements operated at less than 300 kV that distribute power to Load rather than transfer bulk power across the interconnected system. LN's emanate from multiple points of connection at 100 kV or higher to improve the level of service to retail customers and not to accommodate bulk power transfer across the interconnected system. The LN is characterized by all of the following:*

  a) *Limits on connected generation: The LN and its underlying Elements do not include generation resources identified in Inclusions I2, I3, or I4 and do not have an aggregate capacity of non-retail generation greater than 75 MVA (gross nameplate rating);*

  b) *Real Power flows only into the LN and the LN does not transfer energy originating outside the LN for delivery through the LN; and*

  c) *Not part of a Flowgate or transfer path: The LN does not contain any part of a permanent Flowgate in the Eastern Interconnection, a major transfer path within the Western Interconnection, or a comparable monitored Facility in the ERCOT or Quebec Interconnections, and is not a monitored Facility included in an Interconnection Reliability Operating Limit (IROL).*

- ***E4*** *- Reactive Power devices installed for the sole benefit of a retail customer(s).*

  Note - Elements may be included or excluded on a case-by-case basis through the Rules of Procedure exception process.

Agenda Item 6
MRC Meeting
May 6, 2014

Additional Policy Discussion from Board Committee Meetings

Action

Discussion of specific items presented at the Board Committee meetings. Staff presentations made at the Board Committee meetings will not be duplicated at the MRC meeting.

Status

On May 6, 2014, the MRC can expect to continue its increased participation and dialogue during the Board committee meetings in Philadelphia. The MRC will have additional time for policy discussion, as part of its own agenda, to respond to the information that is presented during the committee meetings.

The May 6, 2014 Board committee agendas and associated background materials will be posted on the following webpages:

Finance and Audit Committee Meeting Agenda (agenda to be posted approximately one week prior to the meeting)

Compliance Committee Meeting Agenda

Standards Oversight and Technology Committee Meeting Agenda

Agenda Item 7
MRC Meeting
May 6, 2014

NERC 2015 Business Plan and Budget

Action
Review and Discussion

Background
On May 16, 2014, a consolidated posting of the first drafts of the 2015 NERC and Regional Entity business plans and budgets will be available for a 45-day comment period. On April 22, 2014, in advance of the May 16, 2014 formal posting of the first drafts and prior to the May 6, 2014 MRC meeting, NERC management will be providing the trade associations, the MRC business plan and budget input group and interested stakeholders an update on the development of NERC's business plan and budget, Regional Entity coordination, key priorities and initiatives, as well as preliminary budget estimates. NERC management will also be meeting on April 23, 2014 in closed session with the NERC Finance and Audit Committee to discuss personnel, contract and other matters affecting NERC's 2015 business plan and budget. Management will then present a preliminary overview of the key elements of NERC's draft 2015 business plan and budget at the May 6, 2014 MRC meeting, taking into consideration any input received during the April 22nd and April 23rd meetings. Given the timing of these April meetings, management's presentation for the May 6, 2014 MRC meeting is not anticipated to be available more than a few days in advance of the May 6th MRC meeting. However, the presentation is expected to draw largely upon the information presented at the April 22nd trades meeting which is anticipated to be posted on NERC's website on the 2015 business plan and budget page on or about April 22, 2014.

Following the formal posting of the NERC, Regional Entity and consolidated ERO Enterprise business plans and budgets on May 16, 2014, two open Finance and Audit Committee conference calls are planned for May 21st and July 17th. These conference calls will provide additional opportunities for stakeholder input in the development of the NERC and Regional Entity 2015 business plans and budgets. Stakeholders will also have an opportunity to comment on NERC's final 2015 business plan and budget, which will be posted in mid-July. Each of the Regional Entities also has a process to obtain direct stakeholder input on their business plans and budgets and stakeholders are encouraged to participate in those forums. A complete copy of the 2015 NERC and Regional Entity business plan and budget schedule may be found on NERC's website.

In addition to the 2015 business plan and budget, NERC management will provide a brief update on the approved 2014 performance metrics, and discuss the plan for developing the 2015 performance metrics. The 2014 performance metrics are included with agenda item 12 in the May 7, 2014 Board of Trustees (Board) agenda package that will be posted on the Board agenda webpage.

Agenda Item 8
MRC Meeting
May 6, 2014

2014 Long-Term Reliability Assessment: Development Plan and MRC Input

Action
Information

Status Update
As part of the annual Long-Term Reliability Assessment (LTRA), NERC staff along with regional and industry input, identifies and analyzes the impact of key issues and trends that may affect reliability in the future, such as market practices, industry developments, potential technical challenges, technology implications, and regulatory or legislative policy changes.

The data and information collected for the development of the LTRA reference case incorporates known policies and regulations expected to impact industry throughout the ten-year timeframe, assuming a variety of factors such as economic growth, weather patterns, and system equipment behavior. Over this ten year period (and beyond), a variety of technical challenges to bulk system reliability—largely as a result of emerging regulatory and legislative mandates promoting changes in North America's resource mix—must be well understood and fully evaluated.

Among the variety of potential impacts, NERC must evaluate which long-term issues take priority and have the greatest risk to the reliability of the Bulk Power System. While the LTRA reference case with electric supply and demand projections offer a valuable perspective on the future state of reliability, additional information and guidance from NERC's Operating, Planning, and Member Representatives Committees will enhance the report by offering a more complete explanation of ongoing industry uncertainties and risks – particularly those that may not be captured in the reference case.

The Planning Committee has identified the following high-priority issues impacting long-term planning and operating reliability (in no particular order):

- Resource adequacy concerns in MISO and TRE-ERCOT
- Continued integration of variable generation
- Fossil-fired retirements and coordination of outages for environmental control retrofits
- Increased dependence on natural gas for electric power
- Increased use of demand-side management
- Nuclear generation retirements and/or long-term outages

NERC also continues to monitor other areas of potential concern. While the challenges noted below are considered low-to-medium priority to Bulk Power System reliability than the high-priority issues listed above, NERC will continue to monitor and determine whether these aspects require further evaluation.

- Workforce aging and skills development

- Load forecasting uncertainty
- Smart Grid deployment
- Change in system behavior and composition of system load
- Transmission siting, permitting, and Right-of-Way issues
- Aging infrastructure
- Region/Interconnection-wide modeling and validation
- Operational risks associated with interaction of Special Protection Systems/Remedial Action Schemes
- Global supply chains and fuel reliability
- Coordinated cyber and physical attacks on electricity infrastructure

NERC is seeking guidance from the MRC through a survey mechanism. MRC responses will be used as front-end input for the *2014 Long-Term Reliability Assessment* and also aid the strategic prioritization conducted by the Reliability Issues Steering Committee (RISC). The survey will begin on **May 1, 2014** and continue through **May 30, 2014**.

The survey will focus on the key risk areas noted above, with opportunity to provide open-ended input and long-term reliability policy guidance. The evaluation of these inputs and insights at the early stage of development of the *2014 Long-Term Reliability Assessment* are intended to expand the perspectives of those aspects that could impact the long term Bulk Power System. The proposed schedule for Member Representatives Committee (MRC), Operating Committee (OC), and Planning Committee (PC) input in the development of the report are provided below:

Date	Milestone/Deliverable
Thursday, May 1	Survey Opens for PC, OC, and MRC
Friday, May 30	Survey Closes
Monday, September 8	LTRA sent to PC, OC, and MRC for Review
Tuesday-Wednesday, September 16-17	LTRA Highlights Presented to PC
Thursday, September 25	PC Vote for Report Approval
October TBD	Board of Trustees Approval

In developing comments for the survey, MRC members should also consider the *2013 Long-Term Reliability Assessment*, including the key findings, report structure, and messaging: http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2013_LTRA_FINAL.pdf

Agenda Item 9
MRC Meeting
May 6, 2014

Essential Reliability Services Whitepaper

Action
Information

Status Update

Essential Reliability Services Task Force
The Planning Committee (PC) and the Operating Committee (OC) have formed a task force as a follow-on action to the recommendations from the *2013 Long-Term Reliability Assessment* as well as the results of the California ISO Joint Report last fall. The task force will focus on expanding NERC's methodology for reliability assessment. The approach is expected to include the development of metrics for further evaluation in future long-term reliability assessments and supplement the existing resource adequacy measures. The task force has also developed a technical reference document on essential reliability services (the ERS Whitepaper), which include frequency response, inertia, voltage stability, ramping capability, and other operational requirements needed to ensure Bulk Power System (BPS) reliability.

The PC/OC approved task force scope and roster are included as attachments. The scope and deliverables provide a framework for activities and results anticipated to emerge during the balance of 2014 and into 2015.

Essential Reliability Services Whitepaper
In forming the task force, NERC staff endeavored to develop a foundational whitepaper that could also serve as a technical reference for regulators and policy makers. Informing, educating, and building awareness on the reliability ramifications of the changing resource mix is a prominent NERC reliability function, and is particularly important to provide a foundation for emerging reliability issues.

The objectives of the ERS Whitepaper are listed as follows:

- Identify and define a standardized set of ERS in functional, technology-neutral, performance based terms that can be used to meet the operational needs of the North American BPS.
- Describe why each ERS is important for BPS reliability.
- Describe how each ERS is being stressed given the changes in the overall resource mix.
- Describe how each ERS fits into the overall needs of the BPS in relation to existing services in place as well as the respective inter-relationships.

The whitepaper will be posted on the NERC website on April 23, 2014.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment 1

Essential Reliability Services Task Force (ERSTF) Scope

Background

Essential Reliability Services (ERS) are the elemental 'reliability building blocks' from resources (generation and demand) necessary to maintain Bulk Power System (BPS) reliability. ERS are operational attributes from conventional generation, such as providing reactive power to maintain system voltages and physical inertia to maintain system frequency, necessary to reliably operate the BPS. In contrast, retirement of conventional generation in near future across many areas in North America, coupled with increasing variable generation installation can adversely impact the availability of ERS unless due considerations are given in planning and operations.

There are many factors that contribute to the need for reassessing reliability services. To include a few; variable renewable generation such as distributed, and utility scale solar, and wind generation, retirement of conventional power plants with substantial inertial response capability, increase use of demand response to address load relief, and the change in the operational landscape with integration of renewables and new technology that is used in conjunction with them, like energy storage. The proposed levels of commitment to renewable variable generation is one component of an ongoing shift in resource mix. It is imperative that power system planners and operators understand the potential and cumulative reliability impacts associated with large scale integration of variable generation, an overall capacity reduction in larger base-load generation, increased participation from demand resources and distributed generation, and a more evident increase in reliance on natural gas-fired generation.

As larger amounts of variable generation are added to the system, they have strong potential to displace the traditional large, rotating machines and the operating characteristics those machines and the ancillary benefits to system reliability that these units provided. Variable generation, in particular, has different operating characteristics and responds differently to changes in frequency and voltage on the system. Beyond capacity and energy characteristics, essential reliability services (ERS), such as inertia, frequency response, and voltage control, must be maintained across a given system to ensure reliable operation. These along with other characteristics or functions make up a suite of Essential Reliability Services or ERS.

To meet the needs of the future Bulk Power System, maintaining sufficient ERS will include a mix of market approaches, technology enhancements, and reliability rules or other regulatory rule changes. While the solution sets will likely be different in various regions, it may be necessary for regulators to make appropriate adjustments to market rules and reliability standards that will ensure reliable operation of the BPS.

Purpose

The ERSTF has a multi-faceted purpose that includes developing a technical foundation of ERS; educating and informing industry, regulators, and the public about ERS; developing an approach for tracking and trending ERS; formulating recommendations to ensure the complete suite of ERS are provided and available; and providing guidance necessary for operating a reliable grid. More specifically, the ERSTF will reconcile a collection of analytical approaches for understanding potential reliability impacts as a result of increasing variable resources and how those impacts can affect system configuration, composition, operation and the need for increased ERS. The ERSTF will include membership from existing technical subcommittees and working groups to strengthen the task force platform, and thus producing results which will maintain, enhance, and sustain reliable operation of BPS.

Activities

1. Develop a technical reference document (primer) on ERS. The primer can be used as a reference manual for regulators and policy makers to inform, educate, and build awareness on the reliability ramifications of the elements essential for the reliability of the BPS.
2. Develop an approach and framework for the long-term assessment of essential reliability services to supplement existing resource adequacy assessments. The approach should include a series of metrics that can be continually measured for further evaluation.
    a. Assess impacts on ERS due to increase in variable generation along with retirements of base generation. Articulate how each region is impacted by this scenario.
3. Develop specific recommendations for practices and proposed requirements, including potential reliability standards, that cover the transmission and generation planning, operations planning, and real-time operating procedures.
4. Compose a technically sound guidance document incorporating ERS in operations and operational planning. With retirement of base load generation plants, integration of variable resources and increased use of demand response for load relief; the operational landscape has changed and is projected to continue for near future. Operations personnel will face different methods and modes of operations; for e.g. with increased transmission line construction to accommodate renewable resources, increased number of reactive support devices are installed on the system to compensate for variability of renewables and voltage support. This philosophy and implementation is different from traditional operations with base load generators providing majority of voltage and reactive support.

Based on the work plan generated in this first phase of activity, the OC and PC will determine follow-on activities to support technical committee recommendations, implementation of enhanced reliability assessment approaches, and/or technical guidance to standard drafting teams.

Membership

NERC requests industry's subject experts to continue their efforts and add additional members as needed, with final selection agreed to by the officers of the Planning Committee and Operating Committee. Members must be willing to commit their time to participate in the task force discussions and contribute to writing the final report.

The task force is comprised of the following:

- Co-chaired (OC/PC)
- One representative from each Region
- At least one representatives from the NERC Planning Committee
- At least one representatives from the NERC Operating Committee
- One member-at-large representing Canada
- Additional members can be added:
  - At the request of the Planning and/or Operating Committee sector representatives, or
  - As needed by the NERC coordinator
- One member of the Reliability Assessment Subcommittee (or designated liaison)
- One member of the System Analysis and Modeling Subcommittee (or designated liaison)
- One member of the Resources Subcommittee (or designated liaison)
- One member of the Frequency Working Group (or designated liaison)
- NERC staff coordinator(s)
- Governmental members include, but not limited to:
  - Federal Energy Regulatory Commission
  - United States Department of Energy
  - National Energy Board, Canada

Participation of additional industry subject matter experts may be requested to support task force activities.

The task force co-chairs will be appointed by the chairs of the NERC Planning Committee and Operating Committee. Representation on this task force follows established Planning Committee and Operating Committee guidelines for participation.

Members are appointed by their Region or electric industry sector for two-year terms, without limit to the number of terms. Any Region or electric industry sector may name an alternate representative(s) who may attend task force meetings.

Order of Business

In general, the desired, normal tone of the task force business is to strive for constructive technically sound solutions which also achieve consensus. On the relatively few occasions where that desired outcome cannot be achieved, the task force will defer to a determination by the Planning and Operating Committees to settle the issue. If any strong minority opinions develop, those opinions may be documented as desired by the minority and forwarded to the PC and OC Chair for future meeting consideration.

Reporting

The task force is responsible to the Planning and Operating Committees for the completion of work associated with the scope items outlined above. Final work products of the task force will be approved as necessary by the Planning and Operating Committees and, if necessary, by the NERC Board of Trustees. The task force chairs will periodically apprise the Planning Committee, Operating Committee, and Board of Trustees, as required, on the task force's status, activities, assignments, and recommendations.

Meetings

Weekly to biweekly conference calls can be expected. Additionally, two to three open in-person meetings per year may be needed.

Approved by the NERC Planning Committee: March 5 , 2014

Approved by the NERC Operating Committee: March 5 , 2014

Essential Reliability Services Task Force

Mark Ahlstrom CEO	WindLogics Inc. 1021 Bandana Boulevard East Suite 111 St. Paul, Minnesota 55108	(651) 556-4262 (651) 556-4210 Fx Mark.Ahlstrom@ windlogics.com
Steven D Ashbaker Director of Operations	Western Electricity Coordinating Council 155 N 400 W Suite 200 Salt Lake City, Utah 84103	(801) 883-6840 (801) 582-3918 Fx ashbaker@ wecc.biz
Gerald D Beckerle Senior Transmission Operations Supervisor	Ameren Services 1901 Chouteau Avenue, MC 630 St. Louis, Missouri 63166	(314)-554-6413 gbeckerle@ ameren.com
Layne Brown Manager, Reliability Assessments	Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, Utah 84103	(801) 582-0353 (801) 582-3981 Fx lbrown@wecc.biz
James D. Castle Manager of Reliability Compliance and Industry Affairs	New York Independent System Operator 10 Krey Blvd Rensselaer, New York 12114	(518) 356-6244 jcastle@ nyiso.com
Bob M. Collins Reliability Engineer III	Texas Reliability Entity, Inc. 805 Las Cimas Parkway Suite 200 Austin, Texas 78746	(512) 583-4986 (512) 233-2233 Fx
Bob M. Collins Reliability Engineer III	Texas Reliability Entity, Inc. 805 Las Cimas Parkway Suite 200 Austin, Texas 78746	(512) 583-4986 (512) 233-2233 Fx bob.collins@ texasre.org
David J Devereaux Manager of Control Room Support	Independent Electricity System Operator 2635 Lakeshore Road West Mississauga, Ontario L5J 4R9	905-855-6439 david.devereaux@ ieso.ca
J.S. Holeman Director, Engineering and Training	Duke Energy 526 South Church Street EC02B Charlotte, North Carolina 28202	(704) 382-0011 (704) 382-6938 Fx Sam.Holeman@ duke-energy.com
Richard C Hydzik Transmission Operations Engineer	Avista Corp. 1411 East Mission MSC-16 PO Box 3727 Spokane, Washington 99220-3727	509 495 4005 rich.hydzik@ avistacorp.com
Larry J. Kezele Manager of Operations	North American Electric Reliability Corporation 3353 Peachtree Road, N.E. Suite 600, North Tower Atlanta, Georgia 30326	(609) 273-0839 (404) 446-2595 Fx larry.kezele@ nerc.net
Brendan Kirby	Consult Kirby 12011 SW Pineapple Ct Palm City, Florida 34990	(865) 250-0753 kirbybj@ieee.org

Clyde Loutan Senior Advisor	California ISO 250 Outcropping Way Folsom, California 95630	(916) 608-5917 cloutan@ caiso.com
Paul McCurley Manager, Power Supply and Chief Engineer	National Rural Electric Cooperative Association 4301 Wilson Blvd Arlinagton, Virginia 22203	(703) 907-5867 (703) 907-5517 Fx paul.mccurley@ nreca.coop
Kenneth P. McIntyre Manager Operation and Planning Standards Compliance	Electric Reliability Council of Texas, Inc. 2705 West Lake Drive Taylor, Texas 76574	(512) 248-3969 (512) 248-3969 Fx kmcintyre@ ercot.com
Michael McMullen Director, West Regional Operations	Midcontinent ISO 1125 Energy Park Drive St. Paul, Minnesota 55108	(651) 632-8404 (612) 632-8417 Fx mmcmullen@ misoenergy.org
Michael Milligan Consultant	National Renewable Energy Laboratory 1617 Cole Blvd Golden, Colorado 80401	(303) 384-6927 (303) 384-6901 Fx michael.milligan@ nrel.gov
Edward Scott Director	Duke Energy Florida 6565 38th Avenue N. St. Petersburg, Florida 33710	(727) 384-7500 (727) 384-7994 Fx edward.scott2@ duke-energy.com
JT Thompson Vice President	Constellation Energy 1331 Lamar, Suite 560 Houston, Texas 77010	(443) 213-3674 Fx jt.thompson@ constellation.com
Donald S. Watkins Manager of Technical Operations	Bonneville Power Administration P.O. Box 491 Vancouver, Washington 98666	(360) 418-2344 (360) 418-2963 Fx dswatkins@ bpa.gov
Joel G Wise Manager, Reliability Operations	Tennessee Valley Authority 1101 Market St, PCC 02A Chattanooga, Tennessee 37402	(423) 697-4165 (423) 697-4120 Fx jgwise@tva.gov
David T. Zwergel Sr. Director,Regional Operations	MISO 701 City Center Drive P.O. Box 4202 Carmel, Indiana 46082-4202	(317) 249-5452 (317) 249-5910 Fx dzwergel@ misoenergy.org
Noha Abdel-Karim Senior Engineer Reliability Assessment	North American Electric Reliability Corporation North American Electric Reliability Corporation Atlanta, Georgia 30326	404-446-4699 (202) 644-8099 Fx noha.karim@ nerc.net
Neil Burbure Engineer of Reliability Initiatives and System Analysis	North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, D.C. 20005	(202) 400-3000 (202) 644-8099 Fx neil.burbure@ nerc.net

Samuel D Chanoski Associate Director of Bulk Power System Awareness	North American Electric Reliability Corporation 3353 Peachtree Road, N.E. Suite 600, North Tower Atlanta, Georgia 30326	(404) 446-2560 (404) 904-2480 Fx sam.chanoski@ nerc.net
Robert W. Cummings Director of Reliability Initiatives and System Analysis	North American Electric Reliability Corporation 3353 Peachtree Road, N.E. Suite 600, North Tower Atlanta, Georgia 30326	(404) 446-9717 (404) 446-2595 Fx bob.cummings@ nerc.net
Michael Moon Senior Director of Reliability Risk Management	North American Electric Reliability Corporation 3353 Peachtree Road, N.E. Suite 600, North Tower Atlanta, Georgia 30326	(404) 446-2560 (404) 446-2595 Fx michael.moon@ nerc.net
John Moura Associate Director of Reliability Assessments	North American Electric Reliability Corporation 3353 Peachtree Road, N.E. Suite 600, North Tower Atlanta, Georgia 30326	(404) 446-2560 (609) 610-6044 Fx john.moura@ nerc.net
Pooja Shah Senior Reliability Risk Assurance Engineer	North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, Georgia 30326	(404) 446-2560 (404) 446-2595 Fx pooja.shah@ nerc.net
Jule W. Tate Manager Event Analysis	North American Electric Reliability Corporation 3353 Peachtree Road, N.E. Suite 600, North Tower Atlanta, Georgia 30326	(404) 446-2572 (404) 446-2595 Fx jule.tate@ nerc.net
Philip J. Tatro Senior Performance and Analysis Engineer	North American Electric Reliability Corporation 3353 Peachtree Road, N.E. Suite 600, North Tower Atlanta, Georgia 30326	(404) 446-2560 (404) 446-2595 Fx phil.tatro@ nerc.net

Agenda Item 10
MRC Meeting
May 6, 2014

Five-Year Performance Assessment Update

Action
Information

Background
Pursuant to Federal Energy Regulatory Commission (FERC) regulations, the North American Electric Reliability Corporation (NERC), as the certified electric reliability organization (ERO), is required to submit to FERC, three years after certification and every five years thereafter, a self-assessment of its performance as the ERO and an assessment of the performance of the Regional Entities as parties to delegation agreements with NERC.

Pursuant to the order on the three-year assessment, NERC is required to prepare "a separate section assessing each Regional Entity's satisfaction of statutory and regulatory criteria, and a more detailed discussion of stakeholder comments regarding each Regional Entity" in order to "aid the Commission in making a determination on whether each of the Regional Entities is performing properly under its delegated authority."[1]

The first five-year self-assessment will be filed with FERC on July 21, 2014.

Summary
On March 3, 2014, NERC posted a draft of the five-year performance assessment which consisted of the following: (i) the Statement of Activities and Accomplishments, (ii) a discussion of how NERC meets the ERO certification criteria, (iii) a joint assessment prepared by the Regional Entities assessing their performance over the past five years, (iv) an overview of the comments received in response to the October 2013 survey, and (v) a table showing the status of areas of improvement identified in the order on the three-year performance assessment. NERC received seven sets of comments in response to this posting. These comments will be addressed alongside the October 2013 survey comments in the Statement of Activities.

NERC is currently preparing assessments of the Regional Entities' performance of their delegated functions. NERC expects to post a revised draft of the entire five-year performance, including its assessment of the Regional Entities in June 2014.

NERC is on track to file the five-year performance assessment on or before July 21, 2014. A revised timeline is included below:

[1] *Order on the Electric Reliability Organization's Three-Year Performance Assessment*, 132 FERC ¶ 61,217 at P 36 (2010).

May 6, 2014	Discuss timeline for completing five-year performance assessment at MRC meeting
June 2014	Post second draft of five-year performance assessment, including NERC's assessment of Regional Entity performance Deadline for Regional Entity boards to review or approve, as applicable, joint Regional Entity self-assessment
Early July 2014 July 21, 2014	Review and finalize complete performance assessment File complete performance assessment at FERC File information copies with Canadian jurisdictions

Agenda Item 11
MRC Meeting
May 6, 2014

Update on Regulatory Matters
(As of April 7, 2014)

Action
Information

Regulatory Matters in Canada

1. The second agreement among the North American Electric Reliability Corporation (NERC), the Régie de l'Energie Québec (Régie), and the Northeast Power Coordinating Council (NPCC) regarding implementation of mandatory Reliability Standards in Québec is being developed for consideration by the Québec provincial government. On October 30, 2012, the Régie issued a decision adopting 35 Reliability Standards for Québec. On March 20, 2014, the Régie issued another decision in the same proceeding adopting an additional 7 Reliability Standards for Québec, which brings the total number of adopted standards in Québec to 42. It is expected that the Régie will issue a decision concerning additional Reliability Standards within the same proceeding. Hydro-Québec TransÉnergie, the Québec Reliability Coordinator, has initiated a consultation process on 18 NERC Reliability Standards that will be filed with the Régie once its decision on the pending standards is issued. This filing is expected before the end of 2014. The review of the Sanction Guide proposed by Hydro-Québec TransÉnergie and the determination of Reliability Standards enforcement dates remain pending.
2. The Province of Manitoba (Manitoba) enacted the following in order to establish a new statutory framework for compliance with Reliability Standards in Manitoba: (i) amendments to The Manitoba Hydro Act; (ii) amendments to The Public Utilities Board Act; and (iii) a Reliability Standards Regulation. The Reliability Standards Regulation adopts, by way of a schedule, the NERC / Midwest Reliability Organization (MRO) Reliability Standards applicable to Manitoba registered entities and outlines the Compliance Monitoring and Enforcement Process (CMEP) in Manitoba. In 2013, the Manitoba completed consultations regarding amendment of the Reliability Standards Regulation to adopt new standards developed or revised by NERC since April 1, 2012 and to revise the CMEP to allow a fast-track method of enforcement for minor violations, including the "Find, Fix and Track Process." These CMEP amendments are effective March 25, 2014, and the new standards are effective March 31, 2014.
3. British Columbia has vested the British Columbia Utilities Commission (BCUC) with authority to levy monetary penalties for violations. The BCUC has established an inquiry to consider processes for assessing severity and risk for violations and a possible exception process to the British Columbia Rules of Procedure that govern its Mandatory Reliability Standards regime (this relates primarily to the Bulk Electric System definition and remains pending). On December 12, 2013, the BCUC issued order R-41-13 in response to Mandatory Reliability Standards Assessment Report No. 6 and Addendum,

adopting nine revised NERC Reliability Standards, two errata to the Addendum, and five new or revised defined terms in the NERC *Glossary of Terms*.

4. NERC has filed petitions of several Reliability Standards in Alberta, British Columbia, Manitoba, National Energy Board (NEB), Nova Scotia, Ontario, Québec, New Brunswick, and Saskatchewan.
5. New Brunswick's legislation that amends how Reliability Standards are approved, monitored, and enforced received Royal Assent in New Brunswick and was proclaimed on October 2013. The Act led to the amalgamation of the New Brunswick System Operator (NBSO) with the NB Power Group of Companies. The system operation functions performed by the NBSO are now performed within a vertically integrated NB Power. NBSO's role in the adoption, monitoring, and enforcement of North American reliability standards has been transferred to the New Brunswick Energy and Utilities Board (NBEUB). On December 23, 2013, NBEUB issued version 00 of its Reliability Standards, Compliance and Enforcement Program 2014 Annual Implementation Plan. In accordance with the new legislative requirements, NB Power is required to make an application to the NBEUB within 60 days of FERC's approval of NERC Reliability Standards. Since October 2013, NB Power has filed several applications with the NBEUB for approval of NERC Reliability Standards.
6. The NEB issued an order on December 6, 2012 imposing mandatory Reliability Standards on international power lines (IPL) under the NEB's jurisdiction. The NEB is developing an approach on Administrative Monetary Penalties that might be applicable, as appropriate for violation of Reliability Standards.
7. On February 28, 2014, NERC filed its Fourth Quarter 2013 application for approval of Reliability Standards in Nova Scotia. The Third Quarter 2013 application for approval of five Reliability Standards and updated NERC *Glossary of Terms* in Nova Scotia was approved by the Nova Scotia Utility and Review Board on January 8, 2014.
8. Effective January 1, 2014, the Alberta Electric System Operator (AESO) assumed all responsibilities related to the functions of a Reliability Coordinator. Alberta Reliability Standards related to a Reliability Coordinator will be adopted and this work is underway. The AESO remains an active member and supporter of the WECC and looks forward to a strong working relationship with the adjacent Reliability Coordinators, Peak Reliability and SaskPower. On March 25, 2014, the AESO posted an updated Alberta Reliability Standards Project Plan that tracks the adoption of Alberta Reliability Standards. In particular, NERC Reliability Standards CIP-002 through CIP-011 have been reviewed and are targeted for filing with the Alberta Utilities Commission in June 2014, with a forecasted effective date of the Third Quarter 2016.

FERC Orders Issued Since the Last Update

Please find the FERC orders at the following website:
http://www.nerc.com/FilingsOrders/us/Pages/2014fercordersrules.aspx

NERC Filings Since the Last Update

Please find the NERC filings to FERC at the following website:
http://www.nerc.com/FilingsOrders/us/Pages/nercfilings2014.aspx

Canadian Filings and Orders

Please find the NERC filings to Canadian applicable governmental authorities at the following website:
http://www.nerc.com/FilingsOrders/ca/Pages/default.aspx

Anticipated NERC Filings

1. May 15, 2014 – NERC must submit a compliance filing modifying Violation Risk Factors and Violation Severity Levels in response to FERC's November 22, 2013 order approving Version 5 Critical Infrastructure Protection Reliability Standards. *Docket No. RM13-5-000*
2. May 15, 2014 – Within forty-five days of the end of each quarter, beginning with the quarter ending March 31, 2013, NERC will file with the Commission the unaudited report of the NERC budget-to-actual spending variances during the preceding quarter. This report will include information regarding sources and uses of operating and working capital reserves and will match or exceed the level of detail of the quarterly budget-to-actual variance report of NERC expenditures attached to the agenda of NERC Board of Trustees Finance and Audit Committee's October 2012 meeting. *Docket No. FA11-21-000*
3. May 30, 2014 – NERC must submit a quarterly nuclear data filing in response to Paragraph 629 of Order No. 693. *Docket No. RM06-16-000*
4. May 30, 2014 – NERC must submit a quarterly filing in Nova Scotia of FERC approved Reliability Standards.
5. May 30, 2014 – NERC must submit the true-up filing report of comparisons of actual to budgeted costs for the year 2013 for NERC and the Regional Entities.
6. June 5, 2014 – NERC must submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System (CIP-014 Physical Security Measures). *Docket No. RD14-6-000*
7. June 20, 2014 – NERC must submit an annual compliance filing on implementation of the Find, Fix, Track and Report program. *Docket No. RC11-6-004*
8. July 1, 2014 – NERC must submit a quarterly status report informational filing in response to FERC's January 14, 2014 order related to the motion to defer action on revisions to the Transmission Operations (TOP) and Interconnection Reliability Operations and Coordination (IRO) Reliability Standards. *Docket Nos. RM13-12-000, RM13-14-000, and RM13-15-000*

9. July 21, 2014 – NERC must submit the Five-Year ERO Performance Assessment Report in accordance with the requirements of the Commission's regulations at 18 C.F.R. §39.3(c).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Member Representatives Committee Meeting

May 6, 2014 | 1:00 p.m. – 5:00 p.m. Eastern

Hyatt Regency Philadelphia at Penn's Landing
201 S. Columbus Blvd.
Philadelphia, PA 19106

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Opening Remarks by MRC Chair

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consent Agenda

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Regular Agenda

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Recommended Slate of Stakeholder-Based Members to the Reliability Issues Steering Committee (RISC)

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Request for MRC Members to Serve on the Board of Trustees Nominating Committee

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Responses to the Board's Request for Policy Input

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Risk-Based Registration Initiative

Mark Lauby, Senior Vice President and Chief Reliability Officer

Member Representatives Committee Meeting

May 6, 2014

RELIABILITY | ACCOUNTABILITY

Current Registration Challenges

- Some functions may have minimal impact on reliability
- Must follow all Reliability Standard requirements according to function, regardless of reliability impacts
- Conservative criteria and thresholds used to register entities
- Flexibility to use entity risk, but limited application to date

Risk-Based Registration (RBR) Vision

- Manage risk, ensuring right entities doing the right thing
- Differentiate entities exhibiting different levels of risk
  - Clear thresholds
  - Registration based on thresholds
  - Focused Reliability Standard requirements
- Align with:
  - Bulk Electric System (BES) definition
  - Reliability Assurance Initiative (RAI)
  - Reliability Standard reform
  - Third party audit findings
- Systematic, repeatable and comprehensive process

Tailor Requirements Based on Risk

- Alignment with risk-based concepts and themes
  - RAI
  - BES implementation
  - Reliability Standard applicability efforts
- Centralize review process for risk determinations
  - Establish clear criteria and thresholds
  - Consistent ERO-wide risk-based methods to assess entity's impact

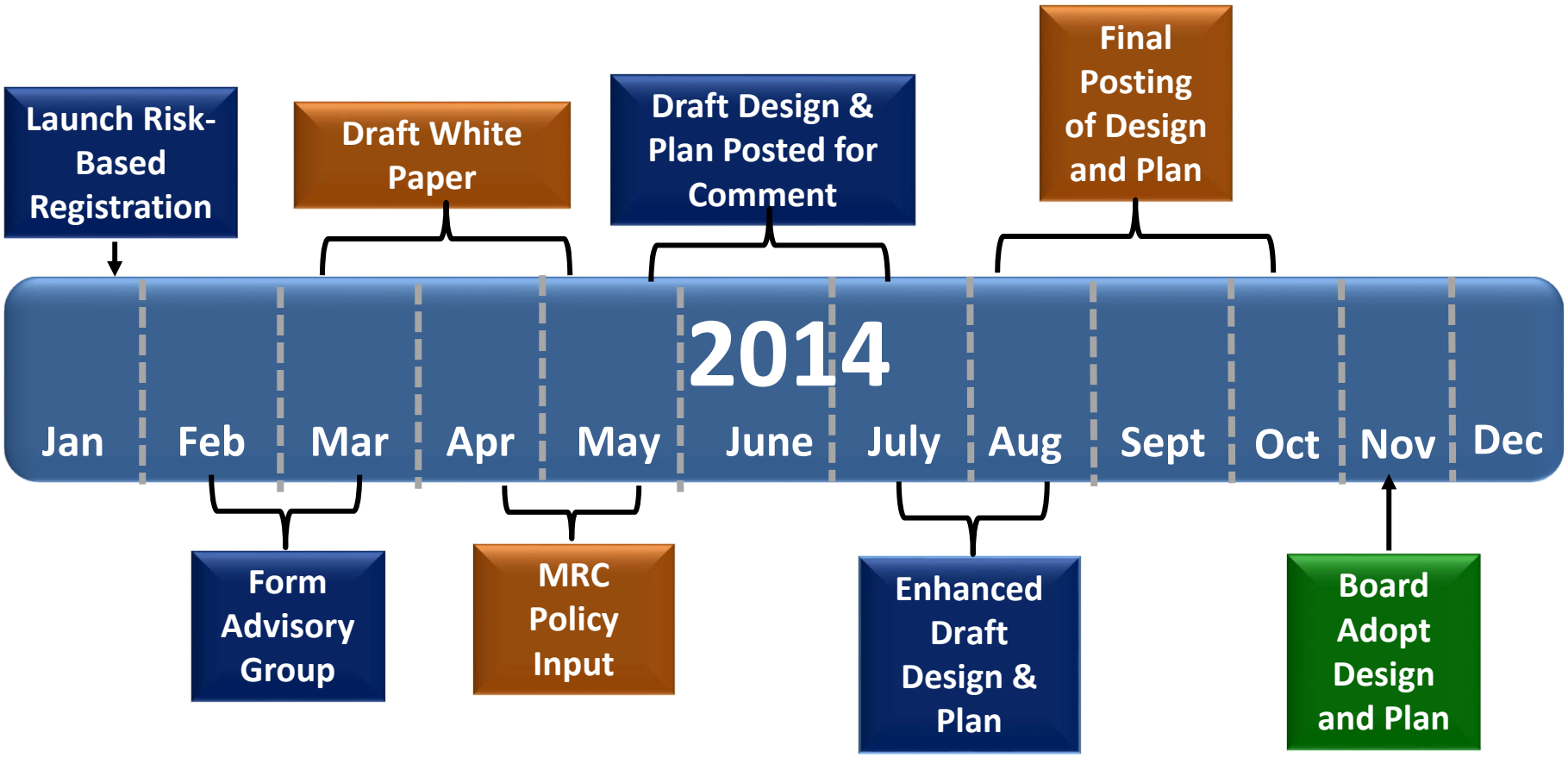
Advisory Group Activities

- Met twice to discuss scope and review draft white paper
- Not all functions require changes to thresholds
- Identified need:
  - Review function and linkage to reliability
  - Process and criteria to identify when entity should be registered
- Formed three *ad hoc* groups for threshold determination
  - Distribution Providers (DPs)/Load-Serving Entities (LSEs)
  - Transmission Owners (TOs)/ Transmission Operators (TOPs)
  - Generator Owners (GOs)/Generator Operators (GOPs)
- Formed one group to assess elimination of Purchasing-Selling Entities (PSE) and Interchange Authorities (IA)
- Draft white paper issued as part of MRC Policy Input Letter

Draft White Paper: Recommendations

- Clarification of terms and improved procedures
- New BES definition as model and anchor for RBR
- Entity risk assessment in a common registration form
- Eliminate functional registrations if not material (PSE & IA)
- Threshold synchronization with the new BES definition
- Standard requirement applicability (DP/LSE, GO/GOP & TO/TOP)
- Status quo for other functional registration categories

RBR Initiative 2014 Timeline



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Potential Alternative Funding Mechanism to Support Expanded Cyber Security Information Sharing and Capabilities

Gerry Cauley, NERC President and CEO
Members Representative Committee Meeting
May 6, 2014

RELIABILITY | ACCOUNTABILITY

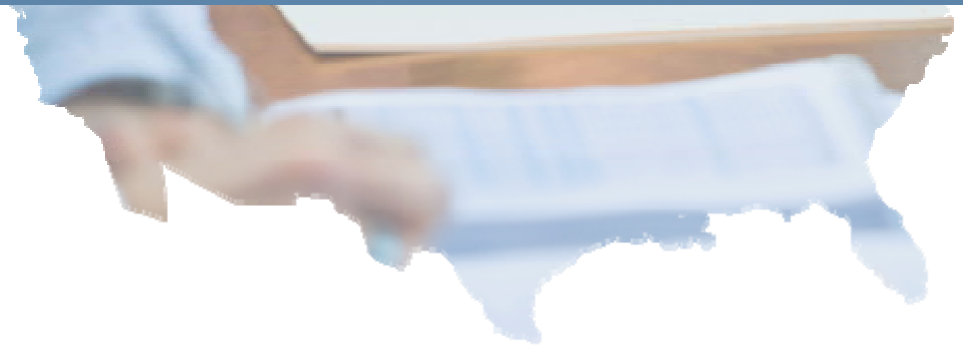
ES-ISAC Organizational Update

- Board adopted policy regarding separation of compliance and enforcement activities
- Recent organizational changes
  - ES-ISAC reports directly to President and CEO
  - CIP auditors transferred to compliance operations
- Moving forward with internal code of conduct further restricting information sharing
- 2015 budget consideration of potential physical separation of ES-ISAC operations within NERC's DC office

CRISP Project Summary – Policy Input Background

- Significant industry interest in project
- Contract/procurement complexity and challenges
- NERC participation tied to minimum level of industry support and resolution of funding and procurement details
- Potential funding from reserves ($200k-$300k) for basic NERC participation
- Policy Input – should NERC consider separate funding directly from CRISP participants to support additional NERC value added analytical services
- Preliminary estimated cost of additional services: $600k-$850k
  - Third party service to store CRISP data
  - Software and hardware to support analyst
  - Additional personnel costs
- Total potential funding $800k-$1.15M

Questions and Answers



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Additional Policy Discussion from Board Committee Meetings

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC 2015 Business Plan and Budget – Draft #1 Overview

Michael Walker, Senior Vice President and Chief Financial and Administrative Officer

Member Representatives Committee Meeting

May 6, 2014

RELIABILITY | ACCOUNTABILITY

Agenda

- **Major Initiatives**
  - Strategic Planning
  - Registration
  - Standards
  - Compliance and Enforcement
  - Reliability Assessments
  - Situation Awareness/Events Analysis
  - Security/ES-ISAC
  - Training
  - Enterprise IT Applications
  - Corporate Services
- **Financial Projections**
- **2015 BP&B schedule**

Strategic Planning Initiatives

- Updated ERO Enterprise Strategic Plan for 2014-2017
  - Improved focus
  - Five goals
  - Metrics- May Board meeting
  - Drives NERC and Regional Entity resource planning and allocation
- 2014 corporate business plan and budget process improvements
  - Improved schedule
  - Coordination with Regional Entities
  - Reliability Issues Steering Committee (RISC) input
- Stakeholder input tracking posted on NERC website; rolling updates

Risk-Based Registration Initiatives

- Deploying sustainable registration program based on reliability risks
- Identifying a properly scoped set of standard requirements, including incorporating BES definition
- Identifying and implementing supporting business processes and systems
- Aligning changes to the registration criteria with other NERC activities

Reliability Standards Initiatives

- Supporting reliability risk management initiatives and process improvements
- Addressing FERC directives
- Continuing to transform standards to steady state
- Improving quality and content of standards
- Facilitating a smooth transition of new standards (e.g. CIP v5 and Physical Security)
- Continuing support of risk-based registration and the development of concurrent RSAWs

Compliance and Enforcement Initiatives

- Implementing consistent RAI techniques and principles
- Facilitating CIP v5 transition
- Auditor training
- Transitioning to single approach compliance monitoring and audit planning
- Identifying and implementing processing efficiencies
- Providing internal controls models
- Initiating compliance phase-in learning for new standards
- Consolidating common set of RSAWs, or successors, for all standards
- Reducing prior caseload

Reliability Assessment and Performance Analysis Initiatives

- Issuing reliability assessments, performance analyses reports
  - 10-year Long-Term Reliability Assessment
  - Two seasonal assessments: Summer and Winter
  - Special Assessment – e.g.: Essential Reliability Services, GMD, TBD
  - Annual State of Reliability Report
- Managing risk registry and prioritization process
  - Risk control strategies
  - Identify and track reliability risk indicators
  - Benchmark and measure reliability performance
- Supporting standards development and response to FERC directives
- Continuing development of reliability database capabilities

Situation Awareness/Events Analysis Initiatives

- Ensuring ERO is aware of BPS events and information is shared
- Collaborating with Forums on joint reliability initiatives and projects
- Keeping industry informed of emerging risks
- Tracking industry responses and providing timely updates
- Facilitating broader analysis of root and contributing causes and related training for industry
- Providing information and analysis to support risk-based methodologies and assessments

Critical Infrastructure Protection Initiatives

- Conducting security incident analyses and identifying lessons learned and security metrics
- Conducting GridSecCon and GridEx, focusing on physical and cyber security
- Coordinating with government agencies on policy issues
- Supporting CIP standards development and implementation
- Working through Critical Infrastructure Protection Committee (CIPC) to address emerging risk issues.

ES-ISAC Initiatives

- Organizational and procedures enhancements providing further separation from compliance operations
- Option of securing additional space in DC office to facilitate further physical separation and security
- Gathering, analyzing and providing secure information regarding cyber threats and vulnerabilities to industry
- Updating portal capabilities and providing self-service access to users for security awareness services

ES-ISAC-CRISP Project

- Industry interest in program but significant procurement and contract issues remain to be resolved-not clear whether project will move forward
- NERC participation at any level will be tied to minimum level of industry support and resolution of funding and procurement details
- Potential funding from reserves ($200-$300k) to fund basic NERC participation as user
- Considering requesting separate funding directly from CRISP participants to support additional NERC value added analytical services
- Preliminary CFM/CRISP resource estimate $600k-$850k
  - Third party service to store CRISP data
  - Software and hardware to support analyst
  - PNNL subscription services
  - 2 additional analyst (FTEs)

Training Initiatives

- Industry training
  - Standards, compliance, root cause analysis, etc.
- ERO Enterprise staff training
  - Regional entity compliance auditors, enforcement, etc.
- System Operator training
  - Initial certification
  - Continuing education
- Internal training
  - NERC employees - policies, information management, handling of confidential information, security, auditor training, etc.

Enterprise Applications

- Applications that support NERC and Regional Entity operations
- Financial update reviewed during FAC meeting
- Additional discussion at SOTC meeting
- Regrouping with Regions on overall strategy and approach
- Increasing focus
  - Controlling pace and costs
  - Improving vendor procurement and contracting
  - Strengthening development oversight and resources

Corporate Services

- Continuing to strengthen internal controls
- Increasing accounting and IT bench strength
- Continuing to evaluate and where practical implement NERC/Regional entity efficiencies
- NERC employee initiatives
  - Building core values into performance management system
  - Training
  - Climate surveys
  - Mentoring
  - Succession planning

NERC Projections

- Less than 1% operating expense increase
- Less than 2 % total increase in operating and capital expenses (net of depreciation)
- 5.7% less than 2015 forecast in 2014 business plan and budget
- Assessment projections under development

NERC Projections (Con't)

- Personnel Costs and Assumptions
  - No net increase in budgeted FTEs over 2014
  - 6% FTE adjustment (attrition, hiring delays)-based on 3 year average
  - 2.5 % average salary increase pool (slightly below 3% market reference)
  - Incentive compensation budgeted at 18.4% of total base salary expense-represents 3 year average
  - Medical and dental benefit plan cost increase based on market data

NERC Projections (Con't)

- 3% reduction in contractor and consulting expense
- Do not include incremental cost for ES-ISAC CRISP participation
  - $200-$300k participant level cost estimate-would increase operating expenses by approximately 0.5%
  - Potential initial funding from reserves
- Do not include cost of potential physical separation of ES-ISAC operations in NERC's DC office
  - $300k per year estimate- would increase operating expenses approximately 0.5%

NERC Projections (Con't)

- Contractor and Consulting Expenses

Consultants & Contracts	2014 BUDGET	2015 BUDGET	INC (DEC) OVER 2014
Total Reliability Standards	-	-	-
			-
Total Regional Entity Oversight	400,000	388,000	(12,000)
			-
Total Reliability Assessments and Performance Analysis	638,085	955,450	317,365
Total Situation Awareness	1,289,108	1,077,321	(211,787)
Total Critical Infrastructure Department	190,000	426,800	236,800
Total ES-ISAC	786,450	703,335	(83,115)
Total Training, Education and Operator Certification	848,830	757,505	(91,325)
Total Policy and External Affairs	75,000	72,750	(2,250)
Total Information Technology	1,944,000	1,629,600	(314,400)
Total Human Resources	257,500	249,775	(7,725)
Total Finance and Accounting	400,000	388,000	(12,000)
TOTAL CONSULTANTS AND CONTRACTS	6,828,973	6,648,536	(180,437)

Cap-x

NERC 2015 CAPITAL BUDGET

Computer & Software CapEx		
ERO Application Development		1,700,000
Generation Data Software		200,000
Hardware		100,000
	$	2,000,000
IT Hardware and Software		
Disaster Recovery		250,000
Data Storage		325,000
Replacement servers		202,000
NERC Software licenses		350,500
Replacement laptops		126,000
Total Computer & Software CapEx	$	1,253,500
Equipment CapEx		
Replacement network devices	$	365,000
Total Capital Budget	**$**	**3,618,500**

NERC Projections (con't)

Statement of Activities and Fixed Assets Expenditures
2014 Budget & Projection, and 2015 Budget
STATUTORY

	2014 Budget	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)	% Inc 2015 over 2014
Expenses				
Total Personnel Expenses	**$ 34,059,654**	**$ 35,159,894**	**$ 1,100,240**	**3.2%**
Total Meeting Expenses	**$ 3,789,525**	**$ 3,476,246**	**$ (313,280)**	**-8.3%**
Total Operating Expenses	**$ 17,612,133**	**$ 17,234,950**	**$ (377,184)**	**-2.1%**
Other Non-Operating Expenses	**$ 144,000**	**$ 144,000**	**$ -**	
Total Expenses	**$ 55,605,313**	**$ 56,015,089**	**$ 409,776**	**0.7%**
Fixed Assets				
Depreciation	$ (2,333,006)	$ (2,333,006)	$ 0	
Computer & Software CapEx	2,904,790	3,253,500	348,710	
Equipment CapEx	213,000	365,000	152,000	
Inc(Dec) in Fixed Assets	**784,784**	**1,285,494**	**500,710**	**63.8%**
TOTAL BUDGET	**$ 56,390,096**	**$ 57,300,583**	**$ 910,486**	**1.6%**
FTEs	**189.53**	**189.48**	**-**	

Assessments

- Projections under development
- Posted on May 16th
- Multiple factors considered
  - NERC and Regional Entity budgets and funding requirements
  - Year end working capital and operating reserve projections
  - Loss $1.2M offset applied to reduce NERC assessments in 2014
  - NERC capital financing plan
  - Penalty offsets
  - Presence or absence of excess reserve offsets at Regions
  - Need to consider reserve requirements over planning period

Remaining Schedule

- May 16 - post NERC, Regional Entity BP&Bs and Consolidated Budget and Assessment Projection-45 day comment period
- May 20 - FERC budget staff briefing
- May 21 - FAC Webinar to review 1st drafts
- July 9 - closed FAC call/meeting to review proposed final budget and assessments
- July 15 - post and distribute final NERC and Regional Entity BP&Bs and assessments to FAC
- July 17 - FAC conference call/webinar for management review of final NERC and Regional Entity BP&Bs

Remaining Schedule (Con't)

- August 13 – FAC meeting to recommend approval of final NERC, Regional Entity BP&Bs and assessments
- August 14 – Board of Trustees meeting to approve final NERC BP&B, Regional Entity BP&Bs and assessments
- August 23 – Submit NERC and Regional Entity BP&Bs and assessments to FERC for approval, with subsequent filings with Canadian authorities

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2014 Long-Term Reliability Assessment: Development Plan

John Moura, Director of Reliability Assessment

Member Representatives Committee Meeting

May 6, 2014

RELIABILITY | ACCOUNTABILITY

Proposed Key Issues for 2014 Long-Term Reliability Assessment

- Accommodating system needs and adapting to change
- Continued integration of variable generation
- Generation retirements and coordination of outages
- Increased dependence on natural gas
- Increased use of demand-side management
- Nuclear generation retirements and/or long-term outages

Seeking MRC Guidance

- Short survey now open
- Opportunity for open-ended input and policy guidance
- Responses will strengthen front-end input
- Support will aid the strategic prioritization by RISC
- Focus on six key risk areas
- Open format to identify other long-term risks

Survey and Report Schedule

Date	Milestone/Deliverable
Thursday, May 1	Survey opens for PC, OC, and MRC
Friday, May 30	Survey closes
Monday, June 2	LTRA development and analysis begins
Monday, September 8	LTRA sent to PC, OC, and MRC for review
Tuesday-Wednesday, September 16-17	LTRA highlights presented to PC
October TBD	Board approval and report published

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Essential Reliability Services Whitepaper

John Moura, Director of Reliability Assessment

Member Representatives Committee Meeting

May 6, 2014

RELIABILITY | ACCOUNTABILITY

Recommendation from 2013 LTRA

Develop primer on essential reliability services (ERS):

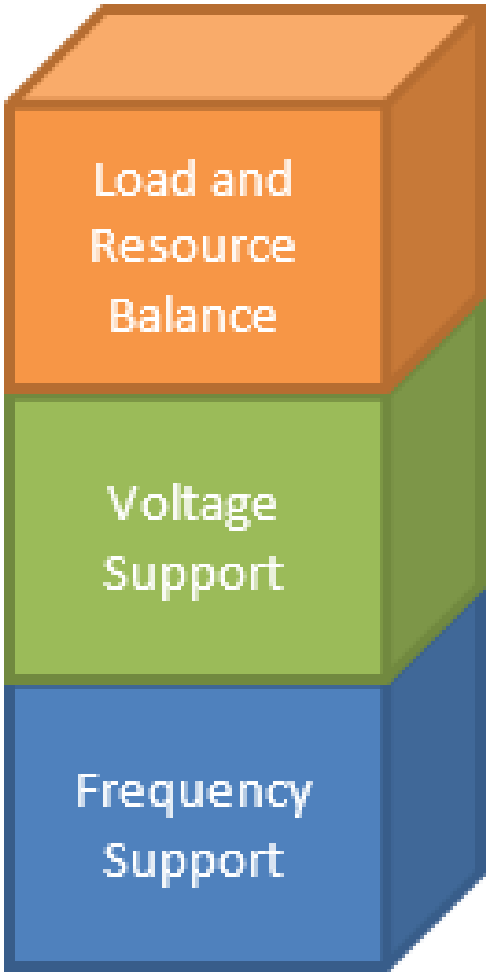
- Develop a reference document on ERS
- Operational requirements needed to ensure bulk power system (BPS) reliability

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Objectives

- Identify a standardized set of ERS
  - Simple tutorial
  - Functional, technology neutral, and performance-based
- Describe the importance for BPS reliability
  - How does the resource mix change affect ERS?
  - What happens when you don't have ERS?
- **Target Audience:** regulators, policy makers, and industry leadership

ERS Fundamentals



- "Building blocks" of physical capabilities
- Accentuated by resource changes
- Some partly covered through ancillary services
- Accommodate local/regional needs

Six Essential Reliability Services

- Operating Reserve
- Frequency Response
- Ramping Capability
- Active Power Control
- Reactive Power and Voltage Control
- Disturbance Ride-Through Tolerance

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Next Steps

- Whitepaper provides a foundation for the task force
- Task force will develop an analytical assessment framework
  - How is the analysis performed for each ERS?
  - What data is needed?
  - What parameters gauge acceptable levels of ERS?
  - How do the parameters relate to the overall resource mix?
- Framework expected in Q4 2014
- Final assessment completed in 2015

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Five-Year ERO Performance Assessment

Willie L. Phillips, Assistant General Counsel

Member Representatives Committee Meeting

May 6, 2014

RELIABILITY | ACCOUNTABILITY

Initial Draft Posting

- Posted on March 3, 2014
- NERC received **seven** sets of comments

Comment Highlights

- **Enforcement**
  - Imposing penalties for administrative violations
  - Impact of the find, fix, and track (FFT) process
- **Compliance**
  - Measuring success of “risk-based” approach to compliance
  - Assess impact of Reliability Assurance Initiative (RAI)

Next Steps

- Update NERC Statement of Activities and Accomplishments
- Individual Regional Entity assessments of enforcement and compliance
- NERC's response to industry comments on initial posting

Timeline

- **May 4:** Preview Regional Entity assessments with ERO Boards
- **End of May:** Finalize Regional Entity assessments
- **June:** Post revised draft of five-year assessment
- **July 21:** File five-year assessment with FERC

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Regulatory Update

RELIABILITY | ACCOUNTABILITY

MEETING LOCATION

Hyatt Regency Philadelphia at Penn's Landing
201 S. Columbus Blvd.
Philadelphia, PA 19106
215-928-1234

All times are Eastern.

Schedule of Events – Industry
May 6-7, 2014 — Philadelphia, PA

Conference Calls Before the May 2014 Meetings	
May 1, 2:00 p.m. to 3:00 p.m.	Corporate Governance and Human Resources Committee **OPEN** Conference Call
Tuesday, May 6, 2014	
8:45 a.m. to 9:45 a.m. **Room name: Grand Ballroom**	Finance and Audit Committee – **OPEN** Session
10:00 a.m. to 11:00 a.m. **Room name: Grand Ballroom**	Compliance Committee – **OPEN** Session
11:00 a.m. to 12:00 p.m. **Room name: Grand Ballroom**	Standards Oversight and Technology Committee – **OPEN** Session
12:00 p.m. to 1:00 p.m. **Room name: Columbus Ballroom AB**	**Lunch**
1:00 p.m. to 5:00 p.m. **Room name: Grand Ballroom**	Member Representatives Committee – **OPEN** Session
5:30 p.m. **Location: Columbus Ballroom AB**	**Reception**
Wednesday, May 7, 2014	
8:30 a.m. to 12:00 p.m. **Room name: Grand Ballroom**	Board of Trustees Meeting

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Board of Trustees

April 23, 2014 | 2:30 p.m. – 3:00 p.m. Eastern

NERC
1325 G Street NW
Suite 600
Washington, DC 20005

Participant Dial-In: 1-800-750-5857

Call to Order

NERC Antitrust Compliance Guidelines and Public Announcement

1. **Physical Security Reliability Standard Update— Information**
2. **Adjournment**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Board of Trustees

May 7, 2014 | 8:30 a.m. - Noon Eastern

Hyatt Regency Philadelphia at Penn's Landing
201 S. Columbus Blvd.
Philadelphia, PA 19106
215-928-1234

Call to Order

NERC Antitrust Compliance Guidelines and Public Announcement

Consent Agenda — Approve

1. **Minutes***
   a. February 6, 2014 Meeting
2. **Committee Membership and Charter Changes***
   a. Compliance and Certification Committee Membership
   b. Compliance Processes and Procedures Subcommittee Formation
   c. Critical Infrastructure Protection Committee Membership
   d. Personnel Certification Governance Committee Membership

Regular Agenda

3. **Opening Remarks by Board Chair**
4. **Remarks by FERC Commissioner Cheryl LaFleur**
5. **Remarks by FERC Commissioner Tony Clark**
6. **Remarks by Mr. Denis O'Brien, CEO, Exelon Utilities**
7. **President's Report**

8. **Standards***
    a. Demand Data (MOD C) – MOD 031-1 — **Adopt**
    b. Voltage and Reactive Control – VAR-002-3 – **Adopt**
    c. Operating Personnel Communictions Protocols – COM-002-4 – **Adopt**
    d. Violation Risk Factor/Violation Severity Level Revisions – **Adopt**
        - TPL-001-4
        - CIP Version 5 (CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-008-5, CIP-009-5)
        - MOD-026-1 and MOD-027-1
        - PRC-005-2 and PRC-005-3
        - BAL-003-1
    e. Physical Security Standard — **Information**
9. **Amendments to SERC Bylaws* – Approve**
10. **State of Reliability Report*— Information**
11. **Summer Assessment*— Information**
12. **ERO Strategic Plan Metrics – Approve**
13. **Canadian Affairs – Jim Burpee — Information**
14. **Committee Reports***
    a. Operating Committee
    b. Planning Committee
    c. Critical Infrastructure Protection Committee
    d. Member Representatives Committee
    e. Personnel Certification Governance Committee
    f. Standards Committee
    g. Reliability Issues Steering Committee
        i. Charter Amendments – **Approve**
        ii. Committee Membership Appointments – **Approve**
    h. Compliance and Certification Committee
        i. 2014-2016 Work Plan – **Approve**
        ii. 2013 Stakeholder Perception Survey Results and Report Recommendations – **Accept**
    i. Electricity Sub-Sector Coordinating Council

15. **Forum and Group Reports***
    a. North American Energy Standards Board
    b. Regional Entity Management Group
    c. North American Transmission Forum
    d. North American Generator Forum
16. **Board Committee Reports**
    a. Corporate Governance and Human Resources
        i. Compliance Committee Mandate Amendments – **Approve**
    b. Compliance
    c. Finance and Audit
        i. 2013 Audit Financial Statements – **Accept**
        ii. First Quarter Statement of Activities – **Accept**
    d. Enterprise-wide Risk
    e. Standards Oversight and Technology

***Background materials included.**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Minutes
Board of Trustees

Agenda Item 1.a

February 6, 2014 | 8:30 a.m.-12:00 p.m. Mountain

Arizona Grand Resort & Spa
8000 S. Arizona Grand Parkway
Phoenix, AZ 85044

Call to Order and Chair's Remarks

Chair Frederick W. Gorbet called to order the duly noticed open meeting of the Board of Trustees ("Board") of the North American Electric Reliability Corporation ("NERC") on February 6, 2014, at 8:30 a.m. Mountain, and a quorum was declared present. The agenda is attached as **Exhibit A**.

Present at the meeting were:

Board Members:
Frederick W. Gorbet, Chair
Paul F. Barber
Janice B. Case
Gerald W. Cauley, President and Chief Executive Officer
Robert G. Clarke
David Goulding
Douglas Jaeger
Kenneth G. Peterson
Bruce A. Scherr
Jan Schori
Roy Thilly

NERC Management
Charles A. Berardesco, Senior Vice President, General Counsel, and Corporate Secretary
Matthew Blizard, Director of Critical Infrastructure Protection
Thomas Burgess, Vice President and Director of Reliability Assessment and Performance Analysis
Mark G. Lauby, Vice President and Director of Standards
Michael Moon, Senior Director of Reliability Risk Management
Mark Rossi, Senior Vice President and Chief Operating Officer
Janet Sena, Senior Vice President and Director of Policy and External Affairs
Earl Shockley, Senior Director of Compliance Operations
Brady Walker, Associate Counsel
Michael Walker, Senior Vice President, Chief Financial and Administrative Officer, and Corporate Treasurer

A listing of industry attendees is attached as **Exhibit B.**

Mr. Gorbet acknowledged and welcomed Mr. Ken Quesnelle, Chair of the Canadian Association of Members of Public Utility Tribunals, and Mr. Richard M. Rosenblum, President and CEO of the Hawaiian Electric Company ("HECO").

NERC Antitrust Compliance Guidelines

Mr. Berardesco directed the participants' attention to the NERC Antitrust Compliance Guidelines included in the agenda, and offered to answer any additional questions the participants had at any time regarding antitrust compliance or other matters.

Executive Session

Mr. Gorbet reported that before the open meeting, as is its custom, the Board met in closed session with NERC management, and subsequently in executive session without NERC management, to review NERC management activities.

Consent Agenda

Upon motion duly made and seconded, the Board approved the consent agenda as follows:

Minutes

The draft minutes for the November 7, 2013 Board meeting, and for the November 21, 2013 and December 20, 2013 Board conference calls, were approved in the form as presented to the Board at the meeting.

Committee Charter Amendments

Standards Committee Charter Amendments

RESOLVED, that the Board hereby approves the amended Standards Committee Charter, substantially in the form presented to the Board at this meeting, to replace the SC Charter approved by the Board on February 7, 2013.

Committee Membership Appointments

Critical Infrastructure Protection Committee

RESOLVED, that the Board hereby approves the election of the following individuals to the Executive Committee of the Critical Infrastructure Protection Committee, each for a term of two years, effective January 1, 2014:

- David Grubbs of the City of Garland
- Marc A. Child of Great River Energy
- Ross Johnson of Capital Power

Compliance and Certification Committee

RESOLVED, that the Board hereby appoints to the Compliance and Certification Committee Silvia Parada-Mitchell, NextEra Energy, for a term of three years.

Welcoming Remarks of Chair Gorbet

Mr. Gorbet welcomed and introduced Mr. Quesnelle and Mr. Rosenblum.

Remarks by Ken Quesnelle

Mr. Quesnelle commented on the significance of the distinctions between the regulatory frameworks of the United States and the Canadian Provinces. He emphasized that a close relationship between NERC and Canadian regulators is essential to building a clear, mutual understanding of the mandates governing each party, and in managing the "seams" issues that often arise.

Mr. Quesnelle referenced a discussion from the previous day regarding "right-sizing" regulation, and identified this as a key factor in creating value for both the industry and for the public at large. He gave several specific examples of the application of this principle, including (i) the adaptation of ancillary services to the introduction of variable generation resources, and (ii) NERC's registration methodology.

Remarks by Richard Rosenblum

Mr. Cauley gave a brief introduction in which he explained why Mr. Rosenblum's attendance at the meeting was particularly important. Specifically, he referenced the joint NERC-California ISO report that had been finalized in November of 2013, and identified some of the operational challenges that penetration of variable generation resources to levels of 20 to 30% of demand can create. Mr. Cauley described these challenges as non-traditional, in the sense that they are not capacity-related and include issues like responsive reserves, load following, frequency response, and voltage control. He described how these factors had historically been taken for granted by system operators because they were inherent in the nature of the North American generation fleet.

Mr. Cauley referenced an increasing push in many jurisdictions toward the greater incorporation of variable generation resources, and identified highlighting these non-traditional challenges for policy makers as a key role for NERC in the coming year. To this end, he noted that he had instructed NERC management to (i) produce a report by early spring presenting these issues in a way that is understandable to policy makers, and (ii) conduct a special assessment that examines regions where the 20 to 30% penetration of variable generation resources is becoming an operational reality. Mr. Cauley emphasized that NERC would highlight these challenges for policy makers while remaining neutral regarding the appropriateness or inappropriateness of any particular generation policy. He identified Hawaii as a region at the forefront of dealing with these issues, and stated that Mr. Rosenblum's willingness to discuss his experience as president and CEO of HECO was therefore particularly important to better understanding these challenges.

Mr. Rosenblum identified some of the technical challenges that HECO has experienced from a reliability perspective as a result of the large-scale integration of variable generation resources. He described these challenges in the context of Hawaii's uniqueness, namely (i) its high cost of generation, (ii) its complete isolation from other interconnected transmission systems, and (iii) the high cost and relative scarcity of available land for constructing new generation facilities. Mr. Rosenblum noted that approximately 10% of HECO customers are currently utilizing rooftop photovoltaic systems, and predicted that this number would increase in the coming years. He noted that he was not taking a position on any particular policy that encourages or discourages the deployment of these resources.

Chairman's Report on Closed Strategic Planning Session

Mr. Gorbet reported that the Board met in a duly noticed closed session in January to discuss a variety of topics, and noted that the Board did not take any action at this meeting. Among the topics discussed were (i) the Three-Year ERO Strategic Plan, (ii) corporate metrics, (iii) preparation of the business plan and budget, and (iv) the relationship between NERC and the Regional Entities.

President's Report

Mr. Cauley noted some of the major achievements of NERC in the past year, and described how these achievements helped to clarify the future goals of the ERO enterprise. Among these achievements, he identified:

1) The significant improvement in the development of Reliability Standards, including (i) the definition of Bulk-Electric System ("BES"), (ii) Geomagnetic Disturbance ("GMD"), and (iii) Critical Infrastructure Protection Version 5 Reliability Standards;
2) The success of NERC's Find, Fix and Track initiative;
3) The progress in the initial development of the Reliability Assurance Initiative ("RAI");
4) Increased communication, engagement, and collaboration with U.S. and Canadian regulatory authorities; and
5) The steps NERC has taken to improve reliability, including (i) vegetation management, (ii) the three-year program on right-of-way maintenance, and (iii) the 345kV circuit breaker alert.

Lastly, Mr. Cauley described the ongoing work between NERC and Regional Entity management, and cited the development of a "Roles and Responsibilities" operations whitepaper that establishes a vision for the ERO in terms of integration and the resolution of internal seams issues. He noted that the whitepaper identified eleven action items, and that he had preliminarily reviewed it with the Board. Mr. Cauley stated that NERC's intention was to review the whitepaper again with the Board and with the Regional Entity Board chairs and vice chairs in May. He further stated that NERC planned to report back to the Member Representatives Committee ("MRC") and to the Board in the coming 12 to 24 months regarding the progress made on integrating ERO infrastructure, policies and practices. Mr. Cauley anticipated that the whitepaper would be made public once he received concurrence from the Regional Entity CEOs.

Election and Appointment of Officers

Upon motion duly made and seconded, the Board appointed the following officers for 2014:

- Frederick W. Gorbet, Chair
- Paul F. Barber, Vice Chair
- Gerald W. Cauley, President and Chief Executive Officer

Upon recommendation of the President, and upon motion duly made and seconded, the Board appointed the following individuals as officers of the corporation:

- Mark Rossi, Senior Vice President and Chief Operating Officer
- Charles A. Berardesco, Senior Vice President, General Counsel, and Corporate Secretary
- Janet Sena, Senior Vice President
- Michael Walker, Senior Vice President, Chief Financial and Administrative Officer, and Corporate Treasurer
- Thomas Bugress, Vice President
- Mark G. Lauby, Vice President

Board of Trustees' Self-Assessment Review

Mr. Gorbet provided an overview of the Board of Trustees' Self-Assessment results and the Member Representatives Committee Board Effectiveness Survey results. Mr. Gorbet stated the Board takes seriously comments on its performance and indicated the Trustees will work with the MRC to address areas identified for improvement.

Three-Year ERO Strategic Plan

Mr. Cauley noted feedback on the Three-Year ERO Strategic Plan that had been received the previous day at the meetings of the Corporate Governance and Human Resources Committee ("CGHRC") and the MRC. In particular, he identified these comments as relating to (i) replacing the term Bulk-Power System "BPS" with the term "BES," and (ii) augmenting the objective regarding the development of a new framework for registration and deregistration of entities. Mr. Cauley recommended that the Board approve the Three-Year ERO Strategic Plan with these two changes, and permit the Plan to become a driving document in the coming months while NERC and the Regional Entities develop their business plans and budgets. He stated that all of the comments received would be compiled into a matrix that indicated how they were addressed. Mr. Cauley also noted that the Three-Year ERO Strategic Plan is reexamined by the Board every year, creating additional opportunities for comments to be incorporated. Lastly, he noted that the metrics associated with the Three-Year ERO Strategic Plan had been separated out, and that an updated version of these metrics would be presented to the CGHRC in March. Upon motion duly made by Mr. Gorbet and seconded by Ms. Schori, the Board approved the Three-Year ERO Strategic Plan, subject to the two changes discussed above and without the associated metrics, as follows:

> RESOLVED, that the Board hereby approves the Three-Year ERO Strategic Plan, substantially in the form presented to the Board at this meeting.

Standards

Mr. Lauby provided an overview of the Reliability Standards program and presented the following items for Board action. After discussion, and upon motions duly made and seconded, the Board approved the following resolutions:

Coordinate Interchange Standards – INT-004-3, INT-006-4, INT-009-2, INT-010-2, INT-011-1

RESOLVED, that the Board hereby adopts, subject to ballot body approval of the definitions for "Request for Interchange" and "Arranged Interchange," the following proposed Coordinate Interchange Reliability Standards, as presented to the Board at this meeting:

- INT-004-3—Dynamic Transfers;
- INT-006-4—Evaluation of Interchange Transactions;
- INT-009-2—Implementation of Interchange;
- INT-010-2—Interchange Initiation and Modification for Reliability;
- INT-011-1—Intra-Balancing Authority Transaction Identification.

FURTHER RESOLVED, that the Board hereby approves the associated implementation plan, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the revised and new NERC Glossary definitions, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Violation Risk Factors and Violation Severity Levels for the proposed Reliability Standards, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Reliability Standards proposed for retirement, as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities.

Operations Personnel Training—PER-005-2

RESOLVED, that the Board hereby adopts proposed Reliability Standard PER-005-2, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the associated implementation plan, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the new NERC Glossary definitions, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Violation Risk Factors and Violation Severity Levels for the proposed Reliability Standard, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Reliability Standard proposed for retirement, as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities.

Available Transmission System Capability—MOD-001-2 (MOD A)

RESOLVED, that the Board hereby adopts proposed Reliability Standard MOD-001-2, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the associated implementation plan, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Violation Risk Factors and Violation Severity Levels for the proposed Reliability Standard, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Reliability Standards proposed for retirement, as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities.

Modeling Data—MOD-032-1, MOD-033-1 (MOD B)

RESOLVED, that the Board hereby adopts the following proposed Modeling Data Reliability Standards, as presented to the Board at this meeting:

- MOD-032-1—Data for Power System Modeling and Analysis;
- MOD-033-1—Steady-State and Dynamic System Model Validation.

FURTHER RESOLVED, that the Board hereby approves the associated implementation plan, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Violation Risk Factors and Violation Severity Levels for the proposed Reliability Standards, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Reliability Standards proposed for retirement, as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities.

Voltage and Reactive Control—VAR-001-4

RESOLVED, that the Board hereby adopts proposed Reliability Standard VAR-001-4, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the associated implementation plan, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Violation Risk Factors and Violation Severity Levels for the proposed Reliability Standard, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Reliability Standard proposed for retirement, as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities.

Operating Personnel Communications Protocols—COM-002-4

Mr. Gorbet noted a productive discussion the previous day in both the Standards Oversight and Technology Committee ("SOTC") and the MRC. Mr. Gorbet stated that the Board is prepared to leave the decision regarding the appropriate next steps for COM-002-4 to the Standard Drafting Team. Mr. Gorbet expressed his hope that the Standard Drafting Team will be expeditious in whatever course it decides to take.

Reliability Standards Reaffirmed by Periodic Review

RESOLVED, that the Board hereby adopts the Reliability Standards reaffirmed by the Periodic Review, as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities.

Unit Auxiliary Transformer – Response to the Board

Mr. Lauby stated that during the discussion and approval of the Reliability Standard relating to generator relay loadability at its August 2013 meeting, the Board asked the Standard Drafting Team to further examine a minority issue. This minority issue related to unit auxiliary transformers, and the relays connected to those transformers.

Mr. Lauby reported that the Standard Drafting Team had studied this issue in detail and concluded that no reliability gaps resulted from the exclusion of low voltage unit auxiliary transformer relays. Mr. Lauby stated that NERC staff would continue to monitor the issue going forward.

WECC Interpretation of TOP-007-WECC-1

RESOLVED, that the Board hereby adopts the proposed Interpretation of Requirement R1 of Reliability Standard TOP-007-WECC-1, as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities.

GridEx II

Mr. Blizard updated the Board on the results of GridEx II.

Status Report on 345kV Breaker Alert

Mr. Thomas J. Galloway, CEO of the North American Transmission Forum, and Mr. Moon updated the Board on the progress made in addressing the issues associated with the 345kV circuit breaker alert.

Reliability Assessment Priorities and Process Update

Mr. Burgess provided a brief overview to the Board of Reliability Assurance and Performance Analysis processes and major strategic priorities.

Canadian Affairs

Mr. James Burpee, President and CEO of the Canadian Electricity Association, presented an update on current Canadian reliability-related initiatives.

Standing Committee Reports

Representatives of the Standing Committees provided reports to the Board highlighting items from their written reports as contained within the agenda package.

Operating Committee

Mr. James D. Castle, chair, highlighted some of the Operating Committee's ("OC's") activities since the last Board meeting. He noted and thanked Ms. Case for her attendance at previous OC meetings, and also thanked Mr. Cauley for sharing his thoughts on improving BES reliability as the industry supply-side landscape has continued to evolve.

Planning Committee

Mr. Benjamin Crisp, chair, identified some of the Planning Committee's ("PC's") key initiatives in 2014. Among these, he described the seasonal and annual reliability assessment studies, the formation of the Essential Reliability Services Task Force, and the ongoing efforts of the PC to support the Reliability Issues Steering Committee ("RISC"). Mr. Crisp also reported that since the last Board meeting, the PC has completed an in-depth review of its strategy document, and identified several areas for improvement.

Critical Infrastructure Protection Committee
Mr. Charles F. Abell, chair, briefly summarized some of the accomplishments of the Critical Infrastructure Protection Committee ("CIPC") in 2013. These included reports on security clearance and information sharing, updating the physical security response guidelines, supplying expertise to GridEx II, and the feedback provided to NERC staff by the Compliance and Enforcement Working Group. Mr. Abell also discussed some of the priorities of the CIPC going forward.

Member Representatives Committee
Mr. John A. Anderson, vice chair, thanked Mr. Gorbet and the Board for the continued use of the MRC's policy input, and summarized several issues that had been discussed at the MRC meeting the previous day.

Personnel Certification Governance Committee
Mr. Brett Hallborg, chair, was not in attendance. Mr. Gorbet referred the meeting participants to the written report of the Personnel Certification and Governance Committee, located in the agenda package.

Standards Committee
Mr. Brian Murphy, chair, expressed his gratitude for the good working relationship between the Standards Committee ("SC") and the Board, NERC staff, industry, and the staff of the Federal Energy Regulatory Commission. He also identified coordination between RISC and the SC as a critical effort, and stated that he was looking forward to working with Robert Schaffeld.

Reliability Issues Steering Committee
Mr. Robert A. Schaffeld, chair, thanked Mr. Murphy and Mr. Rossi for the progress they have made in improving processes across the ERO. He identified some of the key focus areas of RISC in the coming year, with a particular emphasis on unified prioritization at the ERO level, and described how these focus areas will be implemented.

Compliance and Certification Committee
Mr. Terry Bilke, chair, reported on several items that were not listed in the Board package. First, he noted that the annual plan was not being presented at the current Board meeting, but would instead be presented at the next Board meeting and include several additions. Second, Mr. Bilke stated that the Compliance and Certification Committee ("CCC") provided a summary of achievements and issues that still need to be addressed to the Board of Trustees Compliance Committee ("BOTCC"). He reiterated that the CCC stands ready to assist NERC in any activities in the coming year.

Electricity Sub-Sector Coordination Council
Mr. Cauley, executive committee member, reported on the progress of the restructured Electricity Sub-Sector Coordination Council ("ESCC"), and some of its key focus areas. He reported that many industry CEOs regularly attend the meetings, and that Thomas A. Fanning, Chairman and CEO of Southern Company, is now chair of the ESCC.

Forum and Group Reports

North American Energy Standards Board
Mr. Michael Desselle, chair, updated the Board on three matters: (i) beginning the process of coordinating timelines and filings necessary to adopt the recently approved MOD (A) Reliability Standards as the business practices of the North American Energy Standards Board to prevent gaps in coverage; (ii) the development of a Parallel Flow Visualization Project to support the NERC Reliability Standards, and associated coordination with the Interchange Distribution Calculator Association; and (iii) the progress of the transition regarding the NERC Transmission System Information Network Registry tool.

Regional Entity Management Group
Ms. Stacey Dochoda, chair, summarized some of the key focus areas of the Regional Entity Management Group for 2014. These include: (i) improving operations; (ii) increasing board level interactions among Regional Entities; (iii) delivering on RAI; (iv) assessing opportunities for joint employee development; and (v) preparing for review of the Regional Delegation Agreements and completing the five-year assessment.

North American Transmission Forum
Mr. Galloway, president and CEO, summarized some of the key collaborative efforts between NERC and the North American Transmission Forum ("NATF"), including protection system misoperations and the 345kV breaker issue. He also described some of the collaborative efforts with the Electric Power Research Institute and the Institute of Nuclear Power Operation, including (i) a GMD workshop in February, (ii) human and equipment performance improvement, and (iii) improvements to offsite power reliability at nuclear power plants. Mr. Galloway also described some of NATF's security initiatives, and the ongoing effort to incorporate lessons learned from the recent cold snap.

North American Generator Forum
Mr. Allen D. Schriver, chair, stated that in addition to the NAGF's written report, the Forum wanted to thank Mr. Moon and Mr. Galloway for providing many opportunities to collaborate with both NERC and the NATF.

Board Committee Reports

Corporate Governance and Human Resources Committee
Ms. Schori, chair, summarized the open meeting of the CGHRC that was held the previous day, including the following four specific action items: (i) recommendation of approval for the new Enterprise-wide Risk Committee; (ii) recommendation of approval for the Board committee assignments for 2014; (iii) recommendation of approval for the NERC Governance Guidelines; and (iv) recommendation of approval for an 8% contribution to the employee savings and investment plan for 2013. Upon motion duly made and seconded, the Board approved the following resolutions:

RESOLVED, that the Board, upon recommendation of the Corporate Governance and Human Resources Committee, hereby approves the proposed Mandate of the Enterprise-wide Risk Committee, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board, upon recommendation of the Corporate Governance and Human Resources Committee, hereby approves the 2014 Board Committee Assignments, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board, upon recommendation of the Corporate Governance and Human Resources Committee, hereby approves the NERC Governance Guidelines, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board, upon recommendation of the Corporate Governance and Human Resources Committee, hereby approves a contribution into NERC's Savings and Investment Plan for the year ended December 31, 2013 for the account of each eligible employee participant in the Plan equal to 8% of such employee participant's 2013 base salary, as presented to the Board at this meeting.

Board of Trustees Compliance Committee

Mr. Scherr reported that the BOTCC met in executive session on February 4, 2014, and in subsequent open session on February 5, 2014. He reported on some of the issues covered during those meetings, including (i) accomplishments and milestones moving forward for RAI, (ii) enforcement activities associated with RAI, and (iii) highlights of efficiency gains of the ERO in 2013 associated with the processing of noncompliance.

Finance and Audit Committee

Mr. Thilly, chair, reported that on January 30, 2014, the Finance and Audit Committee met and reviewed the Fourth Quarter Unaudited Statements of Activities of NERC and the Regions, and provided input on the proposed process improvements for the 2015 business plan and budgets. Mr. Thilly thanked Mr. Walker, his staff, and the Regional Entities, for their work on improving the process. Upon motion duly made and seconded, the Board approved the following resolution:

RESOLVED, that the Board, upon recommendation of the Finance and Audit Committee, hereby accepts the NERC Fourth Quarter 2013 Unaudited Statement of Activities, as presented to the Board at this meeting.

Standards Oversight and Technology Committee

Mr. Gorbet introduced Mr. Barber, who gave the report of the SOTC on behalf of Mr. Peterson. Mr. Barber reported that the SOTC had examined the committee self-assessment and discussed ways to improve IT oversight. He stated that the SOTC acknowledged policy input from the SC regarding the Strategic Plan and referenced the process that will be used to reconcile differences. Mr. Barber also stated that the members of the SOTC were pleased with the work performed by the SC regarding COM-002-4. He commended the work done thus far on process reforms and Reliability Standard Audit

Worksheets ("RSAWs"), and expressed his hope that improvements in the RSAW process will help to reduce the fear of compliance risk.

Closing Remarks of Chair Gorbet

Mr. Gorbet expressed his appreciation on behalf of the Board to all of those individuals who had made the Board meeting successful. He noted that Mr. Cauley's President's Report referenced how far the ERO enterprise has come in its development and maturity, and stated that while challenges remain, he remains very confident that they will be met.

Adjournment

There being no further business, and upon motion duly made and seconded, the meeting was adjourned at 11:59 p.m. Mountain.

Submitted by,

Charles A. Berardesco
Corporate Secretary

Agenda Item 2.a
Board of Trustees Meeting
May 7, 2014

Compliance and Certification Committee Membership

Action

Approve the Compliance and Certification Committee (CCC) Membership as proposed.

Background

The CCC is recommending that the Board of Trustees: 1) appoint one new CCC representative; 2) reappoint two current CCC representatives; and 3) appoint the CCC chair and vice chair, as follows:

New Member Appointments:

- Mr. Rick Terrill of Luminant Mining.
- Ms. Caroline Dupuis of Hydro-Québec TransÉnergie.

Member Reappointments:

- Mr. William Temple of Northeast Utilities.
- Ms. Jennifer Flandermeyer of Kansas City Power & Light.

Officer Appointments:

- Ms. Patti Metro as the CCC chair for the period of July 1, 2014 – Jun 30, 2016.
- Ms. Jennifer Flandermeyer as the CCC vice chair for the period of July 1, 2014 – Jun 30, 2016.

Agenda Item 2.b
Board of Trustees Meeting
May 7, 2014

Compliance and Certification Committee

Action

The Compliance and Certification Committee (CCC) requests that the Board of Trustees (Board) approve the formation of the Compliance Processes and Procedures Subcommittee (CPPS) and the retirement of the CCC's Standards Interface Subcommittee (SIS) and Procedures Subcommittee (PROCS).

Background

As the ERO has evolved, some of the tasks performed by two of the CCC's subcommittees are either no longer performed or only performed infrequently. In order to streamline support obligations and better align the CCC with NERC's strategic direction, the CCC has approved the scope of a new subcommittee called the CPPS (attached). The subcommittee's scope retains the relevant items from the CCC's SIS and PROCS, and positions the subcommittee to support NERC's compliance monitoring and enforcement improvements.

The CCC requests the Board approve the formation of the CPPS and the retirement of the SIS and PROCS.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Scope Document

Compliance and Certification Committee Compliance Processes and Procedures Subcommittee (CPPS)

March 2014

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface 1

Section 1. Mission 2

Section 2. Compliance Processes and Procedures Subcommittee Tasks and Functions 3

Section 3. Membership 4

3.1. Goals 4

3.2. General 4

3.3. Subgroup Membership and Representation 4

3.4. Membership Not Restricted to CCC Members 4

3.5. Resignations 4

3.6. Proxies 4

3.7. Exclusions 5

3.8. Changes in Member Affiliation 5

3.9. Acknowledgement of a Membership Conflict 5

Section 4. Meetings 6

4.1. Antitrust Guidelines 6

4.2. Open Meetings 6

4.3. Confidential Sessions 6

4.4. Types of Meetings 6

4.5. Majority and Minority Views 6

4.6. Actions without a Meeting 6

4.7 Quorum 6

Section 5. Officers and Staff 7

5.1. General 7

5.2. Chair 7

5.3. Vice Chair 7

5.4. Staff Coordinator 7

6. Subordinate Groups 9

6.1. Committee Organization Hierarchy 9

6.2. Establishing Subgroups 9

Appendix A – CCCPP Responsibilities 10

Preface

NERC Compliance and Certification Committee		CCCXX-00X
Title: XXX		
Version: x.0	**Revision Date: MM/DD/201X**	**Effective Date: MM/DD/201X**

Summary

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the Bulk Power System (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The Compliance and Certification Committee (CCC) is a NERC board-appointed stakeholder committee serving and reporting directly to the NERC Board of Trustees (Board) and is responsible for engaging with, supporting, and advising the NERC Board and NERC regarding all facets of the NERC Compliance Monitoring and Enforcement Program (CMEP), Organization Registration Program (Registration program), and Organization Certification Program (Certification program). The CCC is responsible for establishing and implementing a program as specified in Section 405 of the NERC Rules of Procedure (ROP) to monitor NERC's adherence to ROP for Compliance Enforcement, including but not limited to the uniform Compliance Monitoring and Enforcement Program (Appendix 4C) and the Sanction Guidelines (Appendix 4B).

Revision History

Date	Version Number	Comments
March 12, 2014	1.0	Approved by the Compliance and Certification Committee in order to consolidate PROCS and SIS.
Month DD, YYYY	1.0	Approved by the Board of Trustees

Section 1. Mission

The NERC Compliance and Certification Committee (CCC) is a NERC Board-appointed stakeholder committee serving and reporting directly to the NERC Board. Operation and governance of the CCC is as articulated in the CCC Charter.

The **Compliance Processes and Procedures Subcommittee (CPPS)** is formed by the CCC to assist the committee in fulfilling its mission and functions[1] in a thorough and efficient manner. Further details of what the subcommittee will undertake, on behalf, and under the supervision, of the CCC are provided in Section 2.

[1] See Sections 1 and 2 of the CCC Charter, respectively.

Section 2. Compliance Processes and Procedures Subcommittee Tasks and Functions

To fulfill its mission, the CCC has established the **CPPS** to perform the following tasks on behalf, and under the supervision, of the CCC:

i. Perform document review to promote consistency between multiple documents (procedures, policies, standards, rules, orders, etc.) that comprise the overall NERC Compliance Monitoring and Enforcement Program (CMEP) and to assure documents are clear, unambiguous, consistent and complementary, to advise the CCC of any such situations, and propose changes that it believes will clarify such situations. Activities may include, but are not limited to:

   a. Reviews of changes to the Rules of Procedure related to the Compliance program, Registration program, and Certification program.

   b. Proposals to change the ROP related to the Compliance program, Registration program, and Certification program.

ii. Support the development and implementation of enhancements to the CMEP (including efforts as set forth in the CCC Work Plan) and provide this information to the CCC, applicable CCC subcommittees, and NERC.

iii. Develop and maintain CCC operational procedures with respect to the CCC responsibilities under the CCC Charter, as specified in Attachment A.

iv. Advise and prepare recommendations to the CCC to address any standards related issues relevant to and within the scope of the NERC Compliance and Certification Committee (e.g. request from the Standards Committee, Standard Drafting Team, CCC, NERC Compliance Staff, etc.).

v. Act as liaison of the CCC to the NERC Standards Committee.

vi. Implement CCC oversight, facilitate, participate as needed, in the development of the compliance administration elements (CAEs), including RSAWs, for new Reliability Standards under development or for revisions to existing Reliability Standards.

vii. Prepare and maintain guidance and other related documents and materials for the benefit of Standards Drafting Teams regarding the development of CAEs.

The subcommittee will work within its assigned scope and be accountable for the responsibilities assigned to it by the CCC.

Section 3. Membership

3.1. Goals

The membership of this subcommittee will be established to address the need for expertise and balance of interests to carry out the subcommittee's assigned Tasks and Functions as in Section 2.

3.2. General

General membership requirements for members of a sub-group of the CCC are as articulated in Section 7 of the CCC Charter. Additional membership requirements for this committee are as defined within this scope document.

3.3. Subgroup Membership and Representation

As outlined in the CCC Charter, each member of this subcommittee, and its officers, will be appointed by the chair of the CCC.

3.4. Membership Not Restricted to CCC Members

Members of this subcommittee are not required to be members of the CCC, but must be eligible to be members of the committee.

3.5. Resignations

a. By the Member

In the event a member can no longer serve on the subcommittee, that member will submit a written resignation to the subcommittee chair or the CCC secretary.

b. Requested by the Chair

The chair may request any subcommittee member who ceases to participate in the subcommittee, as indicated by not attending or sending a proxy for two consecutive meetings, to submit a resignation or to request continuation of membership with an explanation of extenuating circumstances. If a written response is not received within 30 days of the chair's request, the lack of response will be considered a resignation.

c. Referral to the CCC Chair

The subcommittee chair will refer the vacancy resulting from a resignation to the chair of the CCC who may recommend a replacement pursuant to the CCC Charter.

d. By the Board

CCC Committee members and, by extension, members of CCC subcommittees serve at the pleasure of the NERC Board which may request resignation, remove or replace a member as it deems appropriate.

3.6. Proxies

A substitute representative, or proxy, may attend on behalf of a member during all or a portion of a subcommittee meeting, provided the absent member notifies the subcommittee chair, vice chair, or CCC secretary of the proxy.

a. Notification

Such notification will be in writing (electronic medium is acceptable). The proxy representatives and their affiliation will be named in the correspondence.

b. May Not Serve as a Proxy for Another Member

A voting member of a subcommittee may not serve as a proxy for another voting member on the same subcommittee (i.e. a member may not cast more than his or her own vote).

3.7. Exclusions

Exclusions shall be as articulated in Section 3 of the CCC Charter.

3.8. Changes in Member Affiliation

A subcommittee member whose affiliation has changed may remain a member of the subcommittee by remaining subject to membership requirements and by notifying the chair of the CCC and the subcommittee chair of the change and receiving the approval of the chair of the CCC to remain on the subcommittee.

3.9. Acknowledgement of a Membership Conflict

No subcommittee member may have a conflict of interest that would impair his or her ability to fulfill obligations under this scope document. Any subcommittee member who knows of any form of membership conflict, such as working for an entity affiliated with that of another subcommittee member, will notify the subcommittee chair and the chair of the CCC within ten business days of obtaining that knowledge.

Section 4. Meetings

In the absence of specific provisions in this document or the CCC Charter, all subcommittee meetings will follow Robert's Rules of Order, Newly Revised.

Actions requiring a vote by the members of the subcommittee will be approved upon receipt of the affirmative vote of the majority of the voting members of the subcommittee present and voting, in person or by proxy at any meeting at which five (5) or more members are present.

4.1. Antitrust Guidelines

All persons attending or otherwise participating in a NERC committee or subgroup meeting will act in accordance with NERC's Antitrust Compliance Guidelines at all times during the meeting.

4.2. Open Meetings

NERC committee meetings will be open to the public, except as noted below under Confidential Sessions.

4.3. Confidential Sessions

With approval of the NERC Director of Compliance Operations, a meeting or portion of a meeting of the sub-committee may have attendance limited based on confidentiality of the information to be disclosed at the meeting. Such limitations should be applied sparingly and on a non-discriminatory basis as needed to protect information that is sensitive information or confidential information to one or more parties. Confidential information will only be disclosed as provided by Section 1500 of the NERC Rules of Procedure. Confidentiality agreements may also be applied, as necessary, to protect sensitive information or confidential information.

4.4. Types of Meetings

Meetings may be conducted in person, by conference call, or other means. The procedures contained in this scope document will apply to all meetings regardless of how they are conducted.

4.5. Majority and Minority Views

All members of the subcommittee will be afforded the opportunity to provide alternative views on an issue. The results of the subcommittee actions, including recorded minutes, will reflect the majority as well as any minority views of the subcommittee members. The chair will communicate both the majority and any minority views in presenting results to the CCC.

4.6. Actions without a Meeting

Actions without a meeting are permitted in accordance with the provisions of the CCC Charter.

4.7 Quorum

A quorum for conducting business is 50 percent of the members listed on the current subcommittee roster. If a quorum is not present, then the subcommittee may not take any actions requiring a vote of the subcommittee. However, the chair may, with the consent of the members present, allow discussion of agenda items.

Section 5. Officers and Staff

5.1. General

a. Number of Positions
The subcommittee will have two officers and a secretary.

b. Officers
The subcommittee officers will be one chair and one vice chair.

c. Secretary
The NERC staff coordinator will serve as the subcommittee's secretary.

d. Officers May Vote
The subcommittee chair and vice chair are voting members of the subcommittee.

e. Officers are Named by the CCC Chair for a Two-year Term
Officers may be reappointed for a second two-year term.

5.2. Chair
The chair will direct and provide general supervision of subcommittee activities, including:

i. Coordinate the schedule of all subcommittee meetings.

ii. Develop subcommittee agendas and rule on any deviation, addition, or deletion from a published agenda.

iii. Preside at, and manage, subcommittee meetings including the nature and length of discussion, recognition of speakers and proxies, motions, and voting.

iv. Will act as the spokesperson for the subcommittee to the CCC.

The subcommittee chair will serve as a member of the Executive of the CCC as described in the CCC Charter. The subcommittee chair must be a member of the CCC.

5.3. Vice Chair
The vice chair will assume the responsibilities of the chair under the following conditions:

i. At the discretion of the chair (for brief periods of time);

ii. When the chair is absent or temporarily unable to perform the chair's duties; or

iii. When the chair is permanently unavailable or unable to perform the chair's duties. In the case of a permanent change, the vice chair will continue to serve until a new chair is appointed by the chair of the CCC.

The vice chair is unable to assume the responsibilities of the chair on the CCC Executive unless the vice chair is also a member of the CCC.

5.4. Staff Coordinator
A member of the NERC staff will be selected by NERC's Director of Compliance Operations to serve as the staff coordinator and secretary of the subcommittee. The staff coordinator is not a subcommittee member and does not have a vote. Under the direction of the subcommittee officers, the chair of the CCC and applicable NERC Bylaws, guidelines and Rules of Procedure, the staff coordinator will:

i. Manage the day-to-day operation and business of the subcommittee.

ii. Prepare and distribute the notices of the subcommittee meetings, prepare the meeting agenda, and prepare and distribute minutes of the subcommittee meetings.

iii. Act as the subcommittee's parliamentarian.

6. Subordinate Groups

6.1. Committee Organization Hierarchy

As allowed in the NERC Bylaws the CCC organizational structure supports a superior-subordinate hierarchy that is ordered as follows:

- Committee
- Subcommittee
- Working Group
- Task Force

6.2. Establishing Subgroups

The CCC has established this subcommittee and is responsible for it to the NERC Board. This subcommittee may establish subordinate groups as discussed in the CCC Charter.

Appendix A – CCCPP Responsibilities

It is envisioned that the other CCC Subcommittees will be primarily responsible for maintaining the CCCPPs that they administer, and CPPS is available as support.[2]

CCCPP	Responsible Subcommittee
• CCC Monitoring Program — CCCPP–001 | Monitoring Program for NERC's Adherence to NERC's Rules of Procedure for Compliance Enforcement	**EROMS**
• CCC Monitoring Program — CCCPP–002–1 | Compliance Monitoring Program for Reliability Standards Applicable to NERC	**EROMS**
• CCC Monitoring Program — CCCPP–003–1 | Monitoring Program for NERC's Reliability Standards Development Procedure	**EROMS**
• CCC Monitoring Program — CCCPP–004–1 | NERC Compliance and Certification Committee Hearing Procedures	**CPPS**
• CCC Monitoring Program — CCCPP–005–1 | NERC Compliance and Certification Committee Hearing Procedures for use in Appeals of Certification Matters	**ORCS**
• CCC Monitoring Program — CCCPP–006–1 | NERC Compliance and Certification Committee Mediation Procedures	**CPPS**
• CCC Monitoring Program — CCCPP–007 | Monitoring Program for NERC's Adherence to NERC's Rules of Procedure for Registration and Certification	**ORCS**
• CCC Monitoring Program — CCCPP–008–1 | Program for Monitoring Stakeholder's Perceptions	**EROMS**
• CCC Monitoring Program — CCCPP–009–1.1 | Confidentiality Protocol - Compliance and Certification Committee	**PROCS, *now* CPPS**
• CCC Monitoring Program - CCCPP-010-1 | NERC Compliance and Certification Committee Criteria for Annual Regional Entity Program Evaluation	**PROCS, *now* CPPS**
• Compliance and Certification Committee Charter	**CPPS**

[2] http://www.nerc.com/comm/CCC/Pages/Related%20Files.aspx

Agenda Item 2.c
Board of Trustees Meeting
May 7, 2014

Critical Infrastructure Protection Committee Membership

Action

The Board of Trustees is asked to approve the following subject matter expert to serve on the CIPC Executive Committee.

- Operations Security: Mr. David Revill, Georgia Transmission

Agenda Item 2.d
Board of Trustees Meeting
May 7, 2014

Personnel Certification Governance Committee Membership

Action

The Board of Trustees is asked to appoint one new member to the Personnel Certification Governance Committee.

- Michael Hoke, Senior Lead Trainer, PJM Interconnection

Demand and Energy Data — MOD-031-1

Action

Adopt the following standards documents and direct staff to file with applicable regulatory authorities:

- **Reliability Standard – MOD-031-1 Demand and Energy Data**

  [MOD-031-1-clean]

- **Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for MOD-031-1**

  [VRFs and VSLs]

- **Implementation Plan for MOD-031-1 Demand and Energy Data**

  [Implementation Plan]

  - This standard shall become effective the first day of the first calendar quarter that is twelve months after the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is twelve months after the date the standard is adopted by the NERC Board of Trustees (Board) or as otherwise provided for in that jurisdiction.

- **Definitions**
  The MOD C Standard Drafting Team (SDT) proposes the following new definition and one revised definition (Demand-Side Management):

  - **Total Internal Demand:** The Demand of a metered system which includes, the Firm Demand, plus any controllable and dispatchable DSM Load and the Load due to the energy losses incurred within the boundary of the metered system.
  - **Demand-Side Management (DSM):** All activities or programs undertaken by any applicable entity to achieve a reduction in Demand.

- **Retirements**
  Retire the following standards midnight of the day immediately prior to the effective date of MOD-031-1:

  - MOD-016-1.1 – Documentation of Data Reporting Requirements for Actual and Forecast Demands, Net Energy for Load, Controllable Demand-Side Management
  - MOD-017-0.1 – Aggregated Actual and Forecast Demands and Net Energy for Load
  - MOD-018-0 – Treatment of Nonmember Demand Data and How Uncertainties are Addressed in the Forecasts of Demand and Net Energy for Load

- MOD-019-0.1 – Reporting of Interruptible Demands and Direct Control Load Management
- MOD-021-1 – Documentation of the Accounting Methodology for the Effects of Demand-Side Management in Demand and Energy Forecasts

The existing definition for Demand-Side Management should be retired midnight of the day immediately prior to the effective date of MOD-031-1.

Background

A fundamental test for determining the reliability of the Bulk Power System is an assessment of whether there is an adequate amount of resources available to serve peak Demand while also maintaining a sufficient margin to address operating events. The purpose of this reliability standard is to provide authority for applicable entities to collect Demand, energy and related data to support reliability studies and assessments. The reliability standard enumerates the responsibilities and obligations of requestors and respondents of the data. The proposed reliability standard consolidates MOD-016 through MOD-019 and MOD-021 into a single standard that comprehensively address Demand and energy data collection requirements.

The SDT considered the Paragraph 81 criteria when it evaluated the draft standard. The SDT concluded that since this data supports reliability, it did not qualify for retirement under the Paragraph 81 criteria. The collection of Demand projections requires coordination and collaboration between Planning Authorities/Planning Coordinators (PCs), Transmission and Resource Planners (TPs and RPs), and Load-Serving Entities (LSEs). Ensuring that planners and operators have access to complete and accurate load forecasts—as well as the supporting methods and assumptions used to develop these forecasts—will ultimately enhance the reliability of the Bulk Electric System. Consistent documenting and information-sharing activities will also improve the efficiency of planning practices and support the identification of needed system reinforcements. Furthermore, collection of actual Demand and Demand-Side Management performance data during the prior year enables comparison to prior forecasts and further contributes to enhanced accuracy of load forecasting practices. Finally, the data to be collected under the standard is necessary for the ERO to conduct its reliability assessments, such as the Long Term Reliability Assessment.

The SDT concluded that a standard was necessary to meet thse reliability needs and help ensure that data will be collected and shared among the necessary parties (LSEs, PCs, TPs, RPs, Balancing Authorities (BAs), Distribution Providers (DPs), Transmission Service Providers (TSPs), etc.) in the United States and Canada to support reliability assessments.

Pertinent FERC Order No. 693 directives

Project 2010-04, MOD C, addressed 14 FERC directives from FERC Order No. 693 Mandatory Reliability Standards for the Bulk Power System. These FERC directives are in paragraphs 1232, 1249, 1250, 1251, 1252, 1255, 1256, 1265, 1276, 1277, 1287, and 1298.

Standard Development Process

Three drafts of MOD-031-1 were posted for industry comment during the development period. Draft 3 of the standard was posted for an additional comment period from February 25 through April 10, 2014, with a ballot that was conducted from April 1 through April 10, 2014. The results of the additional ballot and subsequent final ballot were not available when these materials were prepared and will be reported during the May 7, 2014 Board meeting.

Unresolved Minority Issues

There were three minority issues raised by industry stakeholders, as identified below. These issues were resolved by the majority of stakeholders.

Issue: Several stakeholders stated that the existing MOD C standards (MOD-016-1.1, MOD-017-0.1, MOD-018-0, MOD-019-0.1 and MOD-021-1) should be retired. These stakeholders argued that the data could be collected by NERC and the Regional Entities through data requests issued pursuant to Section 800 or Section 1600 of NERC's Rules of Procedure.

Response: The SDT concluded that a standard was necessary for two reasons:

- First, the standard provides a mechanism for (1) PCs and BAs to obtain Demand and energy data from data owners for their own reliability purposes that is not necessarily connected to the ERO's reliability assessments; and (2) the sharing of Demand and energy data between neighboring LSEs, DPs, PCs, BAs, RPs and TPs to provide additional clarity in their system analysis. Replacing standard MOD-016 through MOD-019 and MOD-021 with a data request geared to provision of data to NERC would not provide a mechanism for this data sharing or enable PCs and BAs to obtain Demand and energy data from data owners for their own reliability purposes. The SDT concluded that because there is a reliability need for PCs and BAs to obtain demand data for their own reliability purposes and for data sharing between Registered Entities, a standard was necessary.
- Second, the standard provides an efficient and enforceable mechanism for NERC and the Regional Entities to obtain Demand and energy data from all applicable registered entities across the entire continent. Because certain Canadian provinces have adopted only select portions of the NERC Rules of Procedure, a standard is necessary to ensure that the authority to collect the necessary data from all applicable Registered Entities is in place. The data to be collected under the standard is necessary for the ERO to conduct its reliability assessments, such as the Long Term Reliability Assessment.

Issue: A few stakeholders stated that they were unsure of the value of collecting weather normalized data.

Response: The SDT is responding to a FERC directive to collect weather nomlaized data. However, the SDT modified the requirement to identify only those entities whose Demand varies due to weather-related conditions would need to provide this data.

Issue: Some stakeholders disagreed with allowing an entity, other than the PC or BA, to have the opportunity to request data from its neighbors.

Response: The SDT disagrees with the stakeholders as there are instances when a neighboring entity has a reliability related need for the data. Additionally, this opportunity exists in the present FERC approved standards.

Additional Information

A link to the project history and files is included here for reference:

[**Project 2010-04 Demand Data (MOD C)**]

Voltage and Reactive Control – VAR-002-3

Action

Adopt the following standard documents and authorize staff to file with applicable regulatory authorities:

- **Reliability Standard – VAR-002-3— Generator Operation for Maintaining Voltage Schedules**

  [VAR-002-3- Clean] [VAR-002-3 - Redline to last approved]

- **Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for VAR-002-3— Voltage and Reactive Control**

  [VRFs and VSLs]

- **Implementation Plan for – VAR-002-3 — Generator Operation for Maintaining Voltage Schedules**

  [VAR-002-3 Implementation Plan]

  - The standard shall become effective on the first day of the first calendar quarter after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, VAR-002-3 shall become effective on the first day of the first calendar quarter after the date the standard is adopted by the NERC Board of Trustees (Board) or as otherwise provided for in that jurisdiction.

- **Retirements**

  Retire the following standard midnight of the day immediately prior to the effective date of VAR-002-3:

  - VAR-002-2b, Voltage and Reactive Control

Background

VAR-002-3 is a companion standard to VAR-001-4, which was adopted by the Board at its February 2014 meeting. VAR-002-3 addresses requirements for Generator Owners and Generator Operators (GOPs), and VAR-001-4 addresses requirements for Transmission Operators (TOPs).

VAR-002-3 help ensure that generators provide reactive support and voltage control, within generating Facility capabilities, in order to protect equipment and maintain reliable operation of the Interconnection. The new standard eliminated unnecessary notifications found in VAR-002-2b that may hinder reliability, and the standard requires GOPs to communicate according to the protocols established by TOPs.

Pertinent FERC Order No. 693 and 724 directives

The FERC directives pertaining to the VAR standards were addressed in the VAR-001 standard.

Standard Development Process

This standard development project began as an informal development project in February 2013. The informal development transitioned to formal development in July 2013 with the posting of the Standards Authorization Request, along with a draft of the proposed VAR standards for comment and ballot, and the formation of a Standard Drafting Team. Drafts of the standard were posted for three comment and ballot periods, ending in August 2013, November 2013, and April 2014. The results of the last additional ballot and subsequent final ballot were not available when these materials were prepared and will be reported during the May 7, 2014 Board meeting.

Unresolved Minority Issues

There are no unresolved minority issues.

Additional Information

A link to the project history and files is included here for reference:

[**Project 2013-04 Voltage & Reactive Control**]

Operating Personnel Communication Protocols—COM-002-4

Actions

1. Adopt the following standard documents and authorize staff to file with applicable regulatory authorities:

   - **Reliability Standard – COM-002-4—Operating Personnel Communication Protocols**

     [COM-002-4 - Clean] [COM-002-3 - Board adopted]

   - **Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for COM-002-4—Operating Personnel Communication Protocols**

     [VRFs and VSLs]

   - **Implementation Plan for COM-002-4—Operating Personnel Communication Protocols**

     [Implementation Plan]

   - **Definitions**
     Operating Instruction — A command by operating personnel responsible for the Real-time operation of the interconnected Bulk Electric System to change or preserve the state, status, output, or input of an Element of the Bulk Electric System or Facility of the Bulk Electric System. (A discussion of general information and of potential options or alternatives to resolve Bulk Electric System operating concerns is not a command and is not considered an Operating Instruction.).

   - **Retirements**
     COM-001-1.1 Requirement R4, COM-002-2, and COM-002-3, as applicable, shall be retired at midnight of the day immediately prior to the effective date of COM-002-4 in the particular jurisdiction in which the new standard is becoming effective.

   - **Reliability Standard Audit Worksheet**

     [RSAW]

2. Rescind the Board of Trustees' (Board's) February 9, 2012 approval, available here, of the Interpretation of COM-002-2, effective (i) for U.S. registered entities upon implementation of COM-002-4 in substantially the form approved by the Board and (ii) for Canadian entities, effective upon implementation of COM-002-4 in substantially the form approved by the Board, as such implementation is approved by the applicable governmental authority for each such entity, it being the intent of the Board that an entity's compliance with existing COM-002-2 continue to reflect the Board's Interpretation of COM-002-2 until such time as COM-002-4 is implemented by each applicable governmental authority.

Background – Action 1

The proposed standard is designed to ensure that reliability-related information is conveyed effectively, accurately, consistently, and in a timely manner towards mutual understanding by all key parties when issuing or receiving Emergency and non-Emergency Operating Instructions.

On November 7, 2013, the Board approved a resolution on Operating Personnel Communications Protocols (OPCP), which is available here. In response to this resolution, the standard drafting team (SDT) developed a new draft of COM-002-4. The COM-002-4 standard

combines COM-002-3 and the draft COM-003-1 standard into a single standard regarding communication protocols. COM-002-4 requires entities to develop specific documented communication protocols for the issuance and receipt of Operating Instructions by operating personnel during Emergency, alert, and non-Emergency situations. Among these protocols are: (1) use of the English language (unless an alternate language is agreed to otherwise); (2) protocols for three-part communications; and (3) protocols for single-party to multiple-party burst Operating Instructions. COM-002-4 also requires entities to conduct initial training for operating personnel on the communications protocols and to provide feedback to those operating personnel on adherence to the communications protocols. Entities are further required to periodically evaluate their set of communications protocols for effectiveness and add protocols, as necessary. Finally, entities are required to always use three-part communication when issuing and receiving oral Operating Instructions during Emergencies.

Background – Action 2

On October 1, 2009, a clarification was requested by the ISO-RTO Council of Requirement R2 of COM-002-2, specifically asking whether "directives" are limited to actions requested during actual and anticipated emergency operating conditions, or whether routine operating instructions are also considered "directives." The interpretation of Reliability Standard COM-002-2 was adopted by the Board on February 9, 2012. Because COM-002-4 no longer uses the undefined term "directive," the ambiguity in COM-002-2 that resulted in the interpretation request has been resolved by the revisions in COM-002-4.

Pertinent FERC Order No. 693 directives

Paragraph 512

> *The Commission finds that, during both normal and emergency operations, it is essential that the transmission operator, balancing authority and reliability coordinator have communications with distribution providers…we adopt our proposal to require the ERO to modify COM-002-2 to apply to distribution providers through its Reliability Standards development process.*

Paragraph 531

> *We adopt our proposal to require the ERO to establish tightened communication protocols, especially for communications during alerts and emergencies, either as part of COM-002-2 or as a new Reliability Standard. We note that the ERO's response to the Staff Preliminary Assessment supports the need to develop additional Reliability Standards addressing consistent communications protocols among personnel responsible for the reliability of the Bulk-Power System.*

Paragraph 532

While we agree with EEI that EOP-001-0, Requirement R4.1 requires communications protocols to be used during emergencies, we believe, and the ERO agrees, that the communications protocols need to be tightened to ensure Reliable Operation of the Bulk-Power System. We also believe an integral component in tightening the protocols is to establish communication uniformity as much as practical on a continent-wide basis. This will eliminate possible ambiguities in communications during normal, alert and emergency conditions. This is important because the Bulk-Power System is so tightly interconnected that system impacts often cross several operating entities' areas.

Paragraph 535

Accordingly, we direct the ERO to either modify COM-002-2 or develop a new Reliability Standard that requires tightened communications protocols, especially for communications during alerts and emergencies.

Paragraph 540

While the Commission identified concerns regarding COM-002-2, the proposed reliability standard serves an important purpose by requiring users, owners and operators to implement the necessary communications and coordination among entities. Accordingly, the Commission approves Reliability Standard COM-002-2 as mandatory and enforceable. In addition, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, the Commission directs the ERO to develop a modification to COM-002-2 through the Reliability Standards development process that: (1) expands the applicability to include distribution providers as applicable entities; (2) includes a new Requirement for the reliability coordinator to assess and approve actions that have impacts beyond the area view of a transmission operator or balancing authority and (3) requires tightened communications protocols, especially for communications during alerts and emergencies. Alternatively, with respect to this final issue, the ERO may develop a new Reliability Standard that responds to Blackout Report Recommendation No. 26 in the manner described above. Finally, we direct the ERO to include APPA's suggestions to complete the Measures and Levels of Non-Compliance in its modification of COM-002-2 through the Reliability Standards development process.

Standard Development Process

The second draft of COM-002-4 (eighth draft overall) was posted on December 30, 2013, for a 30-day comment period and concurrent 10 day ballot period ending January 29, 2014. The standard achieved a quorum and received sufficient affirmative votes for approval. The standard was subsequently posted for a final ballot. The final ballot was conducted from March 28 through April 7, 2014, during which the proposed standard received a final approval of 77.62 percent.

Minority Issues

Issue: Several commenters indicated that Distribution Providers (DPs) should not be included as an applicable entity to COM-002-4 or that, if included, the applicability be limited to DPs who "shed 300 MW or more of load in a single manually initiated

operation or have switching obligations related to Any Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource…."

Response: The OPCP SDT chose to include DPs in the Applicability section because they can be and are on the receiving end of some Operating Instructions. The SDT could not determine a technical basis to support a threshold to exclude certain DPs. The addition of DPs is also responsive to the FERC directive.

Issue: Other commenters noted that the requirements do not differentiate clearly between the actions operators must take during non-Emergency and Emergency situations.

Response: In COM-002-4, the same protocols are to be used for Operating Instructions in all operating conditions, i.e., non-emergency, alert, and Emergency communications. The OPCP SDT believes that one set of communication protocols should be used at all times by operators in order to improve consistency and minimize confusion. The standard uses the phrase "Operating Instruction during an Emergency" in certain Requirements (R5, R6, R7) to provide a demarcation for what is subject to a zero-tolerance compliance approach.

Issue: It was suggested by several individuals and entities that the inclusion of a training requirement was not necessary and or would be better suited for inclusion in PER-005.

Response: The OPCP SDT consulted with the SDT responsible for the development of PER-005 on this concern. The OPCP SDT was advised that while training on communications protocols would fall into an entity's systematic approach to training, the requirements in PER-005 do not mandate training on communications protocols. The OPCP SDT asserts it is essential for all operators to have a common level of understanding and be trained in three-part communication. Therefore, inclusion of a requirement in COM-002-4 to conduct initial training is appropriate.

Issue: Some commenters noted that they felt the "assess adherence and assess effectiveness" contained within Requirement R4, the associated Measure, and VRFs/VSLs was similar to the "identify assess and correct" (IAC) language contained in certain CIP Version 5 requirements, which FERC directed NERC to remove or clarify.

Response: In Order No. 791 approving the CIP Version 5 Reliability Standards, FERC expressed concerns with ambiguities around the meaning of the "identify, assess, and correct" language in certain Requirements. For example, FERC questioned what a reasonable timeframe would be for identifying and correcting a deficiency, whether the language could be used to avoid audit risk, and how the implementation and performance of the language can be expected to be consistent across responsible entities and regions. The obligations required by COM-002-4 do not have the same issues inherent in the "identify, assess, and correct" language. The obligations in

COM-002-4 are clearly defined in the language of Requirement R4 and Measure M4: at least every twelve (12) months, entities must evaluate and document performance of operating personnel based on its documented communications protocols, take corrective action to the assessment as necessary, and periodically assess and document the effectiveness of the documented communications protocols. With respect to implementation of COM-002-4, the standard explicitly creates a system of periodic, backward-looking reviews of systems based on predefined standards that are to be reviewed for efficacy on a regular basis. The program anticipated by Requirement R4 is substantially similar to assessments required in other Reliability Standards (e.g., FAC-003, PRC-005, PRC-006, and PRC-004, and the language of the Requirement and accompanying Measure provide adequate detail regarding the obligations of the entity in performing the assessment.

Additional Information

A link to the project history and files for COM-002-4 is included here for reference:

[**http://www.nerc.com/pa/Stand/Pages/Op_Comm_Protocol_Project_2007-02.aspx**]

A link to the project history and files for the Interpretation of COM-002-2 is included here for reference:
[**http://www.nerc.com/pa/Stand/Pages/Project200922RFICOM0022R2IRC.aspx**]

Violation Severity Levels and Violation Risk Factors for Various Standards

Action

Adopt modified Violation Severity Levels (VSLs) and Violation Risk Factors (VRFs) for the following standards, and authorize staff to file with applicable regulatory authorities:

- **TPL-001-4** [redline showing revised VRF for Requirement R1]
- **CIP-003-5** [redline showing revised VSLs for Requirements R1 and R2]
- **CIP-004-5.1** [redline showing revised VRF and VSLs for Requirement R4]
- **CIP-006-5** [redline showing revised VRF for Requirement R3]
- **CIP-008-5** [redline showing revised VSL for Requirement R2]
- **CIP-009-5** [redline showing revised VSLs for Requirement R3]
- **MOD-026-1** [redline showing revised VSLs for Requirement R6]
- **MOD-027-1** [redline showing revised VSLs for Requirement R5]
- **PRC-005-2** [redline showing revised VSL for Requirement R1]
- **PRC-005-3** [redline showing revised VSL for Requirement R1]
- **BAL-003-1** [redline showing revised VRF and VSLs for Requirement R1]

Background

In several recent orders approving Reliability Standards, the Federal Energy Regulatory Commission (FERC) directed changes to Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs). The NERC Rules of Procedure Section 320 requires the NERC Board of Trustees' (Board's) approval for modifications to VRFs and VSLs resulting from a directive by an applicable regulatory authority. As described below, NERC has prepared the directed revisions in consultation with the relevant drafting teams and is hereby requesting the Board's approval of those revisions.

I. **TPL-001-4, Requirement R1 VRF**. On October 17, 2013, FERC issued Order No. 786 approving TPL-001-4 and directing NERC to modify the VRF for Requirement R1 from Medium to High. Requirement R1 requires Transmission Planners (TPs) and Planning Coordinators to maintain system models within their respective areas for the purpose of conducting studies needed to perform Planning Assessments. The drafting team reviewed the directive and agreed to the change. No other changes have been made to the standard.

II. **Multiple VRFs and VSLs for Version 5 CIP Standards**. On November 22, 2013, FERC issued Order No. 791, *Version 5 Critical Infrastructure Protection Reliability Standards*. In this order, FERC approved the CIP Version 5 standards and directed NERC to modify certain of those standards. In addition, FERC directed NERC to modify certain VRFs and

VSLs for particular CIP Version 5 standards. The directives pertaining to VRFs and VSLs are included in Paragraphs 176, 181-184, 192-195, and 205-210 of FERC Order No. 791.

FERC directed NERC to submit revisions to the VRFs by May 5, 2014, which is 90 days after the February 3, 2014 effective date of the order. March 18, 2014, NERC staff filed a request for an extension of the VRFs' filing deadline in order to afford time for the Board to adopt the revisions at its May 7, 2014 meeting. FERC granted NERC's requested extension and directed NERC to file the revisions by May 15, 2014. FERC did not direct a deadline for filing the revised VSLs.

NERC conferred with the standard drafting team (SDT) for Project 2014-02 CIP Version 5 Revisions because the Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards SDT is no longer convened, and proposes the following revisions to VRFs and VSLs for the Version 5 CIP standards in response to FERC's Order No. 791 directives:

1. **VSLs for CIP-003-5, Requirements R1 and R2**. This standard addresses security management controls for cyber security. Requirement R1 governs management approval of policies on topics addressed in other CIP standards for medium and high impact BES Cyber Systems. Requirement R2 governs policies for low impact BES Cyber Systems. NERC staff, in consultation with the SDT for Project 2014-02 CIP Version 5 Revisions, revised the VSLs in CIP-003-5, Requirements R1 and R2 to eliminate redundant language to meet the FERC directive in P 206 of Order No. 791.
2. **VRF and VSLs for CIP-004-5.1, Requirement R4**. This standard includes requirements for personnel and training related to cyber security. Requirement R4 governs implementation of access management programs. In response to the FERC directive in P 192 of Order No. 791, NERC staff revised the VRF from Lower to Medium. Further, NERC staff, in consultation with the SDT for Project 2014-02 CIP Version 5 Revisions, revised the VSLs to a percentage-based gradation to meet the FERC directive in P 208 of Order No. 791.
3. **VRF for CIP-006-5, Requirement R3**. This standard addresses physical security of BES Cyber Systems. Requirement R3 governs implementation of Physical Access Control System maintenance and testing programs. In response to the FERC directive in P 184 of Order No. 791, NERC staff revised the VRF from Lower to Medium.
4. **Severe VSL for CIP-008-5, Requirement R2**. This standard addresses incident reporting and response planning for cyber security. Requirement R2 governs implementation of documented Cyber Security Incident response plans. In response to the FERC directive in P 209 of Order No. 791, NERC staff revised the Severe VSL to reduce a gap in months between the High VSL and Severe VSL.
5. **VSLs for CIP-009-5, Requirement R3**. This standard addresses recovery plans for BES Cyber Systems. Requirement R3 governs maintenance of the recovery plans. In response to the FERC directive in P 210 of Order No. 791, NERC staff revised the timeframe contained in the VSLs from 90-210 days to 90-120 days.

To respond to the directive in P 205 of Order No. 79, NERC will request Board approval of revisions to the VSLs associated with the requirements that include the "identify, assess, and correct" language when those requirements are modified consistent with FERC's directive to remove or modify that language. The SDT for Project 2014-02 CIP Version 5 Revisions is currently addressing the "identify, assess, and correct" language in the requirements of the CIP standards and will revise the VSLs accordingly.

III. **VSLs for MOD-026-1, Requirement R6 and MOD-027-1, Requirement R5**. On March 20, 2014, FERC issued Order No. 796, *Generator Verification Reliability Standards*. In this order, FERC approved five generator verification standards and directed NERC to make modifications to VSLs for two requirements, each of which require the TP to provide a written response to the Generator Owner that it has received certain model information, and, if the model is unusable, to provide a technical explanation as to why the model is unusable. The modified VSLs address a violation where the model is unusable but the TP fails to provide a technical explanation as to why the model is unusable. The Project 2007-09 Generator Verification drafting team was consulted in developing these revisions.

IV. **VSLs for PRC-005-2 and PRC-005-3, Requirement R1.** On December 19, 2013, FERC issued Order No. 793, approving Reliability Standard PRC-005-2 – Protection System Maintenance, stating that the "Reliability Standard contains overall improvements over the four existing Reliability Standards." However, FERC directed one change to the VSL assignment in Requirement R1 regarding the failure to include station batteries in a time-based maintenance program, noting that "the level of risk associated with the failure to test a given battery is not an appropriate consideration in the context of assigning violation severity levels, but rather, should be considered when assigning a violation risk factor." FERC therefore directed NERC to submit a compliance filing changing the VSL for the failure to include station batteries in a time-based maintenance program to "severe."

    In consultation with the relevant SDTs, NERC has made the change to the VSL in Reliability Standard PRC-005-2 and also made the change in Reliability Standard PRC-005-3, which has been adopted by the Board and since filed for regulatory approval.

V. **VRF and VSLs for BAL-003-1, Requirement R1.** The Board adopted Reliability Standard BAL-003-1 – Frequency Response and Frequency Bias Setting, on February 7, 2013. FERC issued Order No. 794 approving BAL-003-1 on January 16, 2014. This order directed the ERO to: 1) modify the Requirement R1 Violation Risk Factor to a "high" level, and 2) modify the Violation Severity Level for Requirement R1 to remove references to performance by other entities. NERC staff made the modifications to the VRF and VSL in Requirement R1 as directed.

Agenda Item 8.e
Board of Trustees Meeting
May 7, 2014

Physical Security Standard Project

Action
Information

Background
On March 7, 2014, the Federal Energy Regulatory Commission (FERC) issued an order directing NERC to submit for approval, within 90 days of the order, one or more Reliability Standards to address physical security risks and vulnerabilities of critical facilities on the Bulk Power System (BPS).[1]

Summary
The order focuses on critical facilities, directing steps to evaluate physical security threats and implement security plans that continues NERC's ongoing physical security efforts. In the order, FERC stated that the proposed standard(s) should require entities to take a least the following three steps:

- Perform a risk assessment to identify facilities that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or cascading failures on the BPS.
- Evaluate the potential threats and vulnerabilities to those identified facilities.
- Develop and implement a security plan designed to protect against physical attacks to those identified facilities based on the assessment of the potential threats and vulnerabilities to their physical security.

Additionally, FERC directed that the proposed Standard(s) should also: (1) include a procedure that will ensure confidential treatment of sensitive or confidential information; (2) include a procedure for a third party to verify the list of identified facilities and allow the verifying entity, as well as FERC, to add or remove facilities from the list of critical facilities; (3) include a procedure for a third party to review the evaluation of threats and vulnerabilities and the security plan; and (4) require that the identification of the facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. FERC directed that the proposed Physical Security Reliability Standard(s) be filed by June 5, 2014.

In response to the order, NERC staff and the Standards Committee (SC) worked together in order to develop an action plan for meeting the June 5, 2014 filing deadline. The SC approved several waivers to facilitate meeting the required timelines and seated the Standard Drafting Team (SDT) on March 21, 2014. Further details are provided below under the "Standards Development Process Update" section.

[1] *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

Pertinent directives from the FERC Order, *Reliability Standards for Physical Security Measures* 146 FERC ¶ 61,166 (2014):

Paragraph 5

Therefore, to carry out section 215 of the FPA and to provide for the reliable operation of the Bulk-Power System, the Commission directs the ERO to develop and file for approval proposed Reliability Standards that address threats and vulnerabilities to the physical security of critical facilities on the Bulk-Power System.

Paragraph 6

The Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the Bulk-Power System. First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities." A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System.

Paragraph 8

In the second step, the Reliability Standards should require owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities. The threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target. Thus, the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated.

Paragraph 9

Third and finally, the Reliability Standards should require those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security.

Paragraph 10

NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information that is needed to ensure compliance with the Reliability Standards.

Paragraph 11

In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity. The Reliability Standards should include a procedure for the verifying entity, as well as the

Commission, to add or remove facilities from an owner's or operator's list of critical facilities. Similarly, the determination of threats and vulnerabilities and the security plan should also be reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise. Finally, the Reliability Standards should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. NERC should establish a timeline for when such reevaluations should occur.

Standards Development Process Update

Section 16 of the Standards Processes Manual (SPM) allows SPM Provisions to be waived by the SC to meet a regulatory deadline. On March 21, 2014, the SC approved waivers to support drafting activities to meet the FERC-imposed regulatory deadline of June 5, 2014. The SC approved the following waivers of provisions from the SPM for the Physical Security Reliability Standards Project:

1. Standard Authorization Request (SAR) to be posted for a seven-calendar day informal comment period. (Sections 4.1-4.2)
2. Initial formal comment and ballot period reduced from 45 days to 15 calendar days, with a ballot conducted during the last 5 days of the comment period. Form ballot pool in first 10 days. (Sections 4.7-4.9)
3. Additional formal comment and ballot period(s) reduced from 45 days to 10 calendar days, with ballot conducted during the last five days of the comment period. (Sections 4.9 and 4.12)
4. Final ballot from 10 days to five calendar days. (Section 4.9)

On, March 21, 2014, the SC also accepted the Project 2014-04 Standard Authorization Request (SAR) for a seven-calendar day informal comment period posting, pursuant to the SC-approved waiver, and seated the SDT with 11 members. NERC staff posted the SAR from Friday, March 21, 2014, through Friday, March 28, 2014.

On April 1, 2014, NERC staff convened a technical conference in Atlanta, GA, to focus stakeholder discussion on developing a draft of a Physical Security Reliability Standard, with the intent of assisting the SDT to quickly develop and post a Reliability Standard for comment and ballot. The conference provided a forum for industry input on the concepts in the draft standard, to include criteria for determining applicable entities, identification of critical facilities, evaluation of potential threats and vulnerabilities, development and implementation of physical security plans, and the proposed standard's implementation plan. NERC compliance staff also provided an overview of the Reliability Standard Audit Worksheet (RSAW) approach. There were approximately 150 in-person attendees and 550 attendees registered to participate via audio and web presentation.

Given the SC waiver, the SDT developed the draft CIP-014-1 standard and posted it for a 15-calendar day initial formal comment and concurrent 10-day ballot period. NERC compliance

staff, with SDT and Regional Entity input, prepared and posted a draft RSAW concurrent with the posting of the draft standard. At the time of preparing these materials, the dates and results from the ballot were not available. NERC management will provide an update on the ballot results to the Standards Oversight and Technology Committee at the May 6, 2014 meeting and to the NERC Board of Trustees (Board) at the May 7, 2014 meeting.

In addition to completion of the initial formal comment and ballot period, NERC anticipates the SDT will meet the following timeline to complete the project through the standard drafting process:

1. **Early-May:** Additional posting (if needed) of draft CIP-014-1 for 10-day comment and concurrent five-day ballot period, pursuant to the SC-approved waiver.
2. **Mid to late May:** Five-day final ballot, pursuant to the SC-approved waiver.
3. **End of May to Early June (not later than June 5, 2014):** Board adoption; NERC staff file standard with applicable regulatory authorities.

Additional Information

A link to the project history and files is included here for reference:

[**Project 2014-04 Physical Security**]

Agenda Item 9
Board of Trustees Meeting
May 7, 2014

Proposed Amendments to the Delegation Agreement with SERC Reliability Corporation – Amended Exhibit B – the SERC Bylaws

Action

Approve proposed amendments to NERC's Delegation Agreement with SERC Reliability Corporation (SERC), consisting of amendments to Exhibit B – the SERC Bylaws, and file with applicable regulatory authorities for approval. The amendments to the SERC Bylaws do not affect SERC's qualifications to serve as a Regional Entity with delegated authority from NERC and do not adversely impact the ability of SERC to function as a Regional Entity under the Delegation Agreement.

Background

SERC is in the process of transitioning from an Alabama non-profit corporation to a North Carolina non-profit corporation, in consideration of its current base of operations and lack of substantial nexus to the state of Alabama. As part of this transition, SERC has formed a North Carolina non-profit corporation. In October 2012, the SERC Board approved the Articles of Incorporation and initial Bylaws for the North Carolina non-profit corporation. These Bylaws mirrored the pre-existing SERC Bylaws, save for a few amendments.

At the time these initial Bylaws were approved, the SERC Board also directed staff to consider whether it would be appropriate to seek tax-exempt status under Section 501(c)(3) of the Internal Revenue Code, rather than under Section 501(c)(6), the status of the Alabama corporation. The initially-approved Bylaws of the North Carolina corporation contained language necessary to support the 501(c)(3) application.

After consideration, it was decided that it would be preferable to maintain the same tax status for the North Carolina corporation, rather than to seek tax-exempt status under Section 501(c)(3), and in October 2013, the SERC Board unanimously approved amendments to the SERC Bylaws to codify this decision.

The following summarizes the amendments made to the SERC Bylaws. Items #2, 3, 5, 6, and 7 were approved by the SERC Board in October 2012. Items #1 and 4 were approved by the SERC Board in October 2013.

1. In Section 11.2, the "Distribution of Assets" provision was amended to remove language necessary for 501(c)(3) status. Section 501(c)(6) of the Internal Revenue Code requires different language in the Bylaws than is required under Section 501(c)(3). The changes

necessary to support this recommendation are needed prior to filing an application for tax-exempt status in North Carolina.

2. The Table of Contents was updated to reflect changes in pagination caused by the amendments to the Bylaws.

3. In Section 2.2, language was added to state that the terms "Bulk Power System," "Reliability Standards," and "Regional Entity" shall be as defined in 16 U.S.C. § 824o.

4. Section 2.6 was added to clarify that Member Companies shall be non-voting members and shall have no power or authority or right to vote with respect to the actions of the Corporation.

5. Section 4.2 was amended to require corporate affiliates to consolidate and coordinate their representation on the Board and any Board-level committees.

6. In Section 13.1, the terms "Alternate Director" and "Customer Advisor" were added to reflect that this Section applies to these representatives.

7. Article XIV was expanded to apply to the Articles of Incorporation.

The amendments to the SERC Bylaws do not affect SERC's qualifications to serve as a Regional Entity with delegated authority from NERC and do not adversely impact the ability of SERC to function as a Regional Entity under the Delegation Agreement. Accordingly, SERC requests that the Board approve the amended Bylaws and forward to FERC for approval and adoption as a replacement for Exhibit B to the SERC Delegation Agreement.

AMENDED AND RESTATED

BYLAWS

OF

SERC RELIABILITY CORPORATION

A North Carolina Nonprofit Corporation

Approved by the Board of Directors on October 23, 2013

TABLE OF CONTENTS

ARTICLE I - OFFICES 1
1.1 **Principal Office** 1
1.2 **Other Offices** 1

ARTICLE II - MEMBERSHIP 1
2.1 **General** 1
2.2 **Eligibility** 1
2.3 **Termination** 2
2.4 **Sectors** 2
2.5 **Transfer of Membership** 3
2.6 **Powers** 3

ARTICLE III - PURPOSES 3
3.1 **General Purposes** 3
3.2 **Geographic Area** 4
3.3 **Other Statutory Functions** 4

ARTICLE IV - BOARD OF DIRECTORS 4
4.1 **General Powers** 4
4.2 **Composition and Eligibility** 5
4.3 **Regular Meetings of the Board** 5
4.4 **Special Meetings of the Board** ..... ~~5~~6
4.5 **Notice of Special Meetings** 6
4.6 **Election of Board Officers and Executive Committee** 6
4.7 **Agenda** 6
4.8 **Voting Definitions** 6
4.9 **Determination of Adjusted Weighted Vote** 7
4.10 **Voting; Manner of Acting; Voting Rights; Quorum; Proxies** 8
4.11 **Compensation** 8
4.12 **Informal Action by Directors** 8
4.13 **Duties** 9

ARTICLE V - CORPORATE OFFICERS 9
5.1 **Corporate Officers** 9
5.2 **President & Chief Executive Officer** 9
5.3 **Vice President** 10
5.4 **Secretary** 10
5.5 **Treasurer** 10

ARTICLE VI - EXECUTIVE COMMITTEE 11
6.1 **Executive Committee Representatives** 11
6.2 **Ex Officio Representatives** 11
6.3 **Authority of Executive Committee** 11
6.4 **Action** 11

ARTICLE VII - OTHER COMMITTEES 12
7.1 **Designation by Board** 12
7.2 **Rules for Governance** 12
7.3 **Ad-Hoc Support Committees** 12

ARTICLE VIII - MISCELLANEOUS 12
8.1 **Conflicts of Interest** 12
8.2 **Contracts** 12
8.3 **Checks, Drafts, etc.** 12
8.4 **Deposits** 13
8.5 **Books and Records** 13
8.6 **Seal** 13
8.7 **Fiscal Year** 13

ARTICLE IX - EXPENSES 13
9.1 **Allocation of Specific Expenses** 13
9.2 **Statutory Functions** 13
9.3 **Non-Statutory Functions** 13

ARTICLE X - DISPUTE RESOLUTION PROCESS 14
10.1 **Dispute Resolution** 14

ARTICLE XI - DISSOLUTION 14
11.1 **Dissolution** 14
11.2 **Distribution of Assets** 14

ARTICLE XII - WAIVER OF NOTICE 14
12.1 **Waiver** 14

ARTICLE XIII - INDEMNIFICATION ..... ~~14~~15
13.1 **Indemnification of Directors, Committee Members, Officers, Employees and Agents** ..... ~~14~~15

ARTICLE XIV – AMENDMENT OF THE BYLAWS AND ARTICLES OF INCORPORATION 15
14.1 **Amendment of the Bylaws and Articles of Incorporation** 15

AMENDED AND RESTATED

BYLAWS

OF

SERC RELIABILITY CORPORATION
[Hereinafter referred to as the "Corporation"]

A North Carolina Nonprofit Corporation

ARTICLE I - OFFICES

1.1 **Principal Office**. The principal office of the Corporation shall be located in the City of Charlotte, Mecklenburg County, North Carolina. The Board of Directors may by resolution change the location of this office from time to time.

1.2 **Other Offices**. The Corporation may have other offices at such place or places as the Board of Directors may from time to time appoint or the business of the Corporation may require.

ARTICLE II - MEMBERSHIP

2.1 **General**. The Corporation shall be a membership corporation. Entities that meet the eligibility requirements and apply for membership in the Corporation shall hereinafter be referred to individually as a "Member Company" and collectively as "Member Companies".

2.2 **Eligibility**. Membership in the Corporation is open to any entity in the SERC Region (defined in Section 3.2 below) that is a user, owner or operator of the Bulk Power System and is subject to the jurisdiction of the Federal Energy Regulatory Commission for the purpose of complying with Reliability Standards established under Section 215 of the Federal Power Act and all amendments thereto. Membership in the Corporation is voluntary; however, membership is predicated on mandatory acceptance of the responsibility to promote, support, and comply with Reliability Standards of the Corporation and the North American Electric Reliability Corporation ("NERC"), and to assist the Corporation in its compliance with the terms and provisions of a Delegation Agreement (a "Delegation Agreement") with NERC, by which NERC delegates authority to propose and enforce Reliability Standards, pursuant to 16 U.S.C. § 824o or the corresponding provisions of any subsequent U.S. Code revisions. For purposes of

these Bylaws, the terms “Bulk Power System”, “Reliability Standards” and “Regional Entity” shall be as defined in 16 U.S.C. § 824o or the corresponding provisions of any subsequent U.S. Code revisions.

2.3 **Termination**. A Member Company may terminate its membership in the Corporation by giving the Board of Directors at least thirty (30) days written notice of its intent to terminate such membership (such Member Companies shall hereinafter be referred to as "Terminated Member Companies"). Terminated Member Companies shall nevertheless continue to be liable for any and all obligations incurred prior to the end of the calendar year in which such notice is given, including, but not limited to, the obligation to pay a pro rata share of any Corporation expense. In addition to termination of membership by the Member Company, the Board of Directors, following notice to the Member Company, may terminate the membership of a Member Company if in the judgment of the Board of Directors that Member Company has violated its obligations and responsibilities to the Corporation. The termination of the membership of a Member Company by the Board of Directors shall require a Supermajority vote, as defined in these Bylaws.

2.4 **Sectors.** Each Member Company shall be classified by the Executive Committee in one of the following seven (7) Sectors (each a “Sector”, and collectively, the “Sectors”):

(a) Investor-Owned Utility Sector – This Sector includes any investor-owned entity with substantial business interest in ownership and/or operation in any of the asset categories of generation, transmission or distribution.

(b) Federal/State Sector – This Sector includes any U.S. federal entity that owns and/or operates electric facilities and/or provides balancing authority services, in any of the asset categories of generation, transmission, or distribution; or any entity that is owned by or subject to the governmental authority of a state and that is engaged in the generation, delivery, and/or sale of electric power to end-use customers primarily within the political boundaries of the state.

(c) Cooperative Sector – This Sector includes any non-governmental entity that is incorporated under the laws of the state in which it operates, is owned by and provides electric service to end-use customers at cost, and is governed by a board of directors that is elected by the membership of the entity; and any non-governmental entity owned by and which provides generation and/or transmission service to such entities.

(d) Municipal Sector – This Sector includes any entity owned by or subject to the governmental authority of a municipality, that is

engaged in the generation, delivery, and/or sale of electric power to end-use customers primarily within the political boundaries of the municipality; and any entity, whose members are municipalities, formed under state law for the purpose of generating or purchasing electricity for sale at wholesale to their members.

(e) Marketer Sector– This Sector includes any entity that is engaged in the activity of buying and selling of wholesale electric power in the SERC Region on a physical or financial basis.

(f) Merchant Electricity Generator Sector – This Sector includes any entity that owns or operates an electricity generating facility or provides balancing authority services for such entities. This includes, but is not limited to, small power producers and all other non-utility producers such as exempt wholesale generators who sell electricity at wholesale.

(g) ISO-RTO Sector – This Sector includes any entity that operates a FERC approved ISO or RTO.

The Executive Committee's classification of a Member Company in a particular Sector may only be changed by the Executive Committee.

2.5 **Transfer of Membership.** A Member Company may not give or otherwise transfer its membership, except to a successor that becomes a Member Company in accordance with the terms and conditions of these Bylaws, and provided that the successor continues to meet its predecessor's obligations.

2.6 **Powers.** Notwithstanding any other provisions of these Bylaws, except for the appointment of Directors as provided in Section 4.2 below, Member Companies shall be non-voting members and shall have no power or authority or right to vote with respect to the actions of the Corporation, specifically including, but not limited to, the dissolution or merger of the Corporation.

ARTICLE III - PURPOSES

3.1 **General Purposes.** The purpose of the Corporation is to promote effective and efficient administration of Bulk Power System reliability in the SERC Region, as defined in Section 3.2. In pursuit of this goal, the Corporation shall:

(a) enter into a Delegation Agreement to serve as a Regional Entity pursuant to 16 U.S.C. § 824o or the corresponding provisions of any subsequent U.S. Code revisions;

(b) promote the development of reliability and adequacy arrangements among the systems in the SERC Region;

(c) participate in the establishment of Reliability Standards;

(d) participate in the measurement of performance relative to these Reliability Standards;

(e) promote conformance to and compliance with these Reliability Standards;

(f) develop and exchange information with respect to planning and operating matters relating to the reliability and adequacy of the Bulk Power System;

(g) review as necessary activities in the SERC Region on reliability and adequacy in order to meet Reliability Standards;

(h) provide a mechanism to resolve disputes on reliability issues in a manner that meets the needs of the parties and the SERC Region; and

(i) provide information with respect to matters considered by the Corporation, where appropriate, to the Federal Energy Regulatory Commission ("FERC") and to other federal and state agencies concerned with reliability and adequacy.

3.2 **Geographic Area.** The Corporation accomplishes its purposes in a geographic area (the "SERC Region") that is defined in Exhibit A of the Amended and Restated Delegation Agreement Between North American Electric Reliability Corporation and SERC Reliability Corporation.

3.3 **Other Statutory Functions.** The Corporation may also perform statutory functions outside of the SERC Region, on behalf of NERC or other Regional Entities. The Corporation may undertake such activities pursuant to a contract that is approved by the Executive Committee.

ARTICLE IV - BOARD OF DIRECTORS

4.1 **General Powers**. The affairs of the Corporation shall be managed by its Board of Directors except as otherwise provided in these Bylaws.

4.2 **Composition and Eligibility**. The Board of Directors shall be comprised of no fewer than three (3) Directors and no more than two (2) Customer Advisors.

Each Director shall be the principal officer or other authorized employee from a Member Company or a company that controls, is controlled by, or is under common control with such Member Company (an "affiliated entity"). Each Member Company, together with any affiliated entities, may appoint one (1) Director to the Board of Directors. For clarification purposes only, each Member Company and all of such Member Company's affiliated entities (including any affiliated entities which may be a separate Member Company) shall have the right to appoint only one (1) Director to serve on behalf of such Member Company and all of such Member Company's affiliated entities. Each Director shall serve until otherwise replaced by the applicable Member Company, together with any affiliated entities. Each Member Company, together with any affiliated entities, may designate one (1) alternate Director, who shall be a principal officer or other authorized employee from the Director's Member Company or an affiliated entity, to serve in the place of the Member Company's Director at any meeting of the Board of Directors (an "Alternate Director"). Directors may not otherwise use proxy votes. Any vacancy occurring among the Directors or Alternate Directors shall be filled by the applicable Member Company, together with any affiliated entities.

Each Customer Advisor shall be a person who is (i) employed by an entity that receives service at retail and does not otherwise sell, purchase, or transmit power over the Bulk Power System or own, operate or maintain, control or operate facilities or systems that are part of the Bulk Power System; (ii) a state public utility commission representative; or (iii) any other customer advocate. Should the Board of Directors not include two (2) Customer Advisors, the Board of Directors may elect additional Customer Advisors to fill such vacancies. The term of these Customer Advisors shall be for a two (2) year period.

The Chair of FERC and the chair or president of any State Utility Commission in a state in which electric service is provided by a Member Company of the Corporation shall be invited to designate an observer to attend meetings of the Board.

4.3 **Regular Meetings of the Board**. Unless otherwise determined by the Chair, a regular meeting of the Board of Directors shall be held without other notice than these Bylaws on the fourth Wednesday in the months of April and October in each year. Notwithstanding the foregoing, the Chair may elect to hold a regular semi-annual meeting of the Board of Directors on another date provided that the Board receives at least ten (10) days advance notice. If the day fixed for the meeting shall be a legal holiday in the State of North Carolina, the meeting shall be held on the next succeeding business day. The Board of Directors may designate any place as the place of meeting for any meeting. The Board of Directors may provide by resolution the time and place for the holding of additional regular meetings of the Board without other notice than the resolution. Directors or any committee designated by the Board of Directors may participate in such Board or committee meetings by means of a telephone conference, webcast or any other communication by means of which all persons participating in the

meeting can hear each other at the same time, and participation by such means shall constitute presence in person at such meeting.

4.4 **Special Meetings of the Board**. Special meetings of the Board of Directors may be called at the request of the Chair, or by Directors holding twenty percent (20%) or more of the Individual Votes. The Chair may fix any place as the place for holding any special meeting of the Board.

4.5 **Notice of Special Meetings**. Notice of any special meeting of the Board of Directors shall be given at least two (2) days prior to the special meeting by written notice delivered personally, or sent by mail or electronic mail to each Director at the address as shown by the records of the Corporation. If mailed, such notice shall be deemed to be delivered when deposited in the United States mail in a sealed envelope so addressed, with postage prepaid. If sent by electronic mail, such notice shall be deemed to be delivered when sent via electronic mail. Any Director may waive notice of any meeting. The attendance of a Director at any meeting shall constitute a waiver of notice of such meeting, except where a Director attends a meeting for the express purpose of objecting to the transaction of any business because the meeting is not lawfully called or convened. Neither the business to be transacted at, nor the purpose of, any special meeting of the Board need be specified in the notice or waiver of notice of such meeting, unless specifically required by law or by these Bylaws.

4.6 **Election of Board Officers and Executive Committee**. Biennially, at the April meeting, the Board of Directors shall elect Board Officers from among the Directors for the positions of Chair, Vice Chair, and Secretary-Treasurer, each for a term of two (2) years beginning on July 1st after the election. No Director may serve in more than one (1) Board Officer position at the same time. The Chair shall conduct all meetings and shall be responsible for the preparation of the agenda. In the Chair's absence, the Vice Chair shall serve as acting Chair. In the event that a Board Officer cannot complete his or her term, the Board of Directors may hold a special election to elect a replacement Board Officer for the remainder of the unexpired term.

At the same time, the Board shall also approve representatives to the Executive Committee nominated by the Sectors to serve for a period of two (2) years. Each Sector may also elect alternates to the Executive Committee, and, if a Sector has more than one (1) representative on the Executive Committee, such Sector shall designate the priority of succession by such alternates.

4.7 **Agenda**. As far in advance of each regular and special meeting as practical, an agenda shall be distributed to each Director and Customer Advisor.

4.8 **Voting Definitions**.

(a) "Adjusted Weighted Vote" shall mean the number of votes of each Director determined in the manner set forth in Section 4.9 hereof.

(b) "Simple Majority" shall require the presence of a quorum and the (i) concurrence of Directors whose combined Individual Votes are greater than fifty percent (50%) of the total Individual Votes of all Directors present at the meeting and entitled to vote on the issue (the "Individual Vote Test"), (ii) concurrence of Directors whose combined Adjusted Weighted Votes are greater than fifty percent (50%) of the total Adjusted Weighted Vote of all Directors at the meeting and entitled to vote on the issue (the "Adjusted Weighted Vote Test"), and (iii) for at least one of the Individual Vote Test or the Adjusted Weighted Vote Test, on an individual Sector basis, the positive vote shall outweigh the negative vote for at least three Sectors.

(c) "Supermajority" shall require the presence of a quorum and the concurrence of (i) Directors whose combined Individual Votes equal or exceed two-thirds (2/3) of the total Individual Votes of all Directors present at the meeting and entitled to vote on the issue, provided that a quorum is present, and (ii) Directors whose combined Adjusted Weighted Votes are greater than two-thirds (2/3) of the total Adjusted Weighted Vote of all Directors present at the meeting and entitled to vote on the issue.

(d) "Individual Vote" shall mean a single vote accorded to each Director.

(e) "Given Year" shall mean the applicable fiscal year for which the Adjusted Weighted Votes are calculated.

(f) "Reporting Year" shall mean the fiscal year immediately preceding the Given Year.

(g) "Previous Year" shall mean the fiscal year immediately preceding the Reporting Year.

4.9 **Determination of Adjusted Weighted Vote**. The Directors' Adjusted Weighted Votes for a Given Year shall be determined by the following formula:

V = 10(1/N) + 30(B/C) + 30(D/E) + 30(F/G)

V = % of Adjusted Weighted Vote

N = total number of Member Companies

B = Member Company's Previous Year internal peak demand

C = total of factor B for all Member Companies

D = Member Company's owned generating capacity as of January 1 of the Reporting Year

E = total of factor D for all Member Companies

F = Member Company's sum of circuit miles of transmission times the respective operating voltage for facilities of 69 kV and above as of December 31 of the Previous Year

G = total of factor F for all Member Companies

4.10 **Voting; Manner of Acting; Voting Rights; Quorum; Proxies**.

(a) Except as otherwise provided in these Bylaws, all actions by the Board of Directors require approval by a Simple Majority vote.

(b) A motion shall be deemed to have passed if it passes either:

(i) the Individual Vote Test; or
(ii) the Adjusted Weighted Vote Test;

and, for purposes of the failed test (any test that is not satisfied), on an individual Sector basis, the positive votes outweigh the negative votes in every Sector but one.

(c) Directors holding two-thirds (2/3) of the Individual Votes shall constitute a quorum for action by the Board. If Directors holding less than two-thirds (2/3) of the Individual Votes are present at the meeting, a majority of the Directors present may adjourn the meeting from time to time without further notice.

(d) The intent of Section 4.8(b)(iii) and Section 4.10(b) is to ensure that no two Sectors should be able to control any decision and that a single Sector should not be able to veto any matter, respectively (other than amendments to these Bylaws). In the event that either of the foregoing shall nevertheless occur, the Member Companies shall promptly revise the provisions of these Bylaws so that no two Sectors shall be able to control any decision and no single Sector shall be able to veto any matter.

4.11 **Compensation**. Directors shall not receive any compensation from the Corporation for their services to the Corporation.

4.12 **Informal Action by Directors**. Any action required by law to be taken at a meeting of Directors, or any action which may be taken at a meeting of Directors, may

be taken without a meeting if all of the Directors consent in writing to the action so taken.

4.13 **Duties**. The Board of Directors shall have the exclusive responsibility to:

(a) Authorize distributions;

(b) Recommend to members or approve dissolution, merger or the sale, pledge or transfer of substantially all of the ~~c~~Corporation's assets;

(c) Fill vacancies on any of the Board's committees;

(d) Adopt, amend, or repeal the Articles of Incorporation or Bylaws;

(e) Form or dissolve committees of the Board as it deems necessary to carry out the business of the Corporation; and

(f) Resolve any disputes regarding the Member Companies and the Corporation, if those issues cannot be resolved by the standing committees or subcommittees of the Corporation and are not otherwise subject to NERC's dispute provisions for non-compliance with Reliability Standards.

ARTICLE V - CORPORATE OFFICERS

5.1 **Corporate Officers**. The Board of Directors shall appoint a President & Chief Executive Officer, Vice President, Secretary, and Treasurer of the Corporation. Two (2) or more of such offices may be held by the same person, except for the offices of President & Chief Executive Officer and Secretary. The Board of Directors may appoint such other officers and assistant officers as it deems necessary.

5.2 **President & Chief Executive Officer**. The President shall be the Chief Executive Officer of the Corporation and shall manage the operations of the Corporation to the end that its purposes shall be accomplished. The Board Officers shall determine the compensation and benefits for the President & Chief Executive Officer (President). The President shall:

(a) Attend all Board of Directors meetings of the Corporation and NERC Stakeholder and Board of Trustees, meetings, as appropriate;

(b) Assist and coordinate the preparation of testimony and reports;

(c) Coordinate subregional activities and interregional affairs, to include data collection;

(d) Install and maintain an adequate system of accounts and records;

(e) Arrange for meetings as directed;

(f) Assist the Corporation Committee Chairs as appropriate;

(g) Manage the business affairs of the Corporation, including the Corporation staff;

(h) Maintain minutes of all the Corporation-related meetings; and

(i) Provide other assistance to the Corporation and NERC, as appropriate.

5.3 **Vice President.** The Vice President shall perform such duties and exercise such powers as may be assigned to him or her from time to time by the Board of Directors, the Executive Committee, or the President. In the absence of the President, or in the case of the President's inability to act, the Vice President shall perform the duties and exercise the powers of the President, but subject to the control of the Board of Directors and the Executive Committee. The Board Officers shall determine the compensation and benefits of the Vice President.

5.4 **Secretary.** The Secretary shall be custodian of the records and of the seal of the Corporation and in general shall perform all duties incident to the office of Secretary and such other duties as may, from time to time, be assigned to him or her by the Board of Directors, the Executive Committee, or the President.

5.5 **Treasurer.** The Treasurer shall have charge and custody of, and be responsible for, all funds and securities of the Corporation and deposit all such funds in the name of the Corporation in such banks, trust companies, or other depositaries as shall be selected in accordance with the provisions of these Bylaws; and in general, perform all of the duties incident to the office of Treasurer and such other duties as from time to time may be assigned to him or her by the Board of Directors, the Executive Committee, or the President.

ARTICLE VI - EXECUTIVE COMMITTEE

6.1 **Executive Committee Representatives**. The Executive Committee shall be comprised of twelve (12) Sector representatives from the Board of Directors, consisting of:

(a) The Investor-Owned Utility Sector shall have three (3) representatives;

(b) The Federal/State Sector shall have two (2) representatives;

(c) The Cooperative Sector shall have two (2) representatives;

(d) The Municipal Sector shall have two (2) representatives;

(e) The Marketer Sector shall have one (1) representative;

(f) The Merchant Electricity Generator Sector shall have one (1) representative; and

(g) The ISO-RTO Sector shall have one (1) representative.

It is the desire of the Board of Directors that the Cooperative and Municipal sectors have representation from both transmission dependent and transmission owning Members. Each Sector shall be responsible for nominating their representative(s) and alternates from among the Directors. The Chair of the Board shall serve as Chair of the Executive Committee and shall conduct all meetings and shall be responsible for the preparation of the agenda. In the event that a representative on the Executive Committee is unable to complete a term, the Sector's alternate shall replace such representative.

6.2 **Ex Officio Representatives**. The Chair, Vice Chair, and Secretary-Treasurer of the Board of Directors shall also be ex officio representatives on the Executive Committee, but shall not have voting rights unless such Board Officer is also elected by a Sector to the Executive Committee pursuant to Section 6.1 above.

6.3 **Authority of Executive Committee**. Except as limited by Section 55A-8-25 of the North Carolina Nonprofit Corporation Act and Section 4.13 of these Bylaws, the Executive Committee is empowered to make all such decisions and take such actions as are deemed to be necessary for the operation of the Corporation.

6.4 **Action.** Each voting representative on the Executive Committee shall have one vote. The presence of three-quarters (3/4) of the voting representatives on the Executive Committee shall constitute a quorum. The positive vote of two-thirds

(2/3) of Executive Committee voting representatives present and voting is necessary to pass a particular action.

ARTICLE VII - OTHER COMMITTEES

7.1 **Designation by Board**. The Board of Directors, by resolution adopted by a Simple Majority vote, may designate Board committees and standing committees, as shall be necessary to address the purposes of the Corporation. Each Board committee shall have at least two Directors among its members.

7.2 **Rules for Governance**. Each committee shall adopt rules for its own governance that are not inconsistent with these Bylaws, rules adopted by the Board of Directors, applicable NERC or FERC rules or regulations, or applicable state or federal laws. Each committee shall maintain its rules for governance in a written scope document that is approved by the Board of Directors.

7.3 **Ad-Hoc Support Committees**. The Board or its committees may, from time to time, appoint ad-hoc committees to research and/or advise it on compliance or technical issues or matters, among other things. Such ad-hoc committees may be formed on an as-needed basis and may vary in makeup depending on the needs of the Board or its committees.

ARTICLE VIII - MISCELLANEOUS

8.1 **Conflicts of Interest.** All Directors, Alternate Directors, Customer Advisors, and Board committee representatives shall comply with the Corporation's Standards of Conduct policy that prohibits conflicts of interest, as such conflicts could cast doubt on the ability of such persons to act with total objectivity with regard to the overall interests of the Corporation.

8.2 **Contracts**. The Board of Directors may authorize any officer or agent of the Corporation, in addition to the officers so authorized by these Bylaws, to enter into any contract or execute and deliver any instrument in the name of and on behalf of the Corporation, and such authority may be general or confined to specific instances.

8.3 **Checks, Drafts, etc**. All checks, drafts, or orders for the payment of money, notes or other evidences of indebtedness issued in the name of the Corporation, shall be signed by an authorized officer or agent of the Corporation and in such manner as shall from time to time be determined by resolution of the Executive Committee. In the absence of such determination by the Executive Committee, such

instruments shall be signed by the Board's Secretary-Treasurer, the Corporation's President, or the Corporation's Finance Director, as stipulated by the Executive Committee. The Corporation's Finance Director may arrange audits of financial records, sign appropriate documents, and perform such duties normally performed by the Board's Secretary-Treasurer, except duties assigned to the Corporation's President.

8.4 **Deposits**. All funds of the Corporation shall be deposited from time to time to the credit of the Corporation in such banks, trust companies, or other depositories as the Corporation's President may select.

8.5 **Books and Records**. The Corporation shall keep correct and complete books and records of account and shall also keep minutes of the proceedings of the Board of Directors and committees having any of the authority of the Board of Directors, and shall keep at its registered or principal office a record giving the names and addresses of the Directors. All books and records of the Corporation may be inspected by any Director, or agent or attorney representing any Director, for any proper purpose at any reasonable time.

8.6 **Seal**. The corporate seal shall be in circular form and shall have inscribed thereon the name of the Corporation, the words "Corporate Seal", and such other word or words, if any, as may be determined by the Board of Directors to be inscribed thereon.

8.7 **Fiscal Year.** The fiscal year of the Corporation shall begin on the first day of January and end on the last day of December in each year.

ARTICLE IX - EXPENSES

9.1 **Allocation of Specific Expenses.** The expenses of Directors and Board Officers shall be borne by that person's regular employer.

9.2 **Statutory Functions.** The Corporation anticipates that as a general rule all of its expenses shall be incurred in the furtherance of statutory activities pursuant to Section 215 of the Federal Power Act, and that all such expenses shall be funded by NERC, subject to FERC approval.

9.3 **Non-Statutory Functions.** Notwithstanding Section 9.2, the Board of Directors may from time to time authorize the Corporation to participate in non-statutory activities (i.e., activities not described in Section 215 of the Federal Power Act). In the event that the Corporation proposes to engage in non-statutory activities, such activities shall be identified in the Corporation's annual business plan that is submitted to NERC and, if approved by NERC, shall be submitted to FERC for approval in advance of engaging in such non-statutory activities. The expenses incurred by the Corporation for

any such approved non-statutory activities shall be allocated by the Board of Directors to the beneficiaries of such activities on a basis proposed in the business plan submitted for NERC and FERC approval.

ARTICLE X - DISPUTE RESOLUTION PROCESS

10.1 **Dispute Resolution.** All disputes regarding non-compliance with Reliability Standards shall be handled in accordance with the NERC Rules of Procedure. The organizational units of the Corporation shall deal with all other disputes within the framework of their respective organizations. For such other disputes, Member Companies of the Corporation are encouraged to utilize the appropriate Dispute Resolution Process within the Corporation prior to seeking resolution at NERC, FERC, or with legal counsel.

ARTICLE XI - DISSOLUTION

11.1 **Dissolution**. The Corporation may be voluntarily dissolved upon unanimous consent of its Member Companies, and in accordance with Section 55A-14-02 of the North Carolina Nonprofit Corporation Act, as amended from time to time.

11.2 **Distribution of Assets**. Upon dissolution of the Corporation as provided in Section 11.1, the residual assets, after payment of all just obligations, shall be distributed exclusively to organizations which are exempt from federal income tax under ~~Section 501(c)(3)~~Section 501(c)(6) of the Internal Revenue Code of 1986, or corresponding provisions of any subsequent federal tax laws, as the Board of Directors shall determine, ~~or to federal, state, or local governments to be used exclusively for public purposes.~~

ARTICLE XII - WAIVER OF NOTICE

12.1 **Waiver.** Whenever any notice is required to be given under the provisions of the North Carolina Nonprofit Corporation Act or under the provisions of the articles of incorporation or the Bylaws of the Corporation, a waiver thereof in writing signed by the person or persons entitled to such notice, whether before or after the time stated therein, shall be deemed equivalent to the giving of such notice.

ARTICLE XIII - INDEMNIFICATION

13.1 **Indemnification of Directors, Alternate Directors, Customer Advisors, Committee Members, Officers, Employees and Agents**. Every person who is, or has served as, a Director, Alternate Director, Customer Advisor, committee member, Officer, ~~Director by virtue of serving as an Alternate Director,~~ employee, or agent of the Corporation shall be indemnified by the Corporation in the manner and to the extent authorized by the North Carolina Nonprofit Corporation Act. The foregoing rights of indemnification shall be without prejudice to any other rights to which any such Director, Alternate Director, Customer Advisor, committee member, Officer, ~~Alternate Director,~~ employee, or agent may be entitled as a matter of law.

ARTICLE XIV - AMENDMENT OF THE BYLAWS AND ARTICLES OF INCORPORATION

14.1 **Amendment of the Bylaws and Articles of Incorporation**. After a request by twenty percent (20%) of the Board of Directors or an affirmative vote of the Executive Committee, a proposal to amend the Bylaws or the Articles of Incorporation shall be put before the Board of Directors at any regular or special meeting for a vote. Copies of the proposed amendments shall be distributed to the Board of Directors at least thirty (30) days before the meeting at which they are to be considered. An amendment to the Bylaws or the Articles of Incorporation shall be adopted after being approved by a Supermajority vote of the Board of Directors, provided that a quorum is present.

Agenda Item 10
Board of Trustees Meeting
May 7, 2014

2014 State of Reliability Report

Action
Information

Background
The NERC *2014 State of Reliability Report* continues to build upon the analysis and findings presented in the *2013 State of Reliability Report*[1]. This report focuses on analyses of specific aspects of the performance of the bulk power system reliability, based on the integration of a wide variety of information and data sources.

The State of Reliability Report is prepared annually at the request of the Operating Committee and Planning Committee. The primary leads for report development were NERC's Performance Analysis Subcommittee (PAS) and NERC staff in collaboration with many technical support groups, each focused on evaluating specific aspects of reliability, including the Resources Subcommittee (RS), Frequency Working Group (FWG), Operating Reliability Subcommittee (ORS), Event Analysis Subcommittee (EAS), Reliability Assessment Subcommittee (RAS), Protection System and Control Subcommittee (SPCS), Protection System Misoperations Task Force (PSMTF), Transmission Availability Data System Working Group (TADSWG), Generating Availability Data System Working Group (GADSWG), Demand Response Availability Data System Working Group (DADSWG), Spare Equipment Database Working Group (SEDWG), and Compliance and Certification Committee (CCC).

The report objectively reviews and assesses the state of reliability based on the analysis of data and metric trends. The report also provides an integrated view of reliability performance, and identifies potential reliability issues. The key findings and recommendations of the report serve as the technical foundation for NERC's range of risk-informed efforts addressing reliability performance, and serve as key inputs to the annual *RISC Report* and report on *Top Priority Reliability Risks*. The metrics measured in the report address the characteristics of an adequate level of reliability (ALR) and trends indicate the bulk power system has been performing consistently well. There are no significant upward or downward trends from 2009 to 2013.

An overview of the report and key findings will be presented herein with consideration of the final report expected to occur at a future Board meeting.

[1] http://www.nerc.com/pa/RAPA/PA/Performance Analysis DL/2013_SOR_May 15.pdf

Agenda Item 11
Board of Trustees Meeting
May 7, 2014

2014 Summer Reliability Assessment Status Update

Action Required
None

Background
The objectives for NERC's Summer Reliability Assessment are to identify, assess, and report areas of concern regarding the reliability of the North American bulk power system and to make recommendations if actions are needed. The assessment identifies potential summer resource deficiencies and operating reliability concerns, determines peak electricity demand and supply changes, and highlights unique regional challenges. The assessment represents the results of working with the Reliability Assessment Subcommittee (RAS), the Regions, and NERC staff to develop sound technical basis for understanding these challenges. The report is intended to enable entities to better anticipate and respond in ways that ensure bulk power system reliability.

NERC will issue its *2014 Summer Reliability Assessment* on May 15, 2014. The following preliminary findings have been presented to the RAS as potential issues for the upcoming summer:

- **NERC Assessment Areas to Meet the Summer Reference Margin Levels**
  - TRE-ERCOT: adequate margins depend on pending capacity expected in August
  - MISO: unit retirements, derates, and mothballs contribute to reduced margins
  - NPCC-New England: reduced reserve margins due to recent unplanned outages
- **Summer Gas-Electric Transportation Considerations**
  - Meeting summer peaks with increasing dependence on gas-fired
  - Summer pipeline maintenance can create constraints that impact supply
  - Localized deliverability impacts in the Southeast caused by hurricanes
- **Continued Impacts of Baseload Retirements**
  - Contribute to reduced reserve margins in some areas.
  - Ontario retired last coal plant in April; Anticipated Margin is 10 percent lower compared to last summer.
  - Planners and operators continue to address localized reliability issues through transmission enhancements and replacement capacity.
- **Other highlights include (still under evaluation)**:
  - **MISO-South Integration -** North-south transmission constraints
  - **California Drought Impacts -** Conditions have improved substantially since March; issues could arise as drought is expected to continue

- **Rail Shipments of Coal in the Midwest -** Capacity shortfalls will not be an issue this summer; NERC will provide an update and address more thoroughly in the 2014 Long Term Reliability Assessment.

RAS set the draft schedule below for the *2014 Summer Reliability Assessment*:

Dates	Description
Tuesday, April 29	Final draft sent to PC/OC/MRC
Monday, May 5	PC webinar review and approval
Tuesday, May 6	Final draft sent to NERC Board of Trustees
Tuesday, May 13	NERC Board of Trustees webinar review and approval
Wednesday, May 15	Target release

Agenda Item 12
Board of Trustees Meeting
May 7, 2014

ERO Enterprise and Corporate Performance Metrics

Action

Approve the 2014 performance metrics, as an enclosure to the February 6, 2014 ERO Enterprise Strategic Plan.

Background

On February 6, 2014 the NERC Board of Trustees approved the ERO Enterprise Strategic Plan for the 2014-2017 planning period and deferred approval of the proposed performance metrics until its May 7th meeting. On March 20th, the Corporate Governance and Human Resources Committee approved the revised 2014 Performance Metrics for NERC staff compensation purposes and recommended Board approval of the revised metrics for use in the ERO Strategic Plan. These performance metrics will be used to assess the overall effectiveness of the enterprise in addressing risk to the bulk electric system (BES), achieving reliability results, assuring standards and compliance effectiveness and improving risk mitigation and program execution.

Revisions to the metrics include:

- Metric 1: revised to consider a composite of category 1-3 events through more accurate measurement of frequency and impact to determine the influence of NERC on improving reliability. The Daily event Severity Risk Impact data and a statistical evaluation to minimize randomness will be used to create a consistent measurable value for measurement of performance.
- Metric 3: the measure has been revised to include a listing of specific actual and potential risks identified for mitigation.
- Sub-Metric A: the Standards Committee and NERC Staff will work together to develop a periodic review process for steady state Reliability Standards. The process will include a quality and content review and the use or adaptation of the 2013 Independent Expert Review Team's quality and content scoring system will be considered during development. The review will be conducted by a cross-functional task force that will consist of Committee chairs, NERC management, NERC and stakeholder subject matter experts, and other parties as deemed necessary and appropriate. This review may also be incorporated into the current Standards Processes Manual periodic review process to avoid duplication of effort. So that the task force will be able to identify Reliability Standards for inclusion in the 2016-2018 Reliability Standards Development Plan, the task force will be operational no later than mid-2015 to allow ample time for the development of the annual task force review timeline.

Enclosed Attachment

1. ERO Enterprise Strategic Plan, 2014-2017 with enclosed 2014 Performance Metrics

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Electric Reliability Organization (ERO) Enterprise Strategic Plan 2014-2017

A multi-year strategic plan for the Electric Reliability Organization (ERO) Enterprise was originally developed in 2012. The plan was significantly expanded in early 2013 to include additional details on deliverables. The updated draft plan below is intended for use by NERC and Regional Entities in developing 2015 business plans. New this year, is the addition of ERO Enterprise performance metrics that will be initially used in 2014.

The ERO Enterprise is a collaborative, international network comprised of the North American Electric Reliability Corporation (NERC) and the eight Regional Entities that brings together collective leadership, experience, judgment, skills, and technologies for ensuring the reliability of the North American bulk power system. This plan summarizes the ERO Enterprise's mission, vision, values and goals; and provides strategic direction and priorities for 2014 and beyond.

Mission

To ensure the reliability of the North American bulk power system.

Vision

To be the trusted leadership that ensures the reliability of the North American bulk power system by implementing relevant standards; promoting effective collaboration, cooperation, and communication around important risks to reliability; and utilizing expertise from the industry to produce outcomes that effectively manage risks to reliability, in a cost effective manner.

Core Values and Guiding Principles

The following core values and guiding principles serve as guidelines for the conduct and behavior of all involved in the ERO Enterprise.

Accountability and Independence — The ERO Enterprise will:

- Be accountable for the public responsibilities delegated to it (a public trust obligation).
- Be impartial, independent of special interests, and impervious to improper influence.
- Balance its own independent regulatory judgment with the need to involve those with expert knowledge and experience in bulk power system reliability matters.

Responsiveness — The ERO Enterprise will act in a timely manner on the basis of unfolding events, emerging reliability risks, and the needs of industry and other stakeholders.

Fairness and Inclusiveness — The ERO Enterprise will:

- Be open and transparent.
- Provide access for clear communication with stakeholders.
- Ensure the legitimate interests of all parties, including costs imposed on registered entities, are duly considered and balanced in the development of policies and reliability standards, and in its programs and operations.
- Conduct compliance and enforcement actions judiciously and in proportion to risk, paying regard to both potential and actual (realized) risks.

Adaption and Innovation — The ERO Enterprise will:

- Continuously assess and prioritize its goals.
- Embrace change and encourage new ideas that contribute to effective action.
- Recognize the complex relationships and potential tensions between reliability objectives and business imperatives (including cost control).
- Be nimble and artful in development of tools and dissemination of lessons learned and other information to respond to novel, unfamiliar, and emerging challenges.

Excellence —The ERO Enterprise will:

- Promote and rely upon the active participation of the best technical leaders from industry.
- Strive for excellence and efficiency in all aspects of Enterprise activities.

Efficiency —The ERO Enterprise will make informed decisions regarding efficient use of its resources and resources shared by industry, with due consideration of the cost to industry.

Integrity — The ERO Enterprise will:

- Maintain the highest levels of professional and ethical conduct.
- Be independent, impartial, fair, intellectually honest, truthful, and candid.
- Be rigorous and thorough in all it does, doing the right things the right way.
- Earn trust by treating every person with fairness and respect.
- Work to meet or exceed expectations of stakeholders.

Four Pillars for Success

In order to succeed, the ERO Enterprise will emphasize:

- ***Reliability*** – to address events and identifiable risks, thereby ensuring the reliability of the bulk power system through proper mitigation and remediation.
- ***Assurance*** – to provide assurance to the public, industry, and government for the reliable performance of the bulk power system.
- ***Learning*** – to promote learning and continuous improvement of operations and adapt to lessons learned for bulk power system reliability.
- ***Risk-based Approach*** – to focus attention, resources and actions on issues most important to bulk power system reliability.

Strategic Goals 2014 – 2017

The ERO Enterprise has identified five goals in the strategic areas of standards; compliance, registration and certification; risks to reliability; and coordination and collaboration.

Standards

Goal 1. **Develop clear, reasonable and technically sound mandatory reliability standards in a timely and efficient manner.** These standards establish threshold requirements for ensuring the bulk power system is planned, operated, and maintained in a manner that minimizes risks of cascading failures, avoids damage to major equipment, or limits interruptions of bulk power supply.

Objectives and valued outcomes include:

a. Standards are clear, responsive to reliability and security risks, practical to implement and cost effective.

Key deliverables include:

- Ensure all new standards meet quality and results-based criteria[1] by 2017 with subsequent review every five years thereafter, including addressing quality and content issues identified in the 2013 Independent Expert Review Team Report and the work of the standing committees and the Reliability Issues Steering Committee (RISC) and others
- Evaluate significant bulk power system events (Category 3 and above) to identify any gaps in standards and address any such gaps.

[1] Quality criteria are the attributes of excellent reliability standards as stated in Section 300 of NERC's Rules of Procedure. Results based criteria mean each requirement defines a performance outcome, risk mitigation, or essential competency necessary for a reliable bulk power system.

- Develop a bulk power system risk profile and assess standards compared to the profile, address the most important unmitigated risks including applicable high impact low frequency risks.
- Address all high priority risks designated for control by a standard within one year or two years if technical study is required.
- Address all new FERC directives within one year or two years if technical study is required; close all pre-2013 directives by 2015 (by filing or negotiated resolution).
- Facilitate smooth transition of new standards (e.g., CIP Version 5).
- Consolidate to a common set of RSAWs, or successors, for all standards.
- Identify and file requirements to be retired (e.g., Paragraph 81 Phase 2), including addressing recommendations from the Independent Expert Review Team, the standing committees, the Reliability Issues Steering Committee (RISC) and others.
- Develop and implement procedures for assessing the cost effectiveness of reliability standards, as needed.

Compliance, Registration and Certification

Goal 2. **Be a strong enforcement authority that is independent, without conflict of interest, objective and fair and promote a culture of reliability excellence through risk-informed compliance monitoring and enforcement.** The ERO retains and refines its ability to use standards enforcement when warranted and imposes penalties and sanctions commensurate with risk.

Objectives and valued outcomes include:

a. The ERO registers entities commensurate with risk to the bulk power system and ensures all key reliability entities are certified to have essential capabilities.

Key deliverables include:

- Implement the BES exception process.
- Evaluate the certification program for sufficiency and effectiveness, modify as needed.
- Develop a framework and implement criteria for registration based on risk to the bulk power system.
- Develop common and consistent registration processes, information systems and methods among regions.

b. The ERO holds industry accountable for violations that create serious risk to the bulk power system; resulting actions are timely and transparent to industry.

Key deliverables include:

- Develop and implement the Reliability Assurance Initiative (enforcement reform) which includes the objective of improving the efficiency and effectiveness of NERC and Regional Entity operations by focusing on serious risk violations, reducing unnecessary costs of compliance on registered entities while, in each case, ensuring reliability objectives are achieved.
- Develop and implement new caseload and mitigation aging curves and monitor caseload and mitigation performance.
- Develop and implement enforcement strategies based on the Reliability Assurance Initiative, including enhancements to Find, Fix, and Track (FFT).
- Continue to expand use of enforcement discretion.

Goal 3. Promote a culture of compliance that supports reliability excellence within industry. The ERO works with industry to identify standards, procedures, practices and controls to address reliability risks.

Objectives and valued outcomes include:

a. Industry has effective procedures and programs to monitor, detect, correct, report, and prevent compliance, reliability, and security issues.

Key deliverables include:

- Develop and implement Reliability Assurance Initiative (compliance reform) and all Regions implement RAI techniques and principles consistently.
- Make effective internal controls models and information available to industry.
- Initiate compliance phase-in learning periods for new standards.

b. All ERO compliance activities are risk informed, efficient and effective.

Key deliverables include:

- Develop and implement Reliability Assurance Initiative (compliance reform).

- Monitor registered entities and standards requirements commensurate with the risk to reliability and role of each type of registered entity.

Risks to Reliability

Goal 4. Identify the most significant risks to reliability, be accountable for mitigating reliability risks and promote a culture of reliability excellence. The ERO identifies and prioritizes reliability risks, facilitates effective solutions and interventions, and monitors results. The ERO works with industry stakeholders and experts to ensure the mitigation of known risks to reliability and facilitates a learning environment through event causal analysis, communication of lessons learned, tracking of recommendations, and implementation of best practices.

Objectives and valued outcomes include:

a. Risks are identified and prioritized based on reliability impacts, cost/practicality of assessments, projected resources, and emerging issues.

Key deliverables include:

- Continue RISC's work to develop risk profiles and to include HILF issues.
- Prepare an annual state of reliability report and associated reliability metrics.
- Develop the BPS risk profile to prioritize and rank reliability risks
- Develop project plans and business case assessments for high priority risks; implement or facilitate initiatives to address high priority risks.

b. Events and system performance are consistently analyzed for sequence, cause, and remediation to identify reliability risks and trends, and lessons learned.

Key deliverables include:

- Analyze significant events to identify gaps in standards, compliance effectiveness, registration, and risk controls effectiveness.
- Make all bulk power system event reports available on a timely basis to industry through a secure portal.
- Provide lessons learned and recommendations from events and identified risks.
- Merge event driven databases and cause codes into one (e.g., event analysis, TADS, GADS, relay mis-operations).

c. **ERO supports industry situational awareness, cyber security preparedness and provides independent reliability information to policy makers.**

Key deliverables include:

- Expand security maturity model assessments to be widely accessible across industry.
- Issue and track physical security and cybersecurity recommendations to protect the bulk power system.
- Expand the use and value of physical security and cybersecurity threat and vulnerability information sharing, analytics, and analysis.
- Implement periodic wide area security exercises (e.g., GridEx).
- Increase security clearances available to industry and facilitate access to secured briefings through local fusion centers.

d. **Reliability models and data accurately represent system behavior and are shared among reliability entities.**

Key deliverables include:

- Assess data and modeling needs and develop recommendations to ensure quality planning and operating data/models are available to registered entities across each interconnection.
- Evaluate event disturbances using phasor measurements and other methods to assess sufficiency of data and models.

Coordination and Collaboration

Goal 5. **Improve transparency, consistency, quality and timeliness of results; operate as a collaborative enterprise; and improve efficiencies and cost effectiveness.** The ERO accomplishes this through working with the Regional Entities and registered entities to ensure effective coordination, collaboration and process improvements. The ERO, is an efficient steward of resources, and leverages information systems to create efficiencies and process controls.

Objectives and valued outcomes include:

a. **The ERO acts in a coordinated and collaborative manner with stakeholders.**

Key deliverables include:

- Maintain a list of suggestions and recommendations made by stakeholders (e.g. through policy input) and ERO responses to each.
- Engage the support and expertise of stakeholders in prioritizes and resourcing reliability initiatives.
- Communicate expectations clearly and fosters collaboration to deliver important results in advancing system reliability.
- Develop and implement ERO-wide consensus IT solutions for common touch points with Registered Entities.
- Implement collaborative governance by which ERO and Regions are bound by consensus decisions.
- Clearly delineate ERO and Regional Roles and Responsibilities.

b. The ERO acquires, engages, and retains highly qualified talent suited to the mission.

Key deliverables include:

- Implement employee climate surveys and succession planning and promote favorable hiring and retention of ERO staffs.
- Develop ERO qualifications requirements for auditors and other key positions across the ERO and implement training as needed.

c. The ERO internal risks are understood and managed; ERO processes are effective, efficient, and continuously improved.

Key deliverables include:

- Develop, test and deploy ERO enterprise-wide applications, platform and database.
- Implement an ERO-wide internal risk management program.

ERO Enterprise Performance Metrics

New in 2014, NERC and the Regional Entities are introducing a common set of ERO Enterprise performance metrics. These metrics are intended as indicators of the overall effectiveness of the ERO Enterprise in achieving its mission and the goals and objectives outlined in the ERO Enterprise Strategic Plan, 2014-2017. There are four overarching metrics focused on overall effectiveness in addressing bulk power system risks and improving reliability. There are a number of supporting measures that assess the effectiveness of the key operational elements of the ERO Enterprise.

The intent is to report the results of these metrics on an ERO Enterprise-wide basis, and also as applicable distinguish results for NERC and individual regions. NERC and the Regional Entities are encouraged to further use relevant portions of these measures in their internal corporate performance management programs.

Metric 1: Reliability Results

Measure – Determine the frequency of BPS events, excluding weather[2], flood, or earthquake. The target is fewer, less severe events during 2014-2017; no Category 4 and 5 events and Category 3 events are trending down.

Metric 2: Assurance Effectiveness

Measure – Assess all Category 3 and above events. The target is to reach zero gaps in Reliability Standards and compliance monitoring by 2017.

Metric 3: Risk Mitigation Effectiveness

Measure – Review the BES risk profile each year to determine actual and potential risks. The target is to identify, select and mitigate the high priority risks (and issue specific metrics for each established project).

1. **Changing Resource Mix** - As the generation and load on the power system changes, new vulnerabilities may be exposed that the system was not previously designed to address or respond to. Fundamental operating characteristics and behaviors are no longer a certainty and focused action is needed to address this risk.

[2] Terrestrial weather excluded from metric, however space weather (GMD) is included in metric.

2. **Extreme Physical Events** – Risk mitigation efforts (reducing the potential consequence) are underway, but additional focus is needed to address and minimize both the magnitude and duration of the consequences of an extreme physical event.
3. **Protection System Misoperations** – NERC's 2012 and 2013 State of Reliability Reports identified protection system misoperations as a significant threat to BPS reliability. Additional activities are needed to ensure this risk is managed adequately.
4. **Cold Weather Preparedness** - Lack of generator preparedness for cold weather extremes may result in forced outages, de-ratings, and failures to start. Insufficient availability of intra-regional generation and limits on import transfer capability may result in insufficient generation to serve forecasted load, resulting in load shedding.
5. **Right of Way Clearances** - Transmission Owners and applicable Generation Owners may have established incorrect ratings based on design documents, rather than on the actual facilities built. Managing to stay within SOL and IROL limits that are based on incorrect ratings may be inadequate to prevent equipment damage and/or cascading, instability, or separation.
6. **345kV Breaker Failures** - NERC has identified a potential trend of 345 kV SF6 puffer type breakers failing. Circuit breaker failures, in conjunction with another fault, may lead to more BES Facilities removed from service than required to clear the original fault. This poses a risk to the reliability of the BES.

Metric 4: Program Execution Effectiveness

Measure – Sum of the weighted sub-metrics.

Sub metric A *(Primary NERC)* - Percent of all board-approved standards[3] meet quality criteria and results-based construct[4].

The Standards Committee and NERC Staff will work together to develop a periodic review process for steady state Reliability Standards. The process will include a quality and content review and the use or adaptation of the 2013 Independent Expert Review Team's quality and content scoring system will be considered during development. The review will be conducted by a cross-functional task force that will consist of Committee chairs, NERC management, NERC and stakeholder subject matter experts, and other parties as deemed necessary and appropriate. This review may also be incorporated into the current Standards Processes Manual periodic review process to avoid duplication of effort. So that the task force will be able to identify Reliability Standards for inclusion in the 2016-2018 Reliability Standards Development Plan, the task force will be operational no later than mid-2015 to allow ample time for the development of the annual task force review timeline.

[3] Regional standards are not included, this applies to NERC only.
[4] Based on Independent Expert Review Team scoring method 3 out of 3 on content and at least 10 out of 12 on quality.

Sub metric B *(Primary NERC)* - Quality, up-to-date Reliability Standard Audit Worksheets, or any successor guidance, developed for board-approved Reliability Standards.

2014 = Every standard that goes to ballot will have a posted RSAW alongside. Every standard that is reviewed as part of the 5 year review cycle will have a current up-to-date RSAW or successor.

2015 = All RSAWs are converted to the new format and are available to industry.

2016 – 2017 = Violations for new standards do not occur at rates higher than the average rate for standards (or for which they replace) and repeat violations for standards is trending down.

Sub metric C *(Joint ERO Enterprise)* – Implementation of risk-based registration criteria to achieve efficient and effective allocation of compliance obligations. Registration is commensurate with risk and RAI and in light of new BES definition implementation.

2014 = Assessment complete with recommended framework and registration criteria. Implementation plan following assessment, criteria and framework completed.

2015 = Business processes / tools

2016 = Implementation launch

2017 = Stable state

Sub metric D *(Joint ERO Enterprise)* – Timeliness and transparency of compliance results: 12 month rolling average of the ERO Enterprise caseload index trending favorably.[5] Maximum age of unclosed cases is less than 24 months and improving.

2014 = ERO Enterprise caseload index less than or equal to 7 months, with all Regional Entities above average trending downward. ERO Enterprise average violation aging less than or equal to 13.5 months.

2015 = ERO Enterprise caseload index of 8 months, with all Regional Entities above average trending downward. ERO Enterprise average violation aging less than or equal to 13 months.

2016 = ERO Enterprise caseload index of 8 months, with all Regional Entities above average trending downward. ERO Enterprise average violation aging less than or equal to 12.5 months.

[5] ERO Enterprise Caseload Index is defined as Violations in ERO Inventory (defined as Active violations that have not been filed with FERC) divided by the total number of violations filed with FERC over previous 12-months (NOPs, SNOPs, FFTs and Dismissals) multiplied by 12.

2017 = ERO Enterprise caseload index of 8 months. ERO Enterprise average violation aging less than or equal to 12 months.

Sub metric E *(Joint ERO Enterprise)* - Percent of self-identified non-compliances (includes self-reports and self-certifications).

2014 = 70%

2015 = 74%

2016 = 78%

2017 = 80%

Sub metric F *(Joint ERO Enterprise)* - Mitigation aging curve improving[6].

2014 = Percentage of the noncompliance items discovered in that year that are mitigated as of December 31, 2014)

- 2013: 80%
- 2012: 95%
- 2011: 98%
- 2010 (and older): 100%

2015 - 2017 = Mitigation aging curve trending favorably.

Sub metric G *(Joint ERO Enterprise)* - RAI reforms and percent of total findings (excluding dismissals) not going to enforcement or filed with FFT or spreadsheet.

2014 =

- ERO auditor handbook deployment;
- RAI compliance reform design complete and reflected in the CMEP implementation plan for 2015;
- Enforcement pilots completed and FERC filings made, if required;
- Train at least two partnering entities to complete maturity model assessments and complete either directly or through trained partners 20 maturity model assessments;
- At least 75% of noncompliance posing a minimal or moderate risk to the BPS is processed through discretion (i.e.: does not trigger an enforcement action), FFT or SNOP;
- Average time from discovery to posting FFT is 6 months;

[6] Final metrics to be discussed and approved at the February 2014 BOTCC meeting.

- Average time from discovery to decision to enforce or not (i.e.: the triage process) is 60 days.

2015 = Higher percentage of lower and moderate risk violations staying in compliance through exercise of discretion to initiate an enforcement action; audit scope based on common ERO methodology.

2016 = Compliance and enforcement end state designs implemented; continued increase in lower and moderate risk violations staying in compliance through exercise of discretion to initiate an enforcement action.

2017 = Achieve fewer, less severe violations. Positive trend in number of matters dispensed outside of enforcement.

Sub metric H *(Primary NERC)* - Participation in ES-ISAC increased (2013 statistics used as baseline)

2014 =

- 90% of all RCs and TO/TOPs;
- 10% increase in enrollment of all other registered entities;
- 20% increase in information share activity on portal (baseline 2013 uploads figures).
- Develop an ES-ISAC mission performance program, including Key Performance Indicators (KPIs) and benchmarks, by end of Q3.

2015 - 2017 = KPIs trending favorably.

Sub metric I *(Joint ERO Enterprise)* – Assessment of quality and availability of planning and engineering models and data.

2014 = Methodology to validate models developed and endorsed by appropriate technical committees.

2015 = Acquire data and capability for set up / start up.

2016 = Assessment of state and quality of modeling. Establish plan to implement assessment recommendations.

2017 = Implement plan.

Sub metric J *(Joint ERO Enterprise)* – Achieving transition laid out in oversight model regarding ERO Enterprise personnel and ERO Enterprise (NERC and Regional Entity) infrastructure and applications qualifications.

2014= Report quarterly progress and achieve 25% completion of action items.

2015= Report quarterly progress and achieve 50% completion of action items.

2016= Report quarterly progress and achieve 75% completion of action items.

2017= Report quarterly progress and achieve 100% completion of action items.

Sub metric K *(Joint ERO Enterprise)* –Stakeholder annual satisfaction/perception survey of the ERO's effectiveness to manage risk, budget and stewardship.

2014 = Develop questionnaire with stakeholder input and vetting. Survey complete and benchmarks established.

2015 – 2017 = Performance trending favorably.

ERO Enterprise Strategic Plan, 2014-2017

Goal 5: Improve transparency, consistency, quality, and timeliness of results; operate as a collaborative enterprise; and improve efficiencies and cost-effectiveness.

5a - The ERO acts in a coordinated and collaborative manner with stakeholders.

- Maintain a list of suggestions and recommendations made by stakeholders (e.g., through policy input) and ERO responses to each.

Strategic and Business Planning Input

Entity / Stakeholder (Date)	Stakeholder Comment (Abridged version)	Action/Response and Notes
CEA (Jan 2014)	Goal 4: Determine if there can be a deliverable to identify and develop a suite of tools to address reliability issues (as alternatives to standards).	Under consideration by NERC management and referred to RISC and standing committees for input.
	Goal 5: Recognize the obligations to all applicable governmental authorities and modify to indicate "all applicable authorities".	Agreed. Processes are in place to coordinate with both US and Canadian government authorities.
EEI (Jan 2014)	Include a strategic internal management goal with clear accountability of goals and objectives, deliverables and meaningful metrics.	Already in place with integration of NERC metrics to NERC performance management system.
	Map existing program area plans and processes to strategic plan. Specifically, how NERC's plan complements or conflicts with the standards development work plan or the RISC's proposal to address reliability issues.	NERC's priorities for the standards review process are addressed on an ongoing basis and reflected in the Reliability Standards Development Plan developed in collaboration with the Standards Committee. RISC coordination is ongoing in 2014 and will be reflected in plans for 2015.
	Align various metrics with goals and deliverables. • Set clear and measurable metrics for regulatory outreach and advocacy.	Regulatory outreach and advocacy are embedded in our normal work processes and aligned with key initiatives. Consideration to specific metrics for this area will be given for future years.
SM-TDUs (Jan 2014)	Define measures by which the Regional Entities and NERC will evaluate entity risk (as part of RAI).	Will be addressed in the ongoing implementation and development of RAI.
NRECA (Jan 2014)	Recommend replacing BPS with BES throughout the plan	Adopted. NERC updated the Board approved (Feb 6) Strategic Plan replacing BPS throughout.
	Goal 1: Include the SC role and focus on retiring standards and requirements that are not needed to support BES reliability.	The Standards Committee's role in the standards review process will be addressed as part of developing the long term quality review process.
	Goal 2: Include deliverable to add a deregistration process for currently registered entities that have a change. Also add a deliverable that requires development of a single document/resource that describes RAI.	Adopted. NERC updated the Board approved (Feb 6) Strategic Plan adding deregistration.
	Goal 4: Add SC responsibilities.	Standards Committee's responsibilities in the standards development process will be addressed on an ongoing basis.
EPSA (Jan 2014)	Combine metric 1 and 2. These metrics seem interrelated as to not represent two different metrics to score and evaluate.	Not adopted. Metric 1 measures the effectiveness of the ERO Enterprise to influence reliability overall as measured by the frequency and severity of events. Metric 2 focuses on conducting analysis of severe events to assess

		whether there are gaps in reliability standards as currently in force or compliance monitoring on the part on the ERO. Both metrics are focused on accountability of the ERO Enterprise to influence reliability and reduce the occurrence of severe events.
ELCON (Jan 2014)	Encourage specific metrics to allow the measurement of: • Maintain a list of suggestions made by stakeholders and ERO responses • Engage expertise of stakeholders in reliability initiatives • Implement collaborative governance (ERO and Regions) bound by consensus	• This list addresses first bullet. • Not appropriate for a "metric", but we agree conceptually. • Not appropriate for a "metric", but that governance exists in the form of the ERO EMG, which is comprised of the CEOs of all nine entities.
Standards Committee, Brian Murphy (Jan 2014)	Goal 1: Revise to align with the RSDP and SC's work plan (refer to policy input attachment)	Adopted.
NPCC (Jan 2014)	Recommends the implementation of the registration framework and criteria be advanced to 2015 to better align with the implementation of the BES definition.	To be considered during the registration initiative project and will be reflected in the development of the 2015 BP&B if time permits.
SERC (Jan 2014)	Encourages ERO Enterprise to conduct a clean slate review of the strategic plan's content with a particular focus beyond the current 3 year horizon.	To be discussed with ERO EMG.
MRC BP&B Input Group (Jan 2014)	Add important MRC meeting and conference call dates to BP&B schedule.	NERC staff updated BP&B schedule prior to the Jan 30 Finance and Audit Committee meeting to reflect this input.
EEI (Jan 2014)	Describe/ address budget and cost management, coordination among the core operational areas and duplicative activities among the Regions. • Consider cost-benefit analysis, similar to Standards, to help inform decision-making and determine priorities for limited resources.	To be considered by NERC management in the development of the 2015 BP&B.
Sector 4 (Jan 2014)	Consider cost impacts to industry. There are mounting pressures to manage costs and minimize rate impacts to customers. NERC must ensure resources are spent appropriately.	To be considered by NERC management in the development of the 2015 BP&B.
ELCON (Jan 2014)	Specific "IT solution" benefits to Registered Entities should be quantified through cost savings in dollars. Strongly encourages restraint in the amount that will be proposed and recommends keeping the amount level if not reduced.	To be considered by NERC management in the development of the 2015 BP&B.
NPCC (Jan 2014)	Identify "benefits" associated with standards to provide more information surrounding standards' costs vs. benefits.	Efforts are underway to consider cost benefit in the standards development process.

Texas RE (Jan 2014)	Requests there be additional clarity and transparency regarding amounts that the Regional Entities will be expected to expend to support specific enterprise efforts. • If particular ERO-level projects are required the amounts should be identified and incorporated into the Regional Entities' budgets.	Addressed through the coordination and development of the NERC and Regional Entities BP&Bs.
SERC (Jan 2014)	Resource needs and budgets should reflect the stable nature of the enterprise. Effectiveness parameters, including cost, should be established for ERO activities.	Addressed through the coordination and development of the NERC and Regional Entities BP&Bs.
RISC (Jan 2014)	Encourages the inclusion of more explicit focus on reliability risk management and RISC's priority recommendations in the BP&B.	RISC intends to produce its next recommendations in February 2015 for the 2016 BP&B.

Other Input - Related to ERO Enterprise Activities and Priorities

Entity / Stakeholder (Date)	Stakeholder Comment (Abridged version)	Action/Response and Notes
CEA (Jan 2014)	Requests that NERC present # of new or modified standards to NERC BOT for approval.	Addressed in the standards development plan.
	Examine where efficiencies can be gained and where resources can be better focused on core reliability priorities. • Focus on registration criteria for PSEs.	The registration initiative will address criteria for entities such as PSEs. Efficiency opportunities will be addressed through the coordination and development of the NERC and Regional Entities BP&Bs.
EEI (Jan 2014)	Fully implement the RAI before the implementation date of CIP v5, ensure the completion of regional pilots by mid-2014, and address compliance process issues and expectations for entities operating in multiple regions.	RAI compliance pilots are complete and the enforcement pilots will be complete in April. RAI final compliance design will be complete in Q3 2014. Integration with CIP v5 implementation is being planned.
SM-TDUs (Jan 2014)	Afford RAI as the highest priority since it is relied upon in standards development.	RAI is one of the highest priorities this year.
NRECA (Jan 2014)	Consider the challenges of too many initiatives in play at any one time and focus on doing less, better.	Agree conceptually and will continue to work with stakeholders to pace initiatives.
	Develop a revised Statement Compliance Registry Criteria (SCRC) and other needed ROP modifications for BOT approval at its November 2014 meeting. • Develop a project plan with timelines and milestones.	Will be taken under consideration as part of the registration initiative this year.
IRC ISO/RTO (Jan 2014)	Consider developing a structured approach and metrics for exploring and applying alternative approaches to standards • Work with the RISC on an approach that expands on the suite of tools.	Under consideration by NERC management and referred to RISC and standing committees for input.
ELCON (Jan 2014)	Risk-based approach is not fully defined yet and needs to be encoded in priorities such as enforcement principles related to CIP v5 requirements.	RAI implementation will take into consideration, including the CIP v5 implementation.
NPCC (Jan 2014)	Recommends prioritization be given to the development of a secure portal to enable confidential sharing of post-event report.	The portal is in place as is the process for vetting and gaining permission from entities.

	Limit any risk project related to resource adequacy assessments of the reliability impacts of planned resource capacity and projected reserve margins.	That is the intent of that RISC identified project. Resource adequacy was not selected as a major 2014 risk project for the ERO Enterprise. Will be considered in future updates to the risk projects.
MRO (Jan 2014)	Continue risk-based work in the RAI and incorporate risk based concepts across all programs. The work being done in the RAI and through the implementation of the BES definition addresses how risk is to be considered in scoping the ERO's work.	Agreed.
SERC (Jan 2014)	Encourages further coordination of processes and timelines for "feeder" activities which are significant inputs into the business planning processes (RISC, LTRA, etc.).	Will be addressed in ongoing improvement to BP&B process between NERC and the Regional Entities.

Agenda Item 14.a
Board of Trustees Meeting
May 7, 2014

Operating Committee
Board of Trustees Report

Action
Information

Background

I. Operating Committee's (OC) Major Accomplishments for 2014 (Year-to-date)

1. Reliability Guidelines – The OC is currently addressing two reliability guidelines.
   a. In March 2013, the OC approved the *Reliability Guideline: Generating Unit Winter Weather Readiness – Current Industry Practices*. This guideline provides a general framework for developing an effective winter weather readiness program for generating units throughout North America. The focus is on maintaining individual unit reliability and preventing future cold weather related events. At its March 2014 meeting the OC reviewed the impacts to the BES of the Polar Vortex weather phenomenon. As a result of this review, the OC tasked its Event Analysis Subcommittee with conducting a review of the Generating Unit Winter Weather Readiness reliability guideline.
   b. In December 2013, the OC approved the posting for a 45-day comment period the draft *Reliability Guideline: Generating Unit Operations During Complete Loss of Communications*. Comments were due by February 28, 2014 and are currently being reviewed by the Resources Subcommittee. The proposed guideline provides a strategy for power plant operations in the case of complete loss of communications (both data and voice) between the on-site generating unit(s) operator and the System Operator for the Balancing Area, Transmission Operator (TOP) and Reliability Coordinator (RC).
2. MISO Reliability Plan – During the OC's June 20, 2013 meeting, it was reported that an Operations Reliability Coordination Agreement (ORCA) had been reached with Associated Electric Cooperative, Louisville Gas and Electric, Kentucky Utilities, PowerSouth Energy Cooperative, Southern Companies, Southwest Power Pool and Tennessee Valley Authority. Given this agreement, the parties recommended that the OC approve the revised MISO reliability plan. The ORCA provides a long term road map for coordination and study between the parties to ensure reliability in the consolidated MISO Balancing Authority Area that stretches from the gulf coast through the middle of the United States to the U.S. - Canadian border. The OC continues to receive status reports from MISO as the provisions in the ORCA are addressed in accordance with its approval of the reliability plan.

3. NERCnet (ISN) – NERC is in the process of transitioning NERCnet to the Eastern Interconnection Data Sharing Network, Inc. (EIDSN). The EIDSN is a consortium of reliability coordinators in the Eastern Interconnection that has been formed to manage the current NERCnet. In addition, the EIDSN intends to issue a Request for Proposals for a replacement network in the third quarter of 2014.

4. Independent Experts Review of the Reliability Standards – The OC engaged in a discussion of the reliability gaps (outage coordination, generator frequency response, and EMS real time contingency analysis models) identified by the in the independent experts in their report. The OC is developing a response for submittal to the Standards Committee and the Reliability Issues Steering Committee.

5. Essential Reliability Services Task Force (ERSTF) – The OC approved the scoping document for the ERSTF. The scoping document provides that essential reliability services (ERS), in addition to capacity and energy characteristics, must be maintained across a given system to ensure reliable operation. Inertia, frequency response, and voltage control are key ERS. Analysis may determine that other characteristics or functions could be included within the suite of ERS.

II. OC's Major Initiatives for 2014

1. OC Realignment of Activities and Organization – Following the approval of the OC's strategic plan, the committee will, throughout 2014, focus on the realignment and reprioritization of the work of its subgroups. In collaboration with its subcommittees and working groups, the OC will identify and implement opportunities for increased efficiency and use of stakeholder's resources.

2. Event Analysis Subcommittee (EAS) – Following an excellent start-up in 2012, the OC and the EAS continue to work jointly with the NERC Events Analysis (EA) program to further enhance the EA process and to enhance the identification and publication of lessons learned and event reports. In addition, the NERC EA program is beginning to develop and analyze event related metrics to identify trends, reliability gaps, and opportunities for industry improvement.

3. Annual State of Reliability Report – The OC's Event Analysis Subcommittee will partner with the Planning Committee's Performance Analysis Subcommittee to review and develop the 2014 State of Reliability report.

III. March 2014 Meeting Summary:

The following is a summary of the OC's March 2014 meeting, which highlights the latest activities of the OC and its associated subcommittees in support of the NERC or OC mission and corporate goals. The March 2014 OC Meeting Minutes are posted on the NERC website.

1. Reliability Issues Steering Committee (RISC) – On behalf of the RISC, Andy Rodriquez of NERC briefed the OC on the development of the Reliability Risk Management Process and the ERO Top Priority Reliability Risks 2014 – 2017, which identify what the RISC perceives as the most significant reliability concerns for the period 2014-2017.

2. Eastern Interconnection Frequency Initiative – The Resources Subcommittee briefed the OC on an Eastern Interconnection initiative to improve the Eastern Interconnection frequency response. The current initiative focuses on the existing generator fleet with respect to the completeness and accuracy of the data provided in the 2010 NERC generator survey and improving their frequency response capabilities. Following a brief discussion, the OC approved a motion to support the Resources Subcommittee's Eastern Interconnection Frequency Initiative and to encourage participation by Eastern Interconnection balancing authorities and generator operators and owners.

3. Planning Committee's Performance Analysis Subcommittee – Melinda Montgomery, chair of the Performance Analysis Subcommittee (PAS), reviewed proposed revisions to the ALR1-4 (BPS Transmission Related Events Resulting in Loss of Load) metric. The OC endorsed the proposed revision to ALR1-4 and a proposed revision to the Severity Risk Index whitepaper.

4. Polar Vortex Weather Phenomenon – Representatives from ERCOT, FirstEnergy, MISO, South Carolina Electric and Gas, and TVA briefed the OC on the impacts of the polar vortex weather phenomenon on the Bulk Electric System within their respective service areas. A particular concern of the industry was fuel availability during cold weather extremes, particularly the availability of natural gas when competing usage for heating diminishes its supply for generation. The OC will further investigate the current status and future plans for the gas-electric coordination initiatives at its June meeting. The OC tasked its EAS to consolidate all of the lessons learned associated with cold weather operations and distribute them to the OC for review. In addition, the OC charged the EAS to benchmark the OC's Generating Unit Winter Weather Readiness reliability guideline using the 2013/2014 cold weather phenomenon and recommend any improvements at the June 2014 OC meeting. This will in turn enhance the Fall 2014 cold weather preparedness webinar.

5. Eastern Interconnection Data Sharing Network (R. Mandes) – Mr. Mandes discussed the transition of the ISN (formerly NERCnet) to the industry in a secure manner to ensure the continued reliability and redundancy of the tool. The new network is expected to be in service during the first quarter of 2015.

6. Independent Experts Report – The Standards Committee asked the OC to review the Outage Coordination, Generator Governor Frequency Response and RTCA Models (Situational Awareness) gaps outlined in the Independent Experts report and associated draft Authority Standard. During the discussion it became clear that the Independent Experts needed to be involved in the discussion to answer questions and provide their perspective. The OC authorized its Executive Committee (EC) to meet with the Independent Experts and develop a response for use by the Standards Committee and RISC. Following the OCEC-Independent Experts webinar, the OC developed an opinion for each of the three gaps, as requested, and reviewed and provided an opinion for each requirement in the draft Authority Standard.

7. Essential Reliability Services Task Force – Mr. Moura summarized the scope of the Essential Reliability Services Task Force (ERSTF) as a joint OC and Planning Committee

effort to identify critical system reliability products such as inertia, frequency response and voltage control which must be maintained to continue reliable BPS operation as the resource mix changes. He estimated that the effort would require approximately 18 months to fulfill its mission. To provide effective operational input and avoid replication of efforts by the Operating and Planning Committees, the OC appointed a small core of operational representatives with an operational chair who will also serve as the Co-Chair of the Task Force. The OC approved the scope and structure of the ERSTF as presented.

Agenda Item 14.b
Board of Trustees
May 7, 2014

Planning Committee Status Update

Action
None

Status Update
In support of the NERC Planning Committee's (PC) long-term vision, significant tasks have been undertaken in 2013 to support the electric reliability organization's (ERO's) overall reliability mission. These tasks have laid the foundation for the projects being conducted in 2014. Along with the committee's development of a strategic plan and its annually produced reliability assessments, the NERC PC is actively engaged in a number of areas which are important to maintain the reliability of the Bulk-Power system (BPS) of North America.

First Quarter Status Report
The PC has observed significant improvements in the quality of material being submitted to the committee. The following items have been incorporated into the PC's regular course of business and tactical objectives:

- The PC executive team formed a reliability risk team to manage Reliability Issues Steering Committee (RISC) deliverables.
- Regional status reports are now requested at each meeting to get regional perspectives on emerging issues and progress on regional initiatives

Planning Committee's Major Initiatives for 2014

- **2014 Reliability Assessment Reports** – The PC expects to submit three annual assessment reports to the NERC Board of Trustees for their consideration: (1) the *2014 Long-Term Reliability Assessment*, (2) the *2014 Summer Reliability Assessment*, and (3) the *2014/2015 Winter Reliability Assessment*.
- ***2014 State of Reliability Report*** – The *State of Reliability Report* provides NERC's independent view of ongoing BPS trends to objectively analyze the state of reliability based on metric information and provide an integrated view of reliability performance. The report will provide an industry reference for historical BPS reliability as well as analytical insights toward industry action and will enable the discovery and prioritization of specific risk control steps.
- **Geomagnetic Disturbance Task Force (GMDTF)** – The GMDTF is primarily focused on the development of the Phase I and II Reliability Standards and providing technical guidance to the standards drafting team. The GMDTF is also developing a pilot assessment to better understand the planning approaches that will be used in Phase II of the GMD Reliability Standards.

- **Support of Standards Development** – The PC continues to support the NERC Standards Development process. In particular, subcommittees of the PC conduct essential technical research into current and proposed areas of reliability issues to either highlight on-going issues or improve the industry's body of knowledge relating to system planning and reliable operation of the bulk power system. This research is used to inform standards development.

  The PC is also engaged with the Standards Committee (SC) on technical discussions regarding the BPS reliability impacts of the demand response and distributed resources—highlighted as emerging long-term reliability challenges in numerous NERC assessments.

- **Completion of the Integration of Variable Generation Task Force (IVGTF) Work Plan** – In response to the NERC *2009 Summary Report on Accommodating High-Levels of Variable Generation*, the IVGTF is working to address the recommendations through a series of 12 efforts on specific issues such as wind forecasting, distributed variable resources, and capacity contributions of variable generation. A final report is expected in mid-2014 and will be the culmination of this task force's work to address the reliability challenges of integrating large amounts of variable generation.

- **"Essential Reliability Services" Task Force** – The PC (and Operating Committee) has formed a task force as a follow-on action to the recommendations from the *2013 Long-Term Reliability Assessment*. The task force will focus on expanding NERC's methodology for reliability assessment. The new approach may include the development of metrics for further evaluation in future long-term reliability assessments and supplement the existing resource adequacy measures. The task force will also develop a technical reference document on essential reliability services, which include frequency response, inertia, voltage stability, ramping capability, and other operational requirements needed to ensure BPS reliability. A technical reference for regulators and policy makers is needed to inform, educate, and build awareness on the reliability ramifications of a changing resource mix.

- **Coordination with the Reliability Issues Steering Committee (RISC)** – The PC continues to support RISC efforts and provide technical guidance for risk identification, develop gap analyses, and prioritize focus areas. The PC will specifically provide guidance on modeling and data concerns that should be considered as "high-risk" gaps as well as other risk areas detailed in the *State of Reliability Report* and *Long-Term Reliability Assessment*. The PC has focused its efforts on two key risk areas (titles of risk areas may be adjusted):

  - Adaptation and Planning for Change
  - Operational Modeling and Model Inputs

Future Meetings

The PC future meetings are scheduled as follows:

- June 10-11, 2014 – Orlando, FL
- September 16-17, 2014 – Vancouver, BC
- December 9-10, 2014 – Atlanta, GA

Agenda Item 14.c
Board of Trustees Meeting
May 7, 2014

Critical Infrastructure Protection Committee (CIPC) Report

Action
Information

Summary
GridEx II Distributed Play Report
The CIPC Executive Committee (EC) reviewed the recommendations from the GridEx II Distributed Play Report and issued assignments to the following CIPC working groups and task forces:

- Control System Security Working Group (CSSWG)
- Electricity Sub-sector Information Sharing Task Force (ESISTF)
- Security Training Working Group (STWG)
- Business Continuity Guideline Task Force (BCGTF)

March CIPC Meeting Highlights
CIPC Technical Workshop – In conjunction with the March CIPC meeting, a workshop was held in which NERC staff presented an overview of the technical differences between the currently enforceable Critical Infrastructure Protection (CIP) Version 3 NERC Reliability Standards and the recently approved CIP Version 5.

Elections – Mr. David Revill was elected to serve on the CIPC EC, filling the position recently vacated by Mr. Carl Eng.

Physical Security Workshop
At the June CIPC meeting, a Physical Security Workshop will offer a featuring state-of-the-art physical security technology that is currently being used by BC Hydro at its substations.

- Advanced Laser Detection System for substation protection. There will be a demonstration of how BC Hydro views the use of this technology, and Mr. Arik Garber, Senior Security Advisor at BC Hydro, will answer questions.

Future Meetings
The future meetings of the CIPC are scheduled as follows:

- June 10-11, 2014 – Orlando, FL
- September 16-17, 2014 – Vancouver, BC
- September 17-18, 2014 – Vancouver, BC – CIPC EC Planning Meeting

Personnel Certification Governance Committee
Board of Trustees Update Report

Action
Information

Background
This report highlights the key activities of the Personnel Certification Governance Committee (PCGC) during the first quarter 2014. The PCGC meets four times per year. Task force meetings are held as needed. The first quarter 2014 meeting minutes are under review and pending approval. Draft minutes were posted to the NERC website during first quarter in 2014.

Policy Oversight
The System Operator Certification (SOC) Program Manual was updated to reflect the new test center vendor, as well as the vendor's scheduling and cancellation policy. No additional changes were made to the SOC Program Manual. The revised program manual will be posted during second quarter of 2014. No changes were made to any other program document.

Quarterly Metrics
There are several metrics tracked by the NERC Personnel Certification group that are used to evaluate the efficacy of the SOC program. Following is an overview of key metrics for the first quarter 2014.

SOC Exam Development
The SOC Exam Development Metric (Figure 1) is used to track the development of SOC exams during the 36 month development cycle. During each development cycle, the Exam Development and Delivery TaskForce works with the Exam Working Group (EWG) and the Psychometric Consulting and Test Delivery vendor to ensure the exams are timely developed and delivered. As the metric below demonstrates, the PCGC is currently on track to deliver the next set of SOC exams by January 1, 2015.

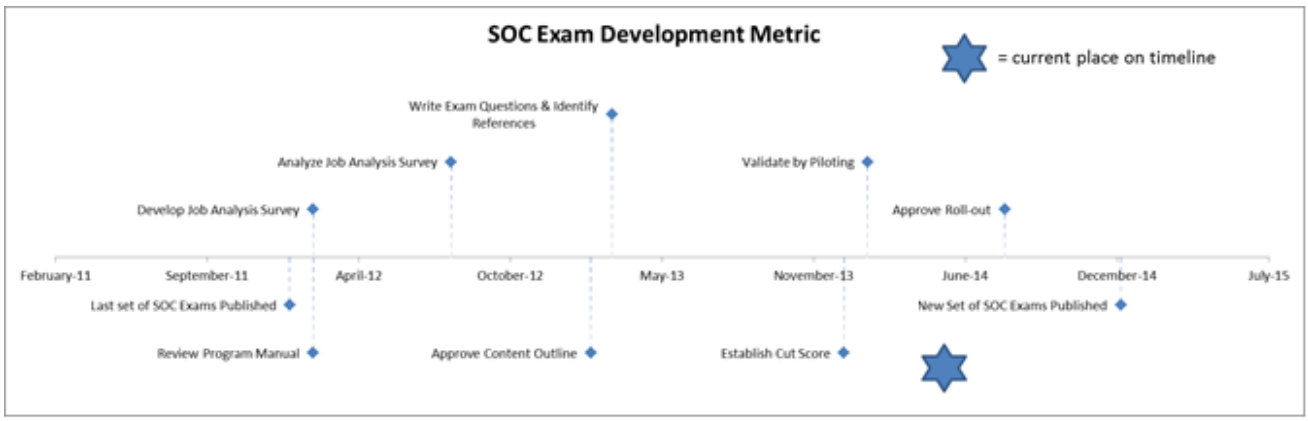


Figure 1: SOC Exam Development Timeline

System Operator Certification and Continuing Education Database (SOCCED) Availability Metric

The SOCCED Availability Metric is used to track the availability of the SOCCED Database. The metric reports the percentage of time both the website and SQL server, used to support the database, are available. As the metric below demonstrates, both the website and SQL server were available 100% during the first quarter of 2014.

Objective	Goal	Actual	Timeframe
Website Availability	99%	100%	1st Quarter 2014
SQL Server Availability	99%	100%	1st Quarter 2014

SOC Examination Pass Rate

The SOC Exam Pass Rate Metric is used to track the pass rate of the SOC exam for the period 2010-2014. Figure 2 compares the number of exams taken to the number of exams passed and Figure 3 compares the current year-to-date breakdown of exams based on the type of System Operator credential.

There are four Certified System Operator exams:

- RC: Reliability Coordinator
- BT: Balancing, Interchange, and Transmission
- BI: Balancing and Interchange
- TO: Transmission Operator

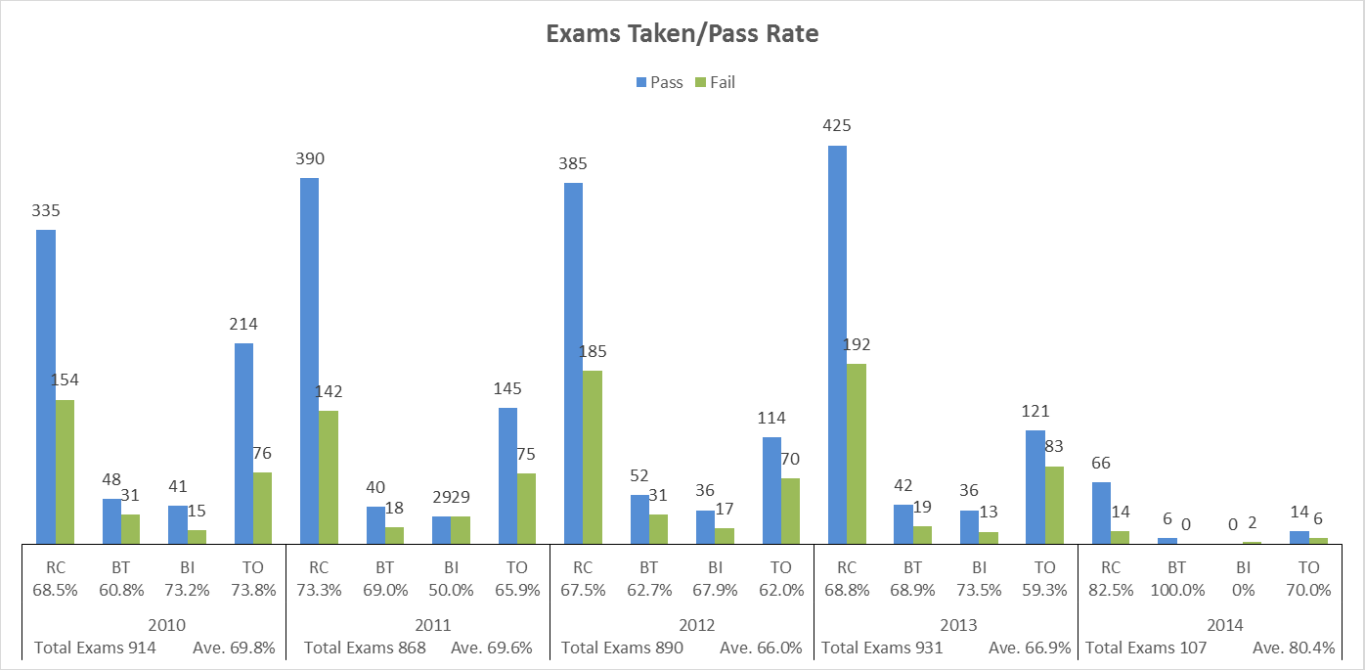


Figure 2: SOC Exam Pass Rate by Exam 2010-2014

The average overall pass rate for all exams for 2010 – 2013 is 68%. In January 2014, the exams were transitioned to a new vendor and no exams were given during the transition period. Due to the lag in exams because of the transition period, the data set for first quarter 2014 does not reflect the historical overall pass rate. As more data points are captured in 2014 and a pass rate is identified, the pass rate is expected to be average and remain in the mid to high 60th percentile. Although first quarter numbers are lower than expected, the projection for new exams taken in 2014 is 900 (Figure 6).

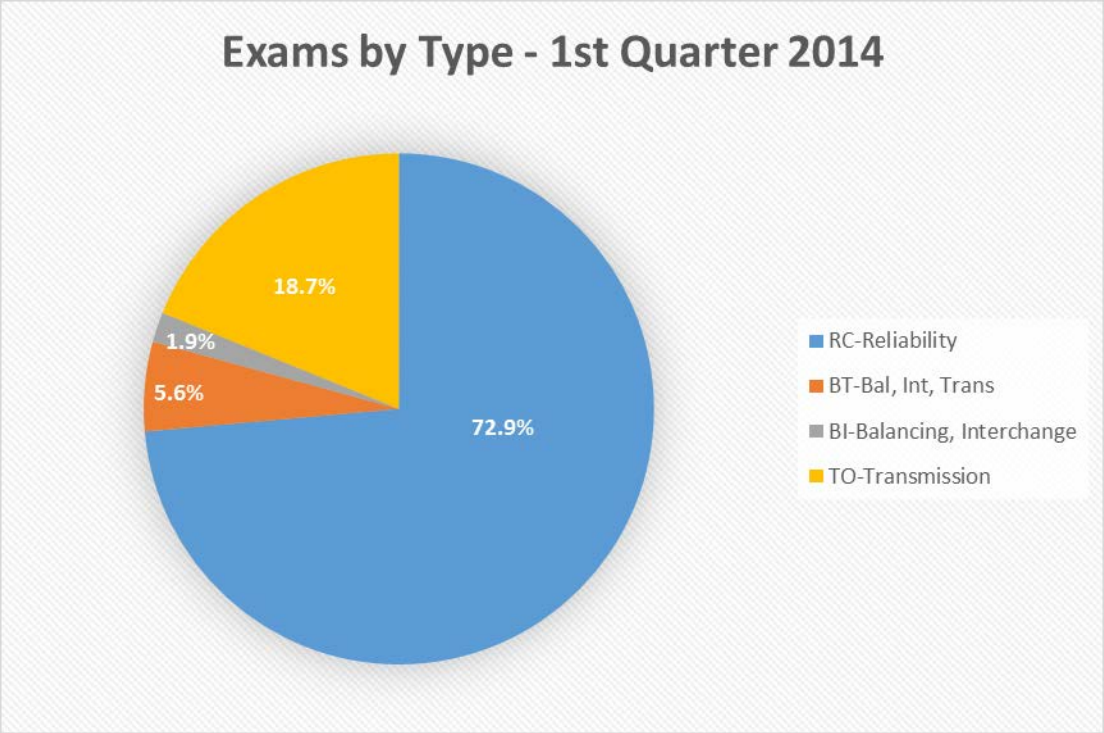


Figure 3: Exams Taken by Type – 1st Quarter 2014

Traditionally, the RC exam is taken more than the other System Operator exams because the RC credential gives the system operator more flexibility in potential jobs. Also, the RC credential is attractive to support functions within the utility industry such Planners and EMS Engineers.

Active Credentials

The Active Credentials Metric details the number of active certificates per credential from 2011 through current YTD (over a four year rolling average). Some operators hold multiple credentials.

Count of Certificate Status Credential Name	2011	2012	2013	2014	Total	Rolling Four Year Avg
Balancing and Interchange	124	100	133	18	**375**	**94**
Balancing, Interchange and Transmission	252	217	267	54	**790**	**197**
Transmission	352	310	445	68	**1175**	**294**
Reliability	1573	1285	1762	270	**4890**	**1223**
Total	**2301**	**1912**	**2607**	**410**	**7230**	

SOC Program Budget

Under Section 602.4.10 of the NERC Rules of Procedure, the PCGC shall have control over the matters related to the Personnel Certification and re-Certification Programs, without being

subject to approval by any other body. Section 602.4.10 further states that financial matters related to the operation of the program shall be segregated from other NERC activities.

The Program Budget Metric tracks the SOC Program budget. While the financials for the SOC Program were not available in time for publication of this report, the YTD-2013 Funding – Actual vs. Budget (Figure 4) details the revenue received from SOC Exams taken and SOC Certifications renewed as compared to the budget allocated for these items. Both, the number of exams taken and the number of credential renewals were higher than projected for 2013; therefore, the Actual funding is greater than the Budgeted funding.

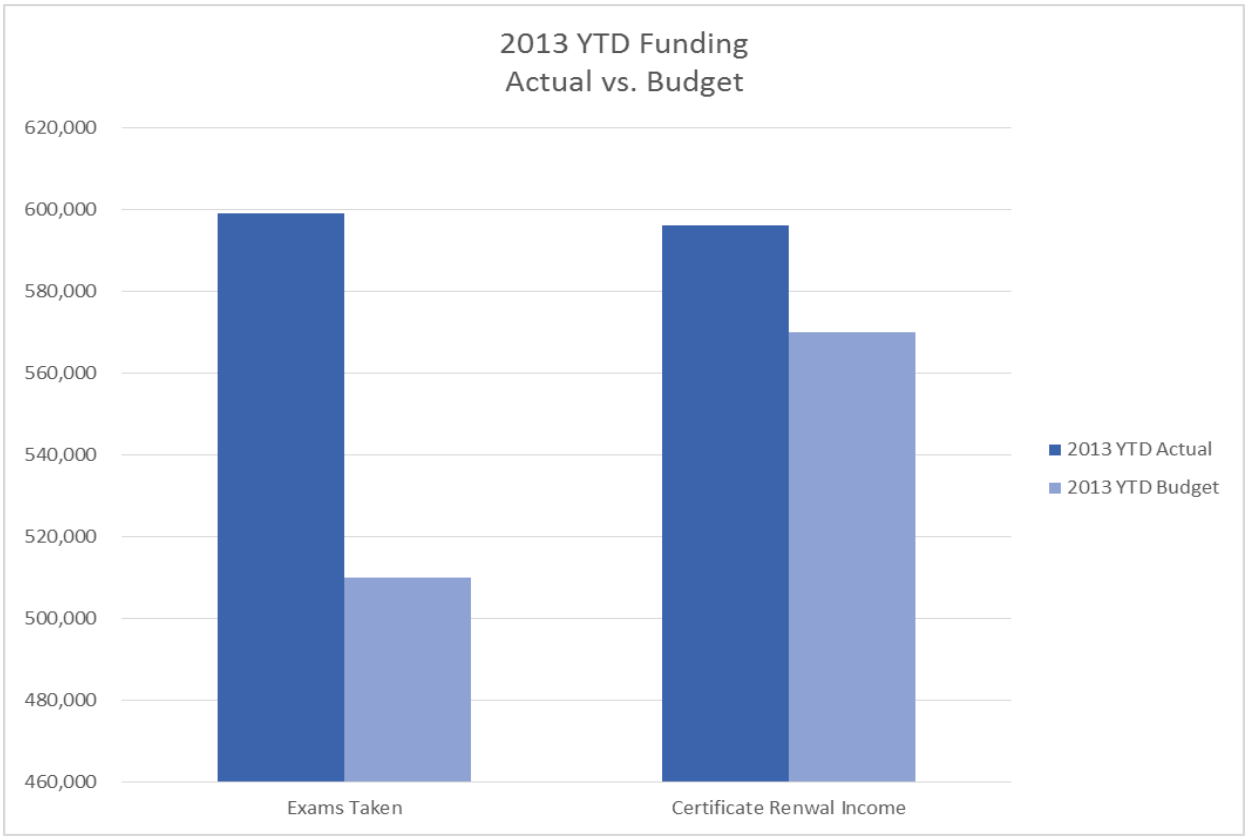


Figure 4: PCGC 2013 YTD Funding

The YTD-2013 Expenses – Actual vs. Budget depicted in Figure 5 details the expenses of operating the program in comparison to the budget from the service providers used to administer the program.

In the AMP column which depicts the Actual vs. Budget expenses (Figure 5) for the vendor AMP, the difference between the actual versus budgeted expenses is the result of a cancelled Item Writing Workshop which was budgeted in 2013 but never occurred.

In the Prometric column which depicts the Actual vs. Budget expenses (Figure 5) for the vendor Prometric, the difference is due to the decrease in exam fees. The number of exams taken was higher than projected for 2013.
In the MCG column which depicts the Actual vs. Budget expenses (Figure 5) for the vendor MCG, the difference includes costs for the SOCCED Upgrade Plan. The Upgrade costs are not directly reflected in the PCGC "fixed costs" budget, rather they are covered under the PCGC Capital Fund.

In the PSI column which depicts the Actual vs. Budget expenses (Figure 5) for the vendor PSI, the difference is the result of preliminary work for the transition to the new test center vendor in 2013.

In the Meeting + Office Costs column which depicts the Actual vs. Budget expenses (Figure 5), the difference includes PayPal fees which increase due to the exams taken and renewals processed in 2013.

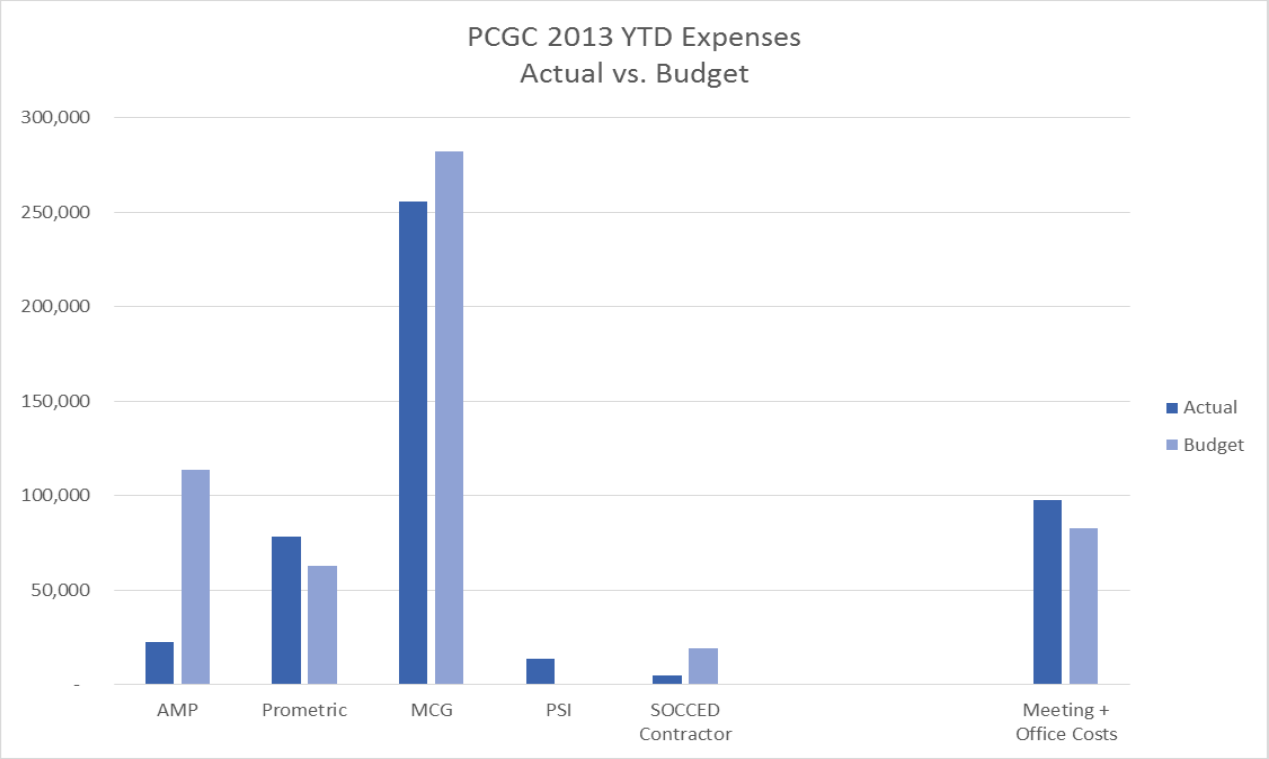


Figure 5: PCGC 2013 YTD Expenses

Figure 6 and Figure 7 detail the Exams Taken and Renewals (2012-YTD2014) which can affect the Actual vs. Budget for revenue.

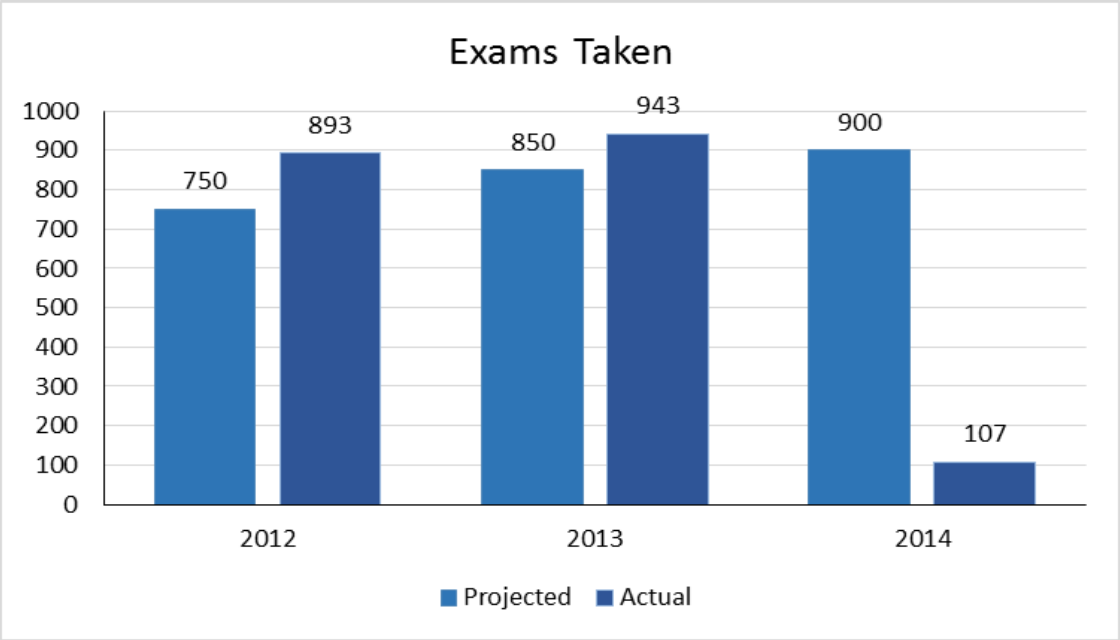


Figure 6: Exams Taken Projected vs. Actual

A reduction in exam fees resulted in a significant increase in exams taken in 2013. In October 2013, a new vendor was selected for the test centers. The exams were transitioned to the new vendor during the month of January. No exams were given during the transition period resulting in the low number for first quarter of 2014.

System operators may renew their credentials as much as six months in advance. The fee for credential renewal was reduced in 2013. System operators who were able to delay their credential renewal waited for the fee reduction date of January 1, 2013.

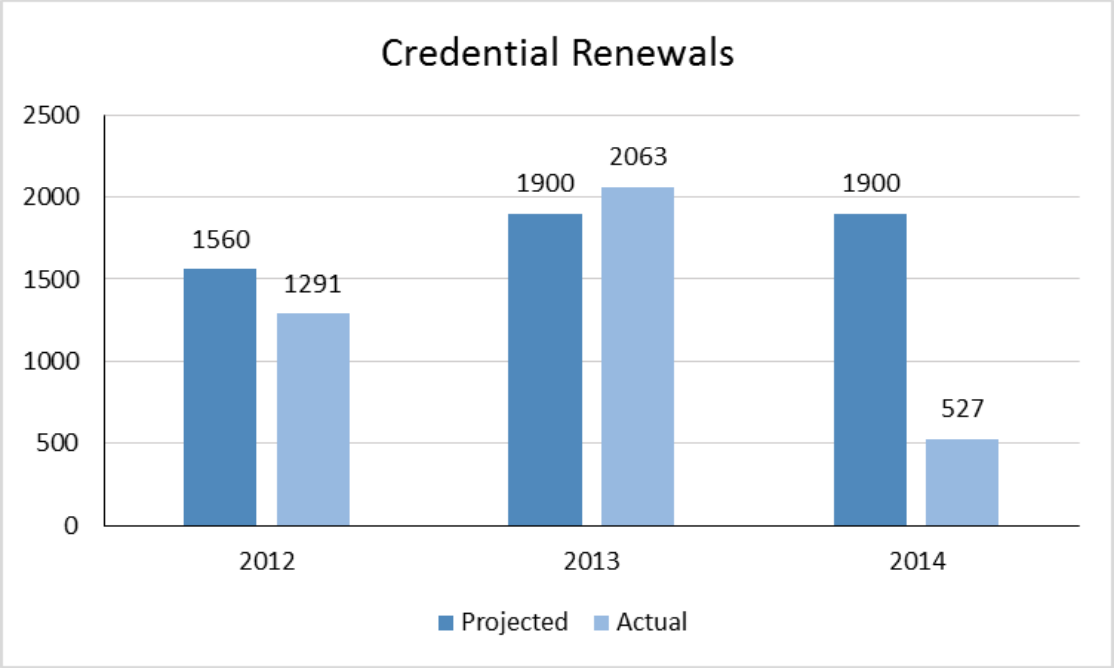


Figure 7: Credential Renewals Projected vs. Actual

Accomplishments

Successfully transitioned from two vendors into one vendor for test centers and exam development services which allow faster testing of sample questions and reduce the exam development cycle.

Future Tasks

- An Item Writing Workshop will be held May 8-9, 2014 in St. Louis, MO.
- Members of the PCGC, Personnel Subcommittee, EWG and industry experts have been invited to participate in creating items for the upcoming 2015 exams. Items are analyzed and evaluated by the psychometric vendor before they are transitioned into exam questions.
- Standing task forces have been created to deliver on each of the metrics included in this report. Each task force meets, outside of the quarterly meetings, as needed to address issues within their scope.

Standards Committee Report

Action
Information

Project 2014-04 Physical Security Waivers
The Standards Committee (SC) approved the waiver of several Standards Process Manual (SPM) provisions on a March 21, 2014 committee call. The waivers were necessary due to a recent Federal Energy Regulatory Commission (FERC) order that provided 90 days to complete the project on developing Physical Security standard(s). The motion on the waivers, as approved by the SC, is as follows:

> Approve the following waiver of provisions of the SPM for the Physical Security Reliability Standard(s) Project:
>
> 1. Standard Authorization Request to be posted for a seven-calendar day informal comment period. (Sections 4.1-4.2)
> 2. Initial formal comment and ballot period reduced from 45 days to 15 calendar days, with a ballot conducted during the last five days of the comment period. Form ballot pool beginning immediately upon approval of this waiver with closure of the ballot pool 10 days after the initial formal comment and ballot period begins. (Sections 4.7-4.9)
> 3. Additional formal comment and ballot period(s) reduced from 45 days to 10 calendar days, with ballot conducted during the last five days of the comment period. (Sections 4.9 and 4.12)
> 4. Final ballot reduced from 10 days to five calendar days. (Section 4.9)

A signed letter, from the SC Chair, Brian Murphy, was sent via e-mail on March 31, 2014, to Ken Peterson, chair of the Standards Oversight and Technology Committee (SOTC), notifying the SOTC of the waivers.

Goals and Metrics SC Endorsement
At a March 12-13, 2014 meeting, the SC endorsed a Standards Metric to be included in the proposed Electric Reliability Organization Enterprise Strategic Plan (ERO SP). The SC also endorsed the implementation of the 2016 and 2017 metric and the effort to develop a periodic review approach for 2016 and beyond. The team conducting the periodic review development has committed to present to the SC, by the end of the second quarter of 2014, the draft approaches to be presented for industry comment. The final periodic review approach is expected to be presented to the NERC Board of Trustees by the end of the first quarter in 2015.

Project Tracking Spreadsheet

The **project tracking spreadsheet** for standards has been enhanced to include prioritization in the 2014-2016 RSDP. It was also updated to depict whether the project is directionally consistent with Independent Expert Review Panel findings.

SC agendas and meeting minutes are posted at: [**Standards Committee**]

Agenda Item 14.g
Board of Trustees Meeting
May 7, 2014

Reliability Issues Steering Committee (RISC) Report

Action

Information, Approve

Background

The Reliability Issues Steering Committee (RISC) is an advisory committee that reports directly to the NERC Board of Trustees (the Board), and assists the Board, NERC standing committees, NERC staff, regulators, Regional Entities, and industry stakeholders in establishing a common understanding of the scope, priority, and goals for the development of solutions to address risks to the Bulk Electric System (BES). To carry out its responsibility to provide a framework for steering, developing, formalizing and organizing recommendations to help NERC and the industry effectively focus resources on addressing critical issues to improve the reliability of the bulk power system, the RISC presented an initial report to the Board in February 2013. The report provided a prioritization of reliability risk areas, categorizing each area as High, Medium, or Low priority. Specific analytical steps were recommended for assessing each risk area, and thoughts regarding the allocation of resources were offered. An update to the report was presented to the Board in August 2013. The RISC has also been working closely with NERC staff to develop an ERO business planning process that incorporates the work products of the RISC into a broad, risk-informed strategy for maintaining reliability around which staff and committees can align their work efforts.

Bob Schaffeld, chair of the RISC, will provide an update on the status of the group. Additionally, the Board is being asked to take the following actions:

1. Approve an amended Charter for the RISC, and
2. Approve term extensions for four members of the RISC, and
3. Approve a slate of new members to the RISC.

Charter Revisions

The MRC conducted a review of the RISC Charter in 2013, and offered no changes or adjustments at its August 14 meeting in Montreal. At the time, it was determined that there were no pressing issues needing resolution that had to be addressed immediately. However, members of the RISC have identified a number of opportunities for improvement within the Charter. Similarly, NERC's legal department has suggested that conforming the RISC charter to the general style and content of the charters of NERC' other committees is advisable. Accordingly, the members of the RISC have, working with NERC's legal department, developed a revised charter that is intended to ensure consistency with the original Standards Process Input Group (SPIG) recommendations, transfer the charter into the common NERC template, and streamline the charter to improve efficiency. This streamlining includes:

- Moving a number of "process/how" elements out of the charter for inclusion in a "Member Handbook," currently in development. The charter has been refocused to emphasize the "scope/what" of the RISC, leaving the details of implementation out of the charter to allow more flexibility in the RISC undertaking its work.
- Clarifying the process for the recommendation and appointment of committee-based, MRC and At-Large members to the RISC.
- Removing the MRC obligation to review the charter every three years. To the extent such review is needed (by the MRC or any other group), that review should be undertaken as needed, rather than on a periodic schedule.

Term Extensions

As documented in the RISC charter, terms of the MRC and At-Large members are to be staggered to ensure continuity (*i.e.*, roughly half the terms should end in odd years, while the other half should end in even years). In addition to the Standing Committee members, the RISC was initially comprised of four MRC members and five At-Large members. All began serving their terms at the same time, and all terms are coming to a close. Several members (Sylvain Clermont, Peter Flynn, Chris Schwab, Brian Silverstein, and Mike Smith) have left the RISC through retirement, career change, or resignation. A recommendation for new members to replace these members follows; however, the terms of the remaining four members of the RISC are still scheduled to expire. Rather than establish the RISC with a complete slate of all new MRC and At-Large members, it is requested that the Board extend the remaining member's terms to ensure continuity as was envisioned by the original staggering requirement. Further, it is recommended that continuity in leadership be effected through the additional extension of the RISC chair's term. Proposed extensions to achieve this are requested as follows:

- MRC representative Scott Helyer, through May 2015
- MRC representative Jason Marshall, through May 2015
- At-Large member and RISC chair Bob Schaffeld, through May 2016
- MRC representative John Twitty, through May 2015

New Members

As described above, a number of RISC members have left through retirement, career change, or resignation. Pursuant to the RISC charter, a RISC nominating committee was formed comprised of Sylvain Clermont, vice-chair of the MRC; Ken Peterson, chair of the Standards Oversight and Technology Committee (SOTC); Bob Schaffeld, chair of the RISC; and Gerry Cauley, president and CEO of NERC. Chaired by Mr. Clermont, this committee reviewed a number of candidates and evaluated them based on general experience and qualifications, as well as diversity within the context of the entire membership of the RISC. Six of the following candidates were selected, and, pending endorsement by the MRC at its May 6, 2014 meeting, the Board is being requested to approve their appointment to the RISC for terms of two years, ending in May 2016. A seventh candidate, Terry Bilke, was separately advanced by the Compliance and Certification Committee (CCC) to replace the current CCC representative, Clay Smith, whose participation on the CCC is

coming to a close. The Board is also being requested to approve Mr. Bilke's appointment. A complete list of candidates recommended for membership on the RISC is as follows:

Name	Title and Company
Daniel Froetscher, At-Large Member	Senior Vice President, Transmission, Distribution, and Customers, Arizona Public Service Company
Ray Gorman, At-Large Member	Chairman, New Brunswick Energy and Utilities Board
Scot Hathaway, At-Large Member	Vice President – Transmission, Dominion Virginia Power
Duane Highley, At-Large Member	President and CEO, Arkansas Electric Cooperative
Nabil Hitti, MRC Member	Vice President, Transmission Network Operations, National Grid
Steve Whitley, At-Large Member	President and CEO, New York ISO
Terry Bilke, CCC Representative	Consulting Advisor, Compliance Services, Midcontinent ISO

Agenda Item 14.g.i

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Issues Steering Committee Charter

Approved by NERC's Board of Trustees
May 7, 2014 (PENDING)

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Table of Contents 2

RISC Charter 3

Section 1. Purpose 3

Section 2. Reporting 3

Section 3. Overview and Functions 3

Section 4. Membership 3

Section 5. Officers 4

Section 6. Meetings 4

RISC Charter

Section 1. Purpose

The Reliability Issues Steering Committee (RISC or Committee) is an advisory committee that triages and provides front-end, high-level leadership for issues of strategic importance to bulk power system (BPS) reliability and offers high-level stakeholder leadership engagement and input on issues that impact bulk-power system reliability. The RISC advises the North American Electric Reliability Corporation (NERC) Board of Trustees (Board), NERC standing committees, NERC staff, regulators, Regional Entities, and industry stakeholders to establish a common understanding of the scope, priority, and goals for the development of solutions to address these issues, including the use of solutions other than the development of new or revised reliability standards. In doing so, the RISC provides a framework for steering, developing, formalizing, and organizing recommendations to help NERC and the industry effectively focus their resources on the critical issues needed to best improve the reliability of the BPS.

Section 2. Reporting

The RISC reports directly to the Board. The Board shall approve this Charter and any amendments to this Charter pursuant to Section 1300 of the NERC Rules of Procedure.

Section 3. Overview and Functions

The RISC performs two primary functions for the Board.

The first function of the RISC is evaluating bulk power system reliability issues and risks. The RISC provides strategic leadership and advice to the NERC Board of Trustees and others to triage key reliability risks and propose solutions to manage those risks.

Second, the RISC provides an annual analysis of risks to the bulk power system, and produces a relative prioritization of the risks. The prioritization is designed to advise:

- annual ERO action planning, resource allocation, budgeting and strategic planning processes; and
- standing committee planning, including the development of the Reliability Standards Development Plan.

In addition, the RISC performs such other functions that may, from time to time, be delegated or assigned by the Board.

Section 4. Membership

The RISC shall be comprised of the following allocation of members:

a. **At least six (6)** stakeholder-based— four (4) from the MRC and at least two (2) At-Large members (not members of the MRC);

b. **Five (5)** committee-based—one (1) from each of the standing committees: Standards (SC), Operating (OC), Planning (PC), Critical Infrastructure Protection (CIPC), and Compliance and Certification (CCC). The Board will be responsible for appointing the committee-based members to the RISC. These members will be the chair or vice chair unless otherwise recommended by the standing committee and be subject to NERC Board approval.

In advance of the annual May Board meeting, a RISC Nominating Committee (RISCNC) chaired by the MRC vice-chair will be formed to solicit a pool of candidates, with the goal of meeting the following general criteria:

a. Geographic and International diversity, including international, such that Eastern, Western, and Texas Interconnections, along with Canada are represented on the RISC;

b. Sector, size, and asset (transmission, distribution, load, generation, etc.) diversity;

c. High-level understanding and perspective on reliability risks;

d. Experience in a leadership role or background in an executive-level position is strongly preferred; and

e. Balanced consideration of these criteria, across the entire membership of the RISC.

The Board is responsible for appointing the committee-based, MRC and At Large members to the RISC. At the May Board meeting each year (or as needed), the RISCNC shall present to the Board a recommended slate of all RISC member candidates as appropriate for consideration and approval. All MRC and At-Large members will be appointed by the Board to serve for two-year terms. Membership terms will be staggered to ensure continuity.

Section 5. Officers

1. **Selection of the Chair.** The Board shall appoint a chair of the RISC to serve a two-year term and direct the activities of the RISC, and work toward reaching consensus on all recommendations and actions.

2. **Selection and Duties of the Secretary.** NERC will appoint one senior staff person to serve as a secretary with the responsibility to:

    a. Prepare, distribute and post notices of Committee meetings, record meeting proceedings, and prepare, distribute and post meeting minutes.

    b. Maintain a record of all Committee proceedings, including responses, and correspondence.

    c. Maintain Committee membership records.

Section 6. Meetings

1. **Open Meetings.** Meetings shall occur at least once every quarter and can be in person or by conference call as determined by the chair. All meetings of the RISC will be open to all interested parties (except as noted in the paragraph below for confidential sessions). Only members may act on items before the Committee. Meeting notices shall be publicly posted on the NERC website on the same day they are distributed to Committee members. Final minutes of Committee meetings shall be publicly posted on the NERC website. Notices shall describe the purpose of meetings and shall identify a readily available source for further information about the meeting.

2. **General Requirements.** The Committee shall hold meetings as needed and may use conference calls or email to conduct its business.

3. **Notice.** The RISC secretary shall announce its regularly scheduled meetings with a written notice (letter or e-mail) to all Committee members not less than ten and no more than sixty calendar days prior to the date of the meeting.

4. **Agenda.** The RISC secretary shall provide an agenda with a written notice (letter, facsimile, or e-mail) for Committee meetings no less than five business days before a proposed meeting.

    a. The agenda shall include, as necessary, background material for agenda items requiring a decision. The agenda shall be posted on the NERC website the same day it is distributed to Committee members.

    b. Items not in the agenda that require a decision cannot be added at a meeting without the consensus of the members present. If such a matter comes up, it may also be deferred to the next meeting so that Committee members have time to consult with others.

5. **Quorum.** The quorum necessary for the transaction of business (*i.e.*, formal actions) at meetings of the committee is a majority of the members currently on the committee roster (*i.e.,* not including vacancies). The committee may engage in discussions without a quorum present.
6. **Proxies.** Proxies are not permitted.
7. **Observers.** Non-members may observe RISC meetings, either in person or via conference call.
8. **Confidential Sessions.** The chair of the RISC may limit attendance at a meeting or portion of a meeting, based on confidentiality of the information to be disclosed at the meeting. Such limitations will be applied sparingly and on a nondiscriminatory basis as needed to protect critical energy infrastructure information and other information that is sensitive to one or more parties.

Agenda Item 14.h
Board of Trustees Meeting
May 7, 2014

Compliance and Certification Committee

Action

Approve the Compliance and Certification Committee (CCC) 2014 Annual Work Plan.

Accept the 2013 Stakeholder Perception Survey results and report recommendations, and the CCC recommendation to extend the period between surveys to 18 months.

Background

The CCC is providing its Annual Work Plan for 2014 for approval, as well as the final report from the 2013 Stakeholder Perception Survey to the Board of Trustees (Board).

Annual Work Plan

The CCC approved its 2014 Annual Work Plan in December. Subsequently, NERC staff requested changes to the plan. The primary change is the addition of an executive summary as well as a listing of the major project areas, activities, and deliverables on which the CCC will focus. The attached work plan reflects input and comments from NERC senior management.

2013 Stakeholder Perception Survey

In the third quarter of 2013, consistent with its 2013 Annual Plan, the NERC CCC conducted its fifth annual survey measuring stakeholder perceptions on the policies, practices and effectiveness of NERC and Regional Entities with respect to the Compliance program, Registration program, and Certification program.[1] This survey is an essential element of the CCC's responsibilities under its Board-approved Charter.

The survey was sent to 1,201 individuals on the NERC Primary Compliance Contact roster. The survey received responses from 352 individuals, a response rate of 29.3 percent. As compared with 2012, there was a nearly 3 percent increase in the response rating. 5 of the 6 survey areas showed improvement over 2012.

See attachment for the full "ERO Effectiveness and Stakeholder Perceptions Survey Report," dated April 2013.

---

[1] The recommendations made in the report are tied to the following themes: (i) Return on Investment (ROI) of the compliance program, (ii) inconsistencies within and across Regions, and (iii) transparency of the enforcement and penalty processes. With regard to the subject of ROI, NERC staff continues to believe that "ROI" is not an appropriate focus or framework in the context of compliance programs. Work to streamline compliance monitoring and enforcement, and to reduce unnecessary compliance burdens is on-going. NERC is committed to continuing these efforts.

The CCC is also recommending extending the period between surveys to 18 months.

Other Highlights

- Held CCC meeting at NERC's Atlanta offices on March 11-12, 2014. The focus of the meeting was on Reliability Assurance Initiative-related topics.
- Subject to Board approval, the CCC will have new leadership in July 2014.
- The CCC is working with Mechelle Ferguson Thomas, NERC's Director of Internal Audit and Corporate Risk Management, on plans for an independent audit of NERC, scheduled in July of 2014. The CCC is assisting with the development of audit criteria, which will cover the handling of the Standards Process and standards applicable to NERC.
- The CCC's Organization Registration and Certification Subcommittee (ORCS) is actively supporting NERC's Risk-Based Registration initiative.

Upcoming Items

- Work with NERC staff on revisions to CCC procedures to reflect the CCC's involvement with the Board's Enterprise-wide Risk Management Committee.
- The next CCC meeting will be June 4-5, at FPL offices in Juno Beach, FL.

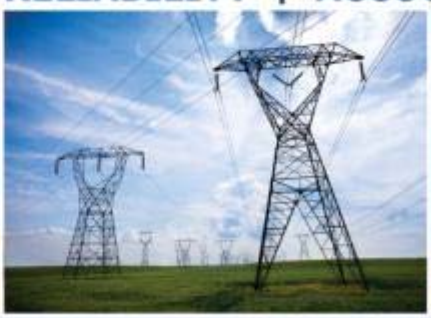
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda Item 14.h.i

NERC Compliance and Certification Committee 2014 Work Plan

April 2014

RELIABILITY | ACCOUNTABILITY



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Summary

The North American Electric Reliability Corporation (NERC) Compliance and Certification Committee (CCC) is a NERC Board of Trustees (Board)-appointed stakeholder committee serving and reporting directly to the Board. The CCC is responsible for engaging with, supporting, and advising the Board and NERC regarding all facets of the NERC Compliance Monitoring and Enforcement Program (CMEP), Organization Registration Program (Registration program), and Organization Certification Program (Certification program). The CCC is also responsible for monitoring NERC's adherence to the Reliability Standards development process and those standards applicable to NERC. In order to support this endeavor, the CCC has developed this annual work plan to identify the activities that the CCC intends to perform in 2014 to fulfill the responsibilities the Board has established for the CCC.

Revision History:

Date	Version Number	Comments
09/25/2013	1.0	Initial Draft
10/25/2013	1.1	CCC Balloted Version
11/08/2013	1.1	Approved by CCC
02/21/2014	1.2	Revised to include NERC Staff input and additional CCC Ballot
02/27/2014	1.2	Approved by CCC

Table of Contents

Summary 2
Revision History 2
Table of Contents 3
Executive Summary 5
Oversight and Deliverables 6
Introduction 10
CCC Organization 11
Organization Registration and Certification Subcommittee (ORCS) 11
Standards Interface Subcommittee (SIS) and Procedures Subcommittee (PROCS) Consolidation to Form Compliance Processes and Procedures Subcommittee (CPPS) 11
ERO Monitoring Subcommittee (EROMS) 12
CCC Nominating Subcommittee 12
Key Responsibilities Not Assigned to Subcommittees 12
Hearing/Mediation Responsibilities 14
Meetings (2014) 15
NERC Board of Trustee Assignments 16
APPENDIX A - CCC Projects/Subcommittee Activities 17
Global CCC Projects/Activities 17
ORCS Activities 17
EROMS Activities (See Appendix B for Monitoring Plan) 17
CPPS (SIS/PROCS) Activities 18
Reliability Assurance Initiative (RAI) Support Teams 18
APPENDIX B - 2014 CCC Monitoring Plan 20
Stakeholder Perceptions Survey 20
NERC Self-Certifications 20
Enterprise-wide Risk Committee (EWRC) 20
Detailed Overview of Monitoring Activities 21
Self-Certifications 21
Audits /Reviews 21
Spot-Checks 22
NERC Audits of Regional Entities 22
Monitoring Stakeholder Perceptions 22
Appendix C - CCC Programs 24
CCCPP-001: Monitoring Program for NERC's Adherence to NERC's ROP 24
CCCPP-002: Compliance Monitoring Program for Reliability Standards Applicable to NERC 24
CCCPP-003: Monitoring Program for NERC's Standards Processes Manual 24

CCCPP-007: Monitoring Program for NERC's Adherence to NERC's ROP for Organization Registration and Certification 24
CCCPP-008: Program for Monitoring Stakeholders' Perceptions of NERC Compliance Program, Registration Program, and Certification Program 24
CCCPP-010: Criteria for Annual Regional Entity Program Evaluation. 24
Appendix D - Logistics and Budget Requirements for CCC Activities 25
CCC Quarterly Meetings 25
Hearings and Appeals 25
Mediation 25
CCC Program Audits/Review 25
WebEx/Conference Calls 25
Stakeholder Perception Survey 25
Training 25

Executive Summary

The purpose of this work plan is to identify the anticipated activities and deliverables of the CCC for the year 2014 and beyond. The plan is based on the responsibilities assigned to the CCC by the Board through programs and tasks identified by the CCC that are required to fulfill these responsibilities. Additionally, the CCC identified projects and deliverables that will further support the goals of the ERO Strategic Plan 2014-2017.

There are four main project areas CCC activities will center on:

1. **Core Function of CCC Oversight of ERO**: As a committee providing support and advice, but otherwise independent of the execution of NERC CMEP, Registration program, and Certification program , and consistent with prior Federal Energy Regulatory Commission (FERC) Orders, the CCC will monitor NERC's compliance with the Rules of Procedure (ROP) for these programs on an ongoing basis. In a similar manner, as a committee independent of the NERC Reliability Standards development process, the CCC will monitor NERC's compliance with the ROP regarding the NERC Reliability Standards development process.
2. **NERC's Risk-based Registration project**: Provide input and support into the design of NERC's risk-based registration development. The CCC will assist in identifying modifications to the Statement of Compliance Registry Criteria and associated changes to the NERC ROP.
3. **ERO's Reliability Assurance Initiative (RAI):** Participate and support RAI activities. The CCC will assist in the transition of compliance monitoring and enforcement processes that are risk-informed, efficient and effective.
4. **Multi-region registered entity process:** Perform outreach and support activities for ongoing NERC multi-region registered entity processes and enhancements.

The CCC has subcommittees performing certain assigned tasks on behalf of and under the supervision of the CCC. The CCC will use these subcommittees, along with NERC and Regional Entity staff, as the primary resource for project and activities. The subcommittees include:

- Organization Registration and Certification Subcommittee (ORCS)
- Standards Interface Subcommittee (SIS) and Procedures Subcommittee (PROCS), pending consolidation to form Compliance Processes and Procedures Subcommittee (CPPS)
- ERO Monitoring Subcommittee (EROMS)
- CCC Nominating Subcommittee

Oversight and Deliverables

Project Area: Core Function of CCC Oversight of ERO-Monitoring Plan			
As a committee providing support and advice, but otherwise independent of the execution of NERC CMEP, Registration program, and Certification program , and consistent with prior FERC Orders, the CCC will monitor NERC's compliance with the ROP for these programs on an ongoing basis. In a similar manner, as a committee independent of the NERC Reliability Standards development process, the CCC will monitor NERC's compliance with the ROP regarding the NERC Reliability Standards development process.			
Project Name	**Activities**	**Schedule**	**Resource(s)**
1. Stakeholder Perceptions Survey	• Conduct and prepare a summary report for the Board • Include lessons learned from the 2013 survey • Continue to refine the question and survey instrument	1st and 2nd Quarters 2014	EROMS, TalentQuest, and Jerry Hedrick (NERC)
2. Independent Audit of Standards Applicable to NERC and the Standards Process Manual	• Develop criteria for audit • Provide subject matter experts to act as observers for audit • Review and accept audit report • Monitor mitigation of any non-conformance audit findings	2nd and 3rd Quarters 2014	EROMS, CCC, Mechelle Thomas (NERC), and independent audit firm
3. NERC Self-Certifications	• Develop self-certification forms and request NERC to self-certify adherence with the ROP for the Compliance Monitoring and Enforcement Program (CMEP) and Organization Registration and Certification Programs (ORCP) • Prepare a summary report of the results of the submitted NERC Self-Certifications for the Board	3rd and 4th Quarters 2014	EROMS, CMMS, and Mechelle Thomas
4. Enterprise-wide Risk Committee (EWRC) 2015 Work-Plan	• Provide input as requested by the EWRC	As requested	CCC Chair and Vice Chair, Mechelle Thomas (NERC), and EWRC

Project Area: Risk-based registration research and project support			
Applicable ERO 2014-2017 Strategic Goal No. 2a: Compliance, Registration and Certification-The ERO registers entities commensurate with risk to the bulk power system and ensures all key reliability entities are certified to have essential capabilities. Coordination and Collaboration (Goal No. 5) – Improve transparency, consistency, quality, and timeliness of results; operate as a collaborative enterprise; and improve efficiencies and cost-effectiveness.			
Project Name	**Activities**	**Schedule**	**Resource(s)**
5. Registration Steering Group	• Participation and support	Ongoing	CCC/ORCS representative
6. Risk-Based Registration Survey	• Develop questions • Analysis of responses	1st and 2nd Quarters 2014	ORCS, CCC, Mark Lauby (NERC), Rebecca Michael (NERC), and Earl Shockley (NERC)
7. Risk-Based Registration White-Paper	• Support and input on whitepaper outline • Support and input on final whitepaper product	2nd and 3rd Quarters 2014	ORCS, CCC, Mark Lauby (NERC), Rebecca Michael (NERC), and Earl Shockley (NERC)
8. Risk-Based Registration Design and Implementation	• Participation and support • Participate in roll-out as requested	4th Quarter 2014	ORCS, CCC, Mark Lauby (NERC), Rebecca Michael (NERC), and Earl Shockley (NERC)

Project Area: Reliability Assurance Initiative			
Applicable ERO 2014-2017 Strategic Goal No. 3a and 3b: Compliance, Registration and Certification- Industry has effective procedures and programs to monitor, detect, correct, report, and prevent compliance, reliability, and security issues. All ERO compliance activities are risk informed, efficient and effective.			
9. Internal Controls-Question and Answer Document	• Update the QA document upon completion of pilots and in response to stakeholder requests	Ongoing and 3rd and 4th Quarters 2014	CCC, CPPS, and Jim Armstrong (NERC)
10. Internal Controls Guide	• Update the document upon completion of pilots • Continue collecting examples of Internal Controls for inclusion in guide	Ongoing and 3rd and 4th Quarters 2014	CCC, CPPS, Tobias Whitney (NERC)
11. RAI Data Retention and Sampling	• Support team responsible for developing the whitepaper based on survey results ▪ Share with NERC RAI leadership (May 2014) ▪ Post paper for public comment (June 2014) ▪ Make changes based on comments (June 2014)	1st – 4th Quarters 2014	CCC, CPPS, and Ed Kichline (NERC)

	• Support communications of potential ROP changes resulting from team results Draft supporting documents (e.g. process bulletin, audit handbook supplement)		
12. Communication Tools Redesign (RSAWs)	• Update previously provided recommendations upon review and input from NERC and Standards Committee. Four initial areas of suggested improvement: ▪ RSAW Structure ▪ RSAW Use ▪ RSAW Development ▪ Internal Controls application • Support communications on RSAW processes and content development ▪ Provide technical reviews where needed	Ongoing	CCC, CPPS, and Matthew Gibbons (NERC)
13. Update criteria for assessing effectiveness of Regional Entity CMEP programs	• After consultation with NERC, update CCCPP-010 to incorporate criteria that appropriately reflects expected program improvements resulting from RAI	4th Quarter (based on input from relevant NERC personnel on progress of RAI projects, either complete initial updating or begin updating)	CPPS, CCC and Jerry Hedrick (NERC)
14. Aggregation of Minimal Issues Pilot Program	• CPPS to provide advisory input to NERC on conclusions drawn from pilot, as pilot will lead to program redesign and possible ROP changes	TBD-NERC	CPPS and Sonia Mendonca

Project Area: Multi-region registered entity process			
Applicable ERO 2014-2017 Strategic Goal No. 2a: Compliance, Registration and Certification - The ERO registers entities commensurate with risk to the bulk power system and ensures all key reliability entities are certified to have essential capabilities. Coordination and Collaboration (Goal 5) – Improve transparency, consistency, quality, and timeliness of results; operate as a collaborative enterprise; and improve efficiencies and cost-effectiveness.			
Project Name	**Activities**	**Schedule**	**Resource(s)**
15. Multi-Region Registered Entity Process	• Perform outreach efforts with stakeholders to determine continued need for this process or to assist with isolation of issues requiring resolution • Determine if guidance documents require adjustment for the current processes or identified areas requiring resolution	2nd - 4th Quarters 2014	ORCS, Mark Lauby and Earl Shockley (NERC)

Introduction

In the capacity of a NERC Board-appointed stakeholder committee serving and reporting directly to the NERC Board under a NERC Board-approved charter,[1] and as approved by FERC[2] and as set forth in NERC's ROP, the CCC will engage with, support, and advise the NERC Board and NERC Board of Trustees Compliance Committee (BOTCC) regarding all facets of the NERC CMEP, Registration program, and Certification program. As a committee providing support and advice, but otherwise independent of the execution of these programs, and consistent with prior FERC Orders, the CCC will monitor NERC's compliance with the ROP for these programs on an ongoing basis. In a similar manner, as a committee independent of the NERC Reliability Standards development process, the CCC will monitor NERC's compliance with the ROP regarding the NERC Reliability Standards development process.

The CCC provides for balanced discussion, commentary, and recommendations on compliance issues by bringing together a wide diversity of opinions and perspectives from NERC member sectors. Members are appointed to the CCC by the NERC Board and serve on the committee at the pleasure of the Board.

Individuals deemed qualified to serve on the committee will generally include senior level industry experts who have particular familiarity, knowledge, and experience in the areas of compliance, compliance enforcement, compliance administration and management, organization responsibilities and registration, organization certification, and NERC and Regional standards.

These individuals are normally involved with internal compliance programs within their respective organizations. Committee members are expected to represent the interests of the sector they represent, to the best of their ability and judgment.

[1] http://www.nerc.com/docs/compliance/ccc/CCC_Charter-Feb_2010.pdf

[2] http://www.nerc.com/files/Order_on_Comp_Filing_06.07.2007_CCC_VSL_Order.pdf

CCC Organization

In addition to certain core responsibilities, the CCC has established subcommittees and a working group to perform certain tasks on behalf of and under the supervision of the CCC. Key responsibilities of these subcommittees are outlined below.

Organization Registration and Certification Subcommittee (ORCS)

To fulfill its mission, the CCC has established the Organization Registration and Certification Subcommittee to perform the following tasks on behalf of and under the supervision of the CCC:

1. Advise and provide support to NERC and the Regional Entities with development and implementation of organization registration and certification processes (i.e., ROP 500 & Appendix 5);
2. Advise and provide ongoing support to NERC and the Regional Entities relating to approved organization registration and certification processes;
3. Evaluate the success and effectiveness of NERC and the Regional Entities' administration of the organization registration and certification processes; and
4. Establish programs to monitor NERC and the Regional Entities' implementation of the organization registration and certification processes.

Standards Interface Subcommittee (SIS) and Procedures Subcommittee (PROCS) Consolidation to Form Compliance Processes and Procedures Subcommittee (CPPS)

To fulfill its mission, the CCC has elected to consolidate the SIS and PROCS. The CCC envisions that this consolidation will: (a) address the increased volume of work associated with RAI, thereby facilitating NERC and CCC communications on key characteristics and activities associated with RAI during its development and once adopted into CMEP, and address NERC Management's invitation to the CCC that it support NERC in the development and implementation of RAI; (b) lessen ERO and ERO Stakeholder administrative burdens by reducing the number of CCC Subcommittees; and (c) reflect a decreased volume of work associated with traditional PROCS and SIS activities. The key objectives of the CPPS are:

1. Perform document review to promote consistency between multiple documents (procedures, policies, standards, rules, orders, etc.) that comprise the overall NERC CMEP and to assure documents are clear, unambiguous, consistent and complementary, to advise the CCC of any deficiencies, and propose changes that it believes will clarify such situations. Activities may include, but are not limited to:
    a. Reviews of changes to the Rules of Procedure related to the Compliance Program, Registration program, and Certification Program.
    b. Proposals to change the Rules of Procedure related to the Compliance program, Registration program, and Certification Program.
2. Support the development and implementation of enhancements to the CMEP (including efforts as set forth in the CCC Work Plan) and provide this information to the CCC, applicable CCC subcommittees, and NERC.
3. Develop and maintain CCC operational procedures with respect to the CCC responsibilities under the CCC Charter;
4. Advise and prepare recommendations to the CCC to address any standards-related issues relevant to and within the scope of the NERC CCC (e.g. request from the Standards Committee, Standard Drafting Team, CCC, NERC Compliance Staff, stakeholders, etc.);
5. Act as liaison of the CCC to the NERC Standards Committee;

6. Implement CCC oversight (facilitating and participating as needed), in the development of the compliance administration elements (CAEs), including Reliability Standards Audit Worksheets (RSAWs), for new Reliability Standards under development or for revisions to existing Reliability Standards; and
7. Prepare and maintain guidance and other related documents and materials for the benefit of Standards Drafting Teams regarding the development of CAEs.

ERO Monitoring Subcommittee (EROMS)

To fulfill its mission, the CCC has established the EROMS to perform the following tasks on behalf of and under the supervision of the CCC:

1. Establish and implement programs to monitor NERC's compliance with the Reliability Standards that apply to NERC;
2. Establish and implement programs to monitor NERC's adherence to the ROP regarding the CMEP as specified in Section 405 of NERC's ROP;
3. Establish and implement programs to monitor NERC's adherence to the ROP regarding the Reliability Standards development process with the exception of appeals of substantive or procedural action or inaction associated with a Reliability Standard or the standards process as defined in the appeals section of the NERC Standards Processes Manual as specified in Section 405 of NERC's ROP;
4. Develop criteria for use by NERC for the annual evaluation of the goals, tools, and procedures of each Regional Entity compliance enforcement program in the determination of the effectiveness of each Regional Entity program as specified in Section 402.1.2 of NERC's ROP;
5. Develop and implement methods to actively solicit information with respect to stakeholder perception of the procedures, policies, standards, rules, orders, etc., and the effectiveness of the NERC CMEP and Standards development activities, and provide this information to the CCC and applicable CCC subcommittees. An annual report on stakeholder perception is provided to the NERC Board; and
6. EROMS, in 2014, will continue working closely with the Enterprise-wide Risk Committee (EWRC) and NERC staff to implement these programs.

CCC Nominating Subcommittee

The CCC annually appoints a Nominating Subcommittee. The subcommittee consists of five members nominated by the committee chair and approved by the committee. The chair of the subcommittee will be selected by the CCC chair from among the five subcommittee members. Members of the Nominating Subcommittee prepare a slate of committee officer candidates for submission to the NERC Board for approval, and prepare a slate of recommended individuals to fill designated committee vacancies as required.

For the year 2014, the Nominating Subcommittee will continue to identify qualified candidates to submit to the NERC Board for approval for those industry sectors that require representation.

Key Responsibilities Not Assigned to Subcommittees

In addition to tasks assigned to subcommittees, the CCC, in general caucus, will continue to address certain key responsibilities. These responsibilities include, but are not limited to:

1. Provide comments to NERC with respect to stakeholders' perception of the policies, practices, consistency, and effectiveness of the compliance, registration, and certification programs;
2. Recommend revisions to sections 400 and 500 (and their appendices) of the NERC ROP to the NERC Board, and provide comments to the NERC Board regarding the same when revisions are proposed by the Industry or NERC personnel;

3. Establish hearing bodies, as directed by the NERC Board, for any contest regarding findings of, or penalties or sanctions for, violation(s) of Reliability Standard(s) where NERC is directly monitoring the entity for compliance with those standards as described in the NERC ROP Section 409 (Registered entity by agreement with a Regional Entity or absent a delegation agreement; the Region itself where approved standards are applicable to the Region);
4. Establish hearing bodies with respect to registered entities Certification Appeals;
5. Serve as a mediator, as directed by the NERC Board, for any disagreements between NERC and the Regional Entities concerning NERC performance audits of Regional Entities' compliance programs;
6. Observe Regional Entity compliance program audits that are conducted at least once every five years for each Regional Entity; and
7. The CCC will provide a representative to participate on the NERC Reliability Issues Steering Committee (RISC) with the CCC providing expertise and input as requested by said member.

Hearing / Mediation Responsibilities

The CCC will conduct hearings as necessary to fulfill its function of serving as the hearing body for any contest between NERC and a Regional Reliability Organization (RRO) or Regional Entity (RE) regarding NERC findings of penalties or sanctions for violation(s) of Reliability Standard(s) by the RRO or RE as described in the NERC ROP Section 409. Note: The CCC's hearing procedures follow the hearing procedures mandated and approved by jurisdictional authorities for use by NERC and the REs in the compliance program.

The CCC will conduct hearings as necessary to fulfill its function of serving as a hearing body for any registered entity appeal regarding the determination that a registered entity is not qualified to be certified to perform the functional activities that require certification by NERC. Note: The Certification Appeal Hearing will be conducted on an expedited basis.

The CCC will conduct mediation activities when requested by the Board.

The CCC hearing and mediation procedures are described in the documents identified below and have been approved by FERC:

- CCCPP-004: CCC Hearing Procedures
- CCCPP-005: CCC Hearing Procedures for Use in Appeals of Certification Matters
- CCCPP-006: CCC Mediation Procedures

Meetings (2014)

CCC quarterly meetings (dates and locations tentative)

- March 11-12: Atlanta, GA (NERC Office)
- June 4-5: Juno Beach, FL (FPL host location)
- September 17-18: Vancouver, BC (Joint Standing Committees location)
- December 3-4: Phoenix, AZ (APS host location)

CCC subcommittees meet as needed. At a minimum, subcommittees meet the morning of the first day of CCC meetings.

NERC Board of Trustee Assignments

The CCC undertakes assignments from the NERC Board or the Board's Committees related to compliance, organization registration, and organization certification.

The primary Board assignments for 2014 are:

- With the ERO undertaking an initiative to transform compliance monitoring and enforcement to processes that are more focused on the adequacy of internal reliability risk controls, the CCC can assist in this effort by gathering examples of internal and reliability risk controls from registered entities, documenting examples of quality programs and providing an update to the BOTCC as well as the NERC Board on the state and progress of the industry in this area. CCC support in encouraging the industry to participate in these efforts also would be very helpful.
- The CCC could continue to support the quality review process in standards development and input to RSAW development during standards development. The CCC could provide additional assistance by supporting voluntary compliance trials after the NERC Board has approved a standard and prior to the mandatory and effective date for such standard. This will provide an opportunity for industry to understand compliance obligations prior to the standard becoming enforceable.
- The CCC will provide support to NERC staff on the Risk Based Registration Initiative to identify modifications to the Statement of Compliance Registry Criteria and associated changes to the NERC Rules of Procedure.

APPENDIX A - CCC Projects/Subcommittee Activities

Global CCC Projects/Activities

- CCC and subcommittee member Audit Training.
- CCC Member Hearing Training.
- Perform a Self-Assessment of the CCC and its subcommittees by July 2014.
- Develop a 2015 Annual Work Plan by November 2014.
- Review and act (if appropriate) upon reports and recommendations provided by NERC and its other Standing Committees.
- Review and comment on FERC and NERC requests for information and comments.

ORCS Activities

- Provide industry perspective and actively participate in the creation of the Risk Based Registration Framework and associated criteria consistent with the developed RAI principles.
    - This will include identification or consideration of the following:
        - Removal of redundancies
        - Ensure adequate or completeness of coverage
        - Removal of complexity
        - Consistency in application
        - Revisions to guidance documents
- Multi-Region Registered Entity Process – Perform outreach efforts with stakeholders to determine continued need for this process or to assist with isolation of issues requiring resolution. Determine if guidance documents require adjustment for the current processes or identified areas requiring resolution.
- Provide assistance with Organization Registration and Certification activities related to NERC initiatives. Monitor initiatives for impacts to guidance documents (Rules of Procedure, Compliance Registry Criteria, etc.) to assure necessary modifications are identified and addressed as needed in a timely manner, i.e. the Bulk Electric System Definition project.

EROMS Activities (See Appendix B for Monitoring Plan)

- Develop reports for the CCC.
- Implement surveys, webinars, and conduct workshops as appropriate.
- Review the criteria for annual Regional Entity Evaluations and CMEP compliance audits in 2014. Suggest modifications to this program and criteria as appropriate.
- Complete and publish the 2013 Stakeholders Perceptions Survey Report, and prepare to conduct the next survey in early 2015.
- Provide input for the EWRC 2015 Work Plan.
- Work with NERC staff to review and revise CCC procedures related to EROMS assignments.

CPPS (SIS/PROCS) Activities

- Coordinate Reliability Standards Quality Reviews on behalf of the CCC.
- Review criteria for audit/review of NERC adherence to Standards Processes Manual.
- Coordinate activities to review and provide input to NERC on compliance administration resources developed by NERC.
- Continue to review and recommend comments for CCC on proposed changes to the ROP.
- Review and format new CCC Programs as needed and as resources allow pending future changes to ROP.
- Review existing CCC Procedures to support 2014 NERC Internal Audits and CCC oversight (i.e., CCCPP-005, CCCPP-006, CCCPP-008, CCCPP-009 and CCCPP-010), and identify any necessary work for 2014 to carry out these CCC Procedures.
- Review relationship between NERC's RAI and ROP.
- Revise CCC Procedures to conform to the new monitoring model that includes NERC internal auditor and EWRC involvement. Receive reports from NERC on status and execution of RAI and to NERC from ad hoc Working Groups.
- Provide input on development of work plan related to RAI elements not part of Calendar Year 2013 RAI work effort.
- Assess how CMEP practices change after RAI is adopted in regards to: (a) monitoring practices (as embodied in CCCPP-010 and also including assisting EROMS in the annual Regional Entity Audit Criteria work); (b) enforcement; and (c) Standards development.

Reliability Assurance Initiative (RAI) Support Teams

- RAI Benefits:
  - Work with staff to provide recommendations and test approaches to take advantage of "low-hanging fruit" identified by stakeholders and NERC. Examples include:
    - Risk-focused monitoring and auditing
    - Expedited disposition approach for minor infractions
- RAI Internal Controls:
  - Work with NERC to evaluate pilots to implement a consistent approach to RAI in all Regions
  - Assist NERC in the implementation of the RAI by completing projects as requested by NERC
  - Review and revise the RAI Question & Answer Document as needed based on current RAI implementation status
  - Review and revise the RAI Internal Controls Guide as needed based on current RAI implementation status
  - Work with staff on a repository to deploy example controls for these high impact requirements
  - Work with staff to develop an information sharing site for application guidance and controls for other requirements
- RAI Data Retention and Sampling

- Draft data retention guidance and sampling documents based on responses to the team's survey
- If not completed in 2013, draft and post conforming changes to the ROP

- RAI RSAW
  - Work to provide input on the content of the current RSAWs and how the RSAWs are used
  - Focus on primary areas of concern, scope, and consistency
  - Four initial areas of suggested improvement:
    - RSAW Structure
    - RSAW Use
    - RSAW Development
    - Internal Controls application

APPENDIX B - 2014 CCC Monitoring Plan

Stakeholder Perceptions Survey

- EROMS will conduct and prepare a summary report for the Board.
  - Include lessons learned from the 2013 survey
  - Continue to refine the question and survey instrument

NERC Self-Certifications

- EROMS will request NERC to self-certify adherence with the ROP for the following areas:
  - Compliance Monitoring and Enforcement Program (CMEP)
  - Organization Registration and Certification Programs (ORCP)
- EROMS will prepare a summary report of the results of the submitted NERC Self-Certifications for the Board.

Enterprise-wide Risk Committee (EWRC)

- The CCC Executive Team will coordinate with the EWRC to determine the use of Spot-Checks of NERC processes in 2014 for those areas for which the CCC is responsible for monitoring in coordination with the EWRC.
- The CCC Executive Team will coordinate with the EWRC to determine the use of a third party to conduct audits of the standards applicable to NERC and the Standard Process Manuel in 2014.

Detailed Overview of Monitoring Activities

In pursuit of its responsibilities, the CCC will mirror the monitoring approaches used by the ERO. To the extent NERC self-reports issues and develops sound internal controls, the approaches to monitoring outlined below will be adjusted.

Self-Certifications

In accordance with CCCPP-001, the EROMS will review and modify (if necessary) the subset of performance items related to the ROP for the CMEP. The CCC will then request that NERC self-certify adherence to ROP for the CMEP, with respect to the subset of performance items, by providing the CCC with a report at its regularly scheduled September 2014 meeting.

In accordance with CCCPP-007, the ORCS will review and modify (if necessary) a subset of performance items related to the ROP for Organization and Registration. The CCC will then request that NERC self-certify adherence to the ROP for Organization Registration and Certification, with respect to the subset of performance items, by providing the CCC with a report at its regularly scheduled September 2014 meeting.

The two reports described above will be in the form of a presentation provided by a NERC officer or equivalent responsible for ensuring adherence to the above identified four elements of the ROP. The presentation will identify adherence to the rules as well as any areas of non-adherence. The CCC will include the results of the self-certifications in these four areas in a report to the Board.

Audits/Reviews

In accordance with CCCPP-001, the CCC will perform an audit/review of NERC's adherence with the ROP for Compliance Monitoring and Enforcement every three years. Additionally, an unscheduled audit/review may be initiated by the CCC if deemed necessary to determine NERC's adherence with the ROP for compliance enforcement or to review deficiencies from previous audits.

In accordance with CCCPP-003, the CCC will perform an audit/review of NERC's adherence with the NERC Standards Processes Manual every three years. Additionally, an unscheduled audit/review may be initiated by the CCC, if deemed necessary, to determine NERC's adherence with the NERC Standards Processes Manual. The audit/review team will develop a draft review report, review it with NERC, make any necessary changes, and then prepare a final report to be submitted to the CCC. The CCC will review/assess the report and provide NERC a final copy. The CCC will advise the NERC Board of any Preliminary Adverse Findings and include the results of the audit/review in the report to the Board. Based on the experience of the 2012 audits, the CCC Executive Team will coordinate with the NERC Board EWRC to determine the use of a third party audit of Reliability Standards development in 2014.

In accordance with CCCPP-007, the CCC will perform an audit/review of NERC's adherence with ROP for Organization Registration and Certification every three years. Additionally, an unscheduled audit/review may be initiated by the CCC, if deemed necessary, to determine NERC's adherence with the ROP for Organization Registration and Certification. The audit/review team will develop a draft review report, review it with NERC, make any necessary changes, and prepare a final report to be submitted to the CCC. In accordance with CCCPP-001, the CCC may initiate an Adverse Finding Investigation, at any time, as directed by the Board or based on an event, complaint, or other possible Adverse Finding identified by any other means. Adverse Finding Investigations will follow the processes outlined in a Compliance Program Audit.

In accordance with CCCPP-003, the CCC may initiate a Standards Development Process Review Investigation, at any time, as directed by the Board or in response to a complaint or evidence that NERC has not adhered to the

Standards Development Process Procedures. Standards Development Process Review Investigations will follow the processes outlined for a Standards Development Process Review.

In accordance with CCCPP-007, the CCC may initiate an Organization Registration and Certification Investigation as directed by the Board, or at any time in response to a complaint or evidence that NERC has not adhered to the ROP for Organization Registration and Certification. Adverse Finding Investigations will follow the processes outlined for a Registration and Certification Program Audit.

Spot-Checks

In accordance with CCCPP-001, the CCC may from time-to-time perform spot-checks to determine whether NERC is adhering and/or has adhered to the ROP for Compliance Enforcement. Spot-checking may also be initiated in response to a directive from the Board or to events or a complaint. Results of spot-checks will be provided to NERC and will be reported to the NERC Board.

In accordance with CCCPP-003, the CCC may from time to time perform spot-checks to determine whether NERC is adhering and/or has adhered to the Reliability Standards development process. Spot-checking may also be initiated in response to a directive from the Board or to events or a complaint. Results of spot-checks will be provided to NERC and will be reported to the NERC Board.

In accordance with CCCPP-007, the CCC may from time to time perform spot-checks to determine whether NERC is adhering and/or has adhered to the ROP for Organization Registration and Certification. Spot-checking may also be initiated in response to a directive from the Board or to events or a complaint. Results of spot-checks will be provided to NERC and will be reported to the NERC Board.

The CCC Executive Team will coordinate with the NERC Board EWRC to determine the use of spot-checks of NERC processes in 2014.

NERC Evaluation of Regional CMEP Implementation

The CCC developed the CCCPP-010 – Criteria for Annual Regional Entity Program Evaluation that, per Rule of Procedure 402.1.2, establishes criteria for NERC to use in order to "annually evaluate the goals, tools, and procedures of each Regional Entity Compliance Monitoring and Enforcement Program to determine the effectiveness of each Regional Entity Compliance Monitoring and Enforcement Program." In 2014, the CPPS is expected to update CCCPP-010, and, as was the case in the original development of CCCPP-010, intends to collaborate with NERC Compliance Operations on developing the Criteria.

Monitoring Stakeholder Perceptions

As stated in the CCC Charter in Section 3, Committee members are expected to represent the interests of the sector they represent, to the best of their ability and judgment. Members are expected to solicit comments and opinions from constituents and groups of constituents, or trade organizations represented by the member and convey them to the CCC. During 2014, committee members will participate in documenting comments to the CCC, with respect to stakeholders' perception of the policies, practices and effectiveness of the CMEP, Registration Program, and Certification Program. The EROMS will lead, direct, and initiate these reviews and surveys of CCC members and provide recommendations for consideration to NERC.

The CCC has developed the Program for Monitoring Stakeholders' Perceptions of NERC CMEP, Registration Program, and Certification Program. An element of this program expected to be carried out in 2014, in addition to obtaining direct feedback from committee members, will include conducting surveys of stakeholders in the second half of the year. Depending upon the level and nature of the feedback gathered, additional elements of

the program may include seeking stakeholder feedback in a CCC-sponsored segment contemporaneous with Regional Entity Compliance Workshops or in conjunction with existing stakeholder compliance working groups. Part of the communication provided in advance would include the explanation of the roles/functions of the CCC, the survey elements being considered, and the manner for providing a feedback report to the Board and the stakeholders. Additional methods of communicating with stakeholders may include providing information regarding the survey in NERC News and direct e-mails to stakeholders.

An important element of the program will be an annual report, presented to the CCC for approval to forward to NERC, the Board, and the stakeholders, as well as quarterly stakeholder perceptions reports to the CCC. Specifically, the NERC BOTCC has asked that the CCC take the lead on analysis of the perception survey responses, refining issue identification, developing possible action plans with industry input, facilitating development of alternatives, and making recommendations to the NERC staff or Board.

In addition to the annual perception survey, the CCC will hold a member roundtable at each CCC meeting. During the roundtable, the members are expected to raise issues, observations and concerns of their stakeholders. The CCC will capture issues raised and work with staff to resolve them as they arise.

Longer term activities, beyond 2014, may include mechanisms for the CCC to directly receive feedback from stakeholders following audits and any of the other effectiveness monitoring inputs or evaluations surrounding the effectiveness metrics endorsed in CCCPP-008.

Appendix C - CCC Programs

The CCC has established several programs to fulfill its obligations. Many of these will be coordinated with the NERC Director of Internal Audit. These programs include specific monitoring activities such as periodic on-site audits/reviews, NERC Self-Certifications, CCC Spot-Checks, CCC Adverse Finding Investigations, NERC Self-Reporting, Periodic Data Submittals, and CCC Review of Stakeholder Complaints. As resources allow, audits and spot-checks may be conducted by independent contractors. The programs are described below.

CCCPP-001: Monitoring Program for NERC's Adherence to NERC's ROP

This program has been established so that the CCC can monitor NERC's adherence to its ROP for Compliance Enforcement. The NERC CCC EROMS will coordinate this effort.

CCCPP-002: Compliance Monitoring Program for Reliability Standards Applicable to NERC

This program has been established so that the CCC can monitor NERC's adherence to NERC Reliability Standards applicable to NERC. The CCC will use a variety of activities to perform the monitoring. The NERC CCC EROMS will coordinate this effort.

CCCPP-003: Monitoring Program for NERC's Standards Processes Manual

This program has been established so that the CCC can monitor NERC's adherence to its ROP concerning Reliability Standards development. The NERC CCC EROMS will coordinate this effort.

CCCPP-007: Monitoring Program for NERC's Adherence to NERC's ROP for Organization Registration and Certification

This program has been established so that the CCC can monitor NERC's adherence to its ROP for Organization Registration and Certification. The NERC CCC ORCS will coordinate this effort.

CCCPP-008: Program for Monitoring Stakeholders' Perceptions of NERC Compliance Program, Registration Program, and Certification Program

This program has been established so that the CCC can gather and report to the Board, stakeholder perceptions with respect to NERC's CMEP, Organization Registration Program and Certification Program and the way the programs are administered. The NERC CCC EROMS will coordinate this effort.

CCCPP-010: Criteria for Annual Regional Entity Program Evaluation

This program has been established to identify the criteria by which these audits are conducted, provide a guidance letter to NERC regarding these criteria, and document the process for the CCC to annually review and affirm these for use. The NERC CCC EROMS will coordinate this effort.

Appendix D - Logistics and Budget Requirements for CCC Activities

Listed below are items identified by the CCC that NERC should take into account with respect to costs NERC will incur concerning CCC activities for 2014-2016.

CCC Quarterly Meetings (Cost to be determined by NERC)

Assumptions: Four CCC meetings per year

- NERC staff attendance
- NERC travel expenses
- Hotel (Conference Rooms and Food)

Hearings and Appeals (Cost to be determined by NERC)

Assumptions: One hearing or appeal in 2014

- Administrative Law Judge's fee
- Hearing refresher training
- Transcription costs
- Travel expenses

Notes:
The CCC conducted hearing training in 2012. It is recommended that training be conducted in 2014 for those CCC members that have not received training or for those that request refresher training.

CCC will notify NERC and the Board if additional hearings are expected.

Mediation (Cost to be determined by NERC)

Assumptions: No mediations expected, but noted here as a placeholder

- Mediator fee and travel expenses

CCC Program Audits/Review

Assumptions: Audit/Review Independent Contractor $125,000 annually

- Audit periodicity will increase as NERC internalizes monitoring capability, based upon recommendations of independent reviewer.

WebEx/Conference Calls (Cost to be determined by NERC)

Assumptions: Three CCC/Subcommittees NERC Web-Ex or conference calls quarterly

Stakeholder Perception Survey (Cost to be determined by NERC)

Assumptions: At the request of the NERC Board, the CCC engaged a professional survey firm to conduct stakeholder perception surveys.

Training (Cost to be determined by NERC)

Assumptions: Half day of hearing training appended to regular CCC meeting every even year.

- Five to ten CCC members will attend NERC auditor training annually.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda Item 14.h.ii

ERO Effectiveness and Stakeholder Perceptions Survey

Report to the NERC Board of Trustees by the Compliance and Certification Committee

April 2014

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Table of Contents 2

Executive Summary 3

2013 Recommendations 4

Introduction 5

Survey Composition and Response Rates/Demographics 6

Rating Scale 6

Survey Items 6

Response Rate and Demographics 8

Summary of Survey Responses 10

Topic Area Analyses 10

Highest and Lowest-rated Items 11

Topic Analyses by Region 13

Favorability Analyses 18

Regional Favorability Analysis 20

Year-over-year Analyses 25

Comment Analysis 32

Compliance Monitoring 33

Enforcement Actions 34

Organization Registration 35

Organization Certification 36

Compliance and Reliability Impact 37

Recommendations: ERO-CMEP 39

Recommendations: Regional Entities 40

Inconsistencies across Regions 41

Conclusion and Recommendations 42

Conclusion 42

2013 Recommendations 42

Executive Summary

In the third quarter of 2013, consistent with its 2013 Annual Plan, the NERC Compliance and Certification Committee (CCC) conducted its fifth annual survey measuring stakeholder perceptions on the policies, practices and effectiveness of NERC and Regional Entities with respect to the Compliance program, Registration program, and Certification program. This periodic review is an essential element of the Board of Trustees (Board) and Federal Energy Regulatory Commission (FERC)-endorsed CCC Charter.

http://www.nerc.com/docs/compliance/ccc/CCC_Charter-Feb_2010.pdf)

The CCC survey is intended to be a source of industry feedback to the NERC Board on NERC's and the Regions' effectiveness and performance. To execute this year's survey, the CCC partnered with third-party provider TalentQuest, a talent management software and human capital management consulting firm, to drive survey enhancements. The CCC also reformulated survey content to create a more discerning, rigorous and valid evaluation, captured demographic data (3-year vs. 6-year audit cycle and registered function), examined responses across Regions, employed favorability analyses to interpret response polarity, conducted a year-to-year comparison of perception to identify trends, and incorporated thematic analysis of written responses. The NERC Board is encouraged to provide feedback and insight to the CCC that would be helpful for future enhancements to this survey.

The 2013 survey employed both a qualitative and quantitative approach to measure perceptions of industry stakeholders. Perceptions were measured across 6 Topic Areas including: Compliance Monitoring, Enforcement Actions, Organization Registration, Organization Certification, Compliance and Reliability Impact, and Other **(Appendix A)**. With the objective of more robust analysis and greater interpretability, a CCC project committee identified, developed and validated a set of 26 items that measured the constructs of the 6 Topic Areas. The CCC also updated the five rating scale descriptors, transitioning to an agreement-driven scale of "Strongly Disagree" to "Strongly Agree." This rating scale captured the degree to which respondents perceived NERC and the Region performance against the referenced program aspect.

Survey participants included all individuals listed on the NERC Primary Compliance Contact (PCC) Roster. For those respondents representing entities in multiple Regions, the 2013 survey form contained a section on each Region represented. NERC and the Regions were evaluated separately in all Topic Areas except Compliance and Reliability Impact and Other where perceptions were measured in the aggregate.

The results provide a range of views from all sectors represented on the CCC and all registered entity functions. The overall responses and comments were insightful in delineating stakeholders' relative perceptions of program strengths and opportunity areas.

Industry feedback of strengths included:

- Compliance Monitoring components involving audit teams, audit processes, and self-certification.
- Positive progress by NERC and the Regions across all Topic Areas between 2012 and 2013 is reflected by increases in perceptions ranging from .05 to .29.

Industry feedback for improvement included the themes:

- Increased consistency and standardization (in processes across Regions, in penalty application and the settlement process, and in communications from NERC and Regional Entities).
- Communication of clearer, more applicable definitions (in the recertification processes, in Joint Registration Organization (JRO) and Coordinated Functional Registration (CFR) processes, in the BES, and in valid reliability measure).

- Greater efficiencies (via increased process timeliness and feedback, increased return on investment of compliance program, continued streamlining of standards, and increased transparency).

In addition, following the preliminary presentation of survey results, including the thematic analysis of all comments, NERC leadership requested additional analysis to uncover more specificity and clarification around any comments that may suggest inappropriate or unprofessional conduct.

2013 Recommendations

Through analysis and interpretation of the 2013 Stakeholder Perception Survey, the CCC has decided to recommend that NERC continue to move forward with the 2012 recommendations which are tied to the three themes that have prevailed over the past three years the survey has been conducted:

1. Return on Investment (ROI) of compliance program;
2. inconsistencies within and across Regions; and
3. transparency of the enforcement and penalty processes

In this context, ROI means reliability benefits versus resources expended on compliance. In addition to the recommendations below, NERC should address the specific conduct concerns that were presented in some of the comments.

These concerns have been presented to NERC under separate cover:

1. The CCC should continue to work with NERC staff to communicate the survey results in a productive way to NERC and the Regions to facilitate performance improvement and positively impact stakeholder perceptions.
2. The recommendations provided in the 2011 Stakeholder Perceptions Survey specifically included items to address ROI (recommendation number one) and transparency (recommendation number four). NERC should compile a new list of action items based on this 2012 survey and those provided in the 2011 survey. The CCC should have a standing item on its agenda for the next year to review NERC's progress on its action plan, offer assistance where requested, and work with NERC to communicate its successes to improve the results of future surveys.
3. NERC should review key/identified post-audit processes (audit reports, mitigation plans and settlements) with the objective of standardizing the process across Regions, streamlining components, and reducing the total process time.
4. NERC staff should review the free form written responses to the survey to identify the predominant consistency issues and develop an action plan to address them. NERC should implement a Multi-Region Registered Entity (MRRE) process by the end of 2014 (this was also addressed in the 2011 survey recommendations).

The CCC thanks the industry for their participation and the feedback provided in the survey. The CCC also wants to recognize NERC's support in facilitation of the CCC Stakeholder Survey, and its provision of an outside consultant to drive survey enhancement. The CCC requests that the Board consider releasing a public version of the report.

Introduction

The CCC Electric Reliability Organization Monitoring Subcommittee (EROMS) conducted a survey of stakeholder perceptions in accordance with the NERC CCC Charter.[1] Primary Compliance Contacts in the NERC database (1201 PCCs) were polled to measure stakeholder perceptions of NERC and Regional Entity effectiveness in implementing and executing components of the continent-wide Compliance, Registration, and Certification programs since June 18, 2007.

The 26 item survey measuring the constructs of the 6 Topic Areas was transmitted to the NERC PCC Roster in order to solicit response from the broad stakeholder spectrum within registered entities. The CCC received a 29.3 percent response rate to the 2013 survey, a 3 percent increase compared to 2012.

The Topic Areas evaluated in the 2013 survey included the following:

- Compliance Monitoring
- Enforcement Actions
- Organization Registration
- Organization Certification
- Compliance and Reliability Impact
- Other

To facilitate greater interpretability and more robust analysis, a CCC project committee identified, developed and validated the set of 26 items measuring the constructs of the 6 Topic Areas **(Appendix A)**. These items were evaluated via a five-point, agreement-based rating scale ("Strongly Disagree" to "Strongly Agree"). Stakeholders were asked to evaluate NERC and the Regions separately on the first four Topic Areas (Compliance Monitoring, Enforcement Actions, Organization Registration, and Organization Certification), and for a combined NERC/Region evaluation in the Compliance and Reliability Impact and Other Topic Areas. Qualitative data was gathered at the Topic Areas and through three open-ended questions. The qualitative data was interpreted through a thematic analysis to quantify open-ended perceptions. Demographics gathered included Region, Registered Function, and Audit Cycle. In addition to Regional topic and item analyses, the survey reported item favorability (item response distribution), and year-over-year trend analyses.

[1] Section 2.2.a: "Provides comments to NERC with respect to stakeholder's perception of the policies, practices and effectiveness of the Compliance program, Registration program, and Certification program."

Survey Composition and Response Rates / Demographics

Rating Scale

1 – Strongly Disagree

2 – Disagree

3 – Neither Disagree nor Agree

4 – Agree

5 – Strongly Agree

Survey Items

Compliance Monitoring [NERC, Regions evaluated separately]

1. Our most recent audit process (including pre- and post- audit activities) was conducted in a timely manner.
2. The audit team conducts themselves in a professional and credible manner.
3. The audit team is prepared and organized to conduct the audit process.
4. The audit team adheres to established rules and processes.
5. The spot check process is well-defined, organized and timely.
6. The self-reporting process is well-defined, organized and timely.
7. The self-certification process is well-defined, organized and timely.

Please provide any recommendations regarding Compliance Monitoring: _____

Enforcement Actions [NERC, Regions evaluated separately]

8. The audit report identifies clear, definitive, and actionable items to address.
9. All communication of violations clearly and specifically describe the manner in which a requirement was violated.
10. All communication of violations clearly and specifically describe the risk of the PV both actual and potential.
11. The mitigation plan submission and approval process is efficient and effective.
12. The settlement process is transparent, consistently applied, and clearly communicated.
13. The penalty process and penalties are transparent, consistently applied, and clearly communicated.

Please provide any recommendations regarding Enforcement Actions: _____

Organization Registration [NERC, Regions evaluated separately]

14. The functional model is clear and minimizes overlaps and gaps.
15. The Organization Registration process minimizes overlaps and gaps.
16. The Organization Registration process is well-defined and efficient.
17. The rules for assigning registered functions to entities are clear and accurately applied.
18. The Joint Registration Organization (JRO) and Coordinated Functional Registration (CFR) processes are clear and consistently implemented.

19. Inquiries about the registration process are responded to in a timely and effective manner.
20. There is a timely and effective response during the Registry Appeals Process.

Please provide any recommendations regarding Organization Registration: _____

Organization Certification [NERC, Regions evaluated separately]

21. Organization Certification rules and procedures are clear and consistent

Please provide any recommendations regarding Organization Certification: _____

Compliance and Reliability Impact

22. NERC Compliance programs and corresponding industry efforts have enhanced reliability of the bulk power system.
23. Regional Entity Compliance programs and corresponding industry efforts have enhanced reliability of the bulk power system.
24. The Standards Driven Index (SDI) which includes the Compliance Index (CI) coupled with the Adequate Level of Reliability (ALR) demonstrates enhanced reliability for the industry.
25. The reliability benefits experienced are worth the degree of compliance effort (time and resources) our entity has expended.

Please provide any recommendations regarding Compliance and Reliability Impact: _____

Other

26. The Compliance Monitoring and Enforcement processes are applied consistently across NERC and the Regions.
    - *If applicable, please provide specific examples of inconsistencies across Regions and/or NERC*
    - *Please provide any recommendations regarding the ERO CMEP: _____*

Please provide any recommendations regarding the Regional Entities: _____

Response Rate and Demographics

There were 1201 PCCs invited to respond to the 2013 survey. There were 352 individual survey respondents (29.3 percent response rate). PCCs representing entities in multiple Regions completed the survey for each applicable Region resulting in more Regional data points than individual respondents. The response rating increased from 26.4 percent to 29.3 percent over 2012 despite a 78 decrease in number of respondents.

Regional Responses (frequencies) by Registered Function

While the Registered Function demographic was not utilized in response analysis, the data more fully describes the respondent sample.

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
FRCC	8	17	17	16	8	14	9	11	0	10	1	14	12	11	6
MRO	15	20	21	22	6	21	5	28	4	19	1	23	15	18	11
NPCC	3	17	44	43	3	18	3	26	2	3	1	11	9	9	10
RFC	6	21	50	49	2	20	3	43	2	4	0	15	4	3	2
SERC	15	33	48	46	12	32	13	38	5	14	5	20	14	15	11
SPP	12	22	25	24	1	23	1	21	3	13	1	21	13	11	1
TRE	1	17	37	32	1	23	1	12	1	1	0	20	15	18	2
WECC	17	57	79	75	1	58	14	52	1	22	1	42	31	23	20
TOTAL	77	204	321	307	34	209	49	231	18	86	10	166	113	108	63

Regional Responses (frequencies) by Audit Cycle

While Audit Cycle demographics were not utilized in response analysis, the data more fully describes the respondent sample.

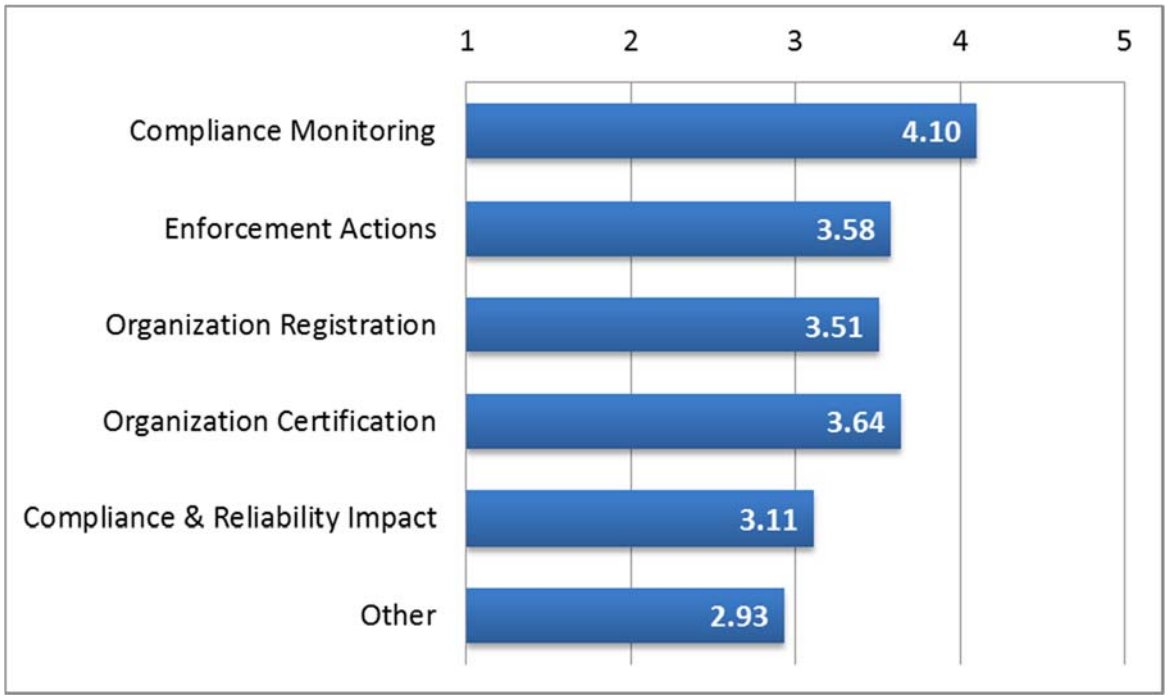
	3 Year Audit Cycle	6 Year Audit Cycle
FRCC	13	18
MRO	22	22
NPCC	12	60
RFC	17	66
SERC	21	59
SPP	19	33
TRE	23	41
WECC	42	92
TOTAL	169	391

Summary of Survey Responses

Topic Area Analyses

The first level of analysis was conducted at the Topic Area level and considered all survey responses in aggregate (NERC and Regions combined). Compliance Monitoring was the highest-rating Topic Area (mean = 4.10), with all five of the survey's highest-rated items emerging from Compliance Monitoring. The lowest rated Topic Area, "Other" (mean 2.93) was comprised of a single item, "The Compliance Monitoring and Enforcement processes are applied consistently across NERC and the Regions." The four remaining lowest-rated items were distributed across the Topic Areas of Compliance and Reliability Impact, Organization Registration, and Enforcement Actions.

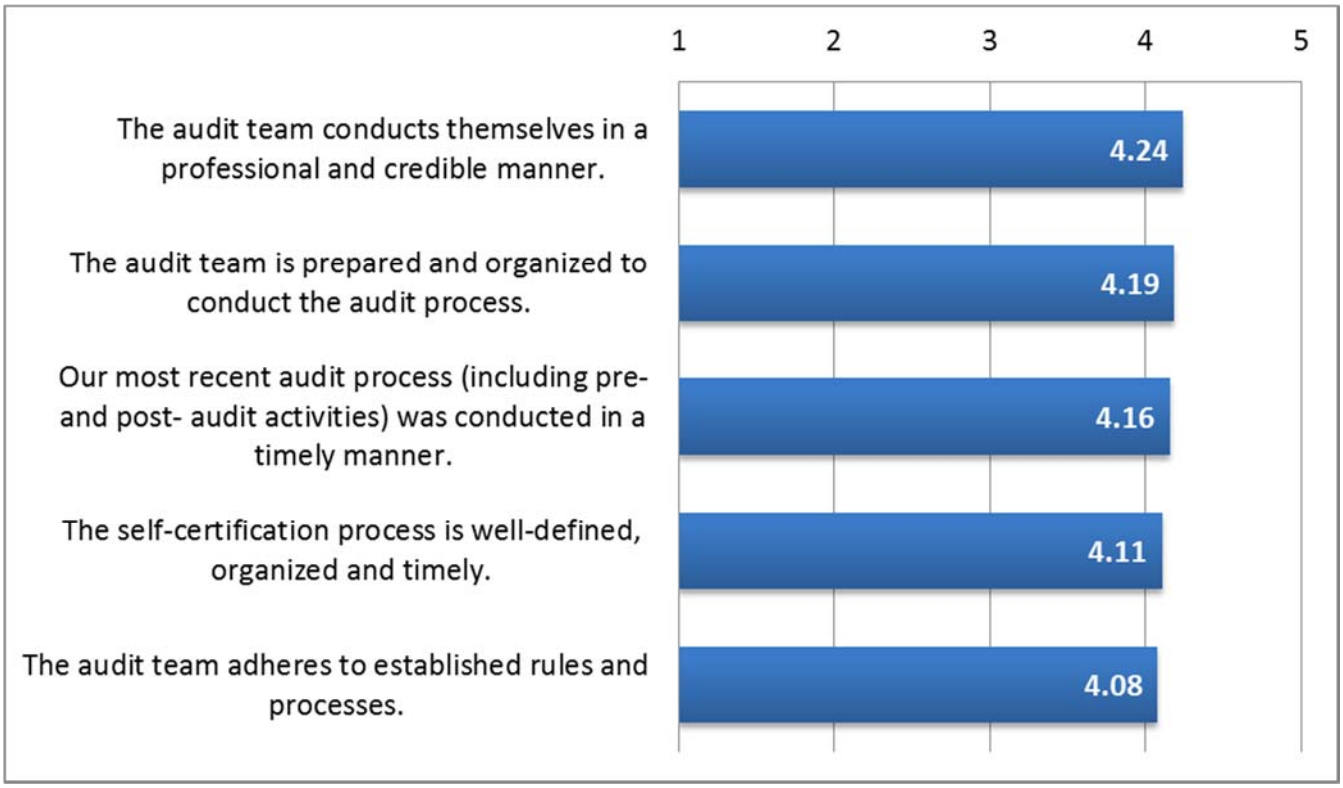
Topic Area Means



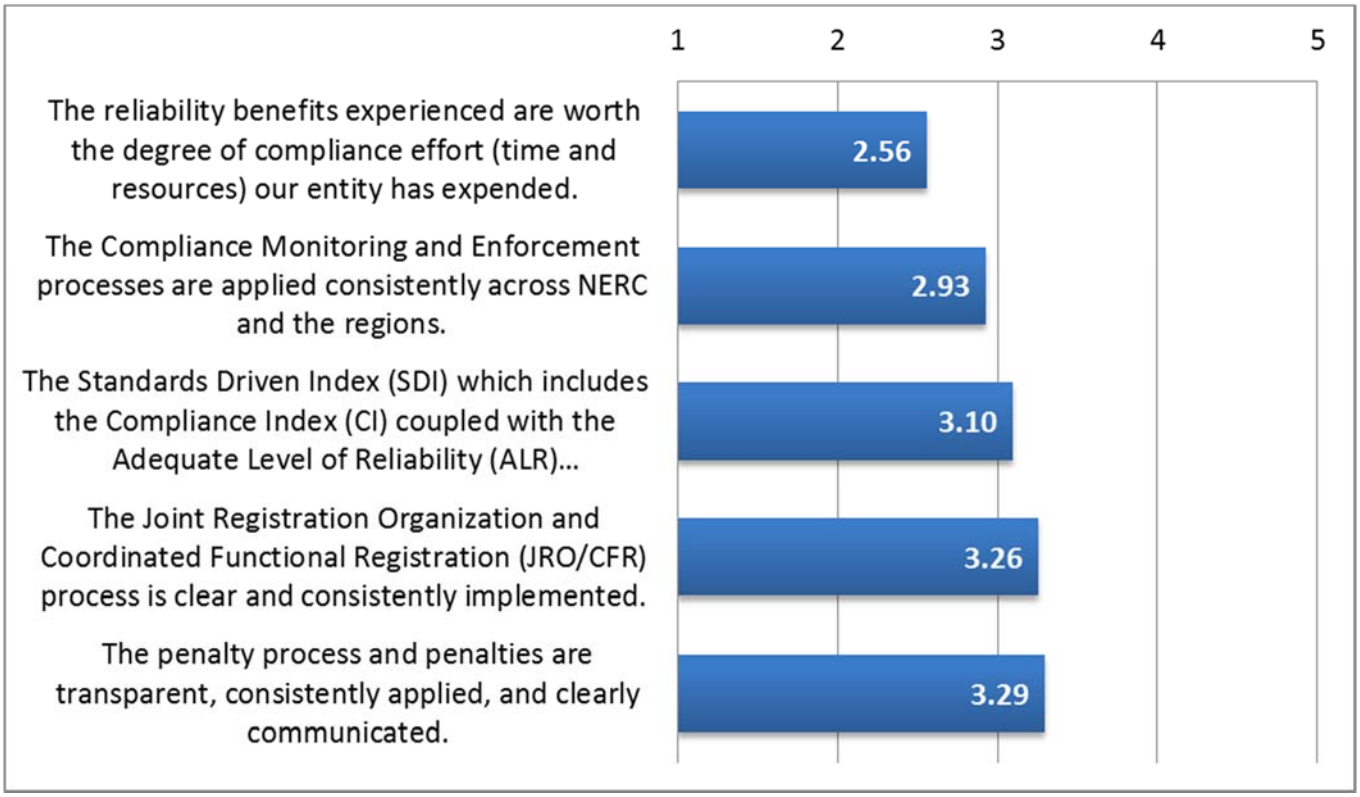
Highest and Lowest-rated Items

All five of the survey's highest-rated items were in the Compliance Monitoring Topic Area with means of 4.08 and above. The lowest-rated item means ranged from 2.56 to 3.29 and were distributed across Topic Areas of Other, Compliance and Reliability Impact, Organization Registration, and Enforcement Actions. All item means can be found in **Appendix A**.

Highest-Rated Items



Lowest-Rated Items



Topic Analyses by Region

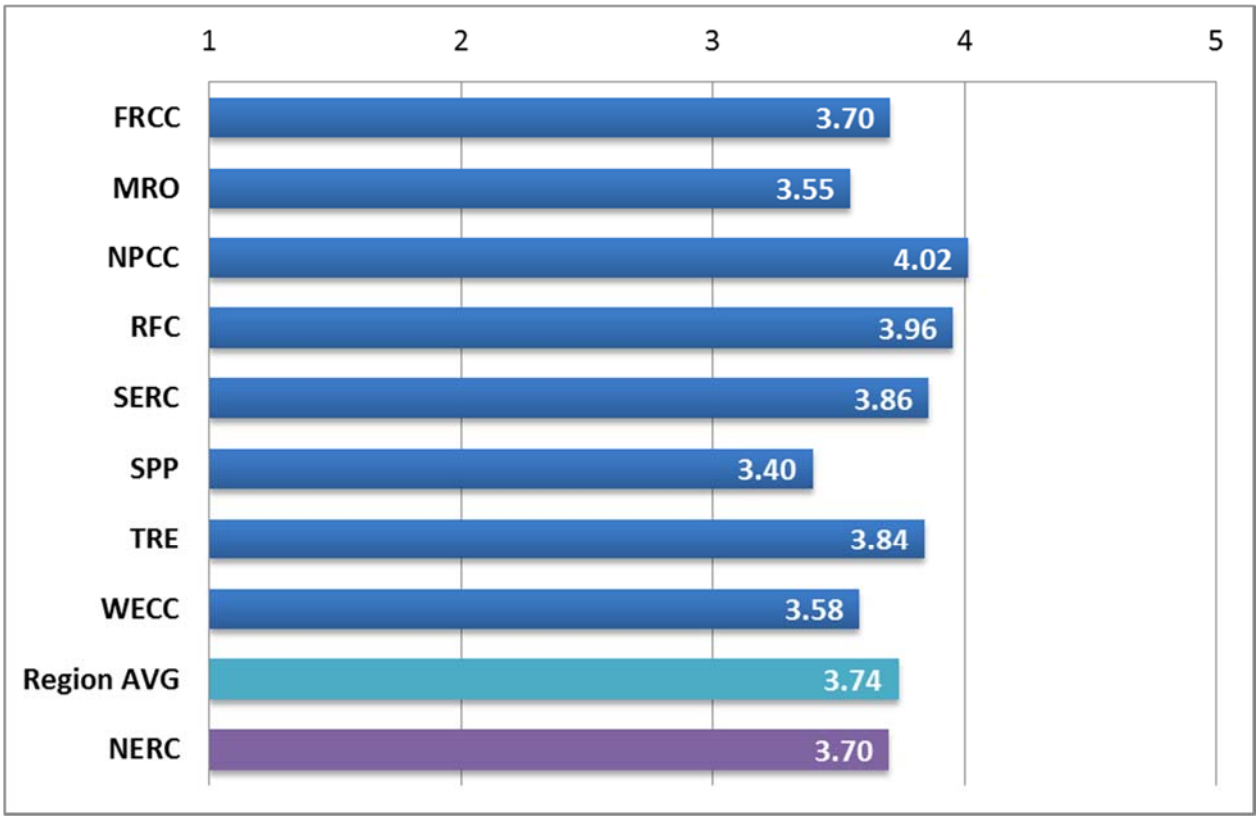
For the 4 Topic Areas where ratings were gathered for NERC and the Regions, analysis was conducted for both the Regions and NERC. Those Topic Areas were: Compliance Monitoring, Enforcement Actions, Organization Registration and Organization Certification. The following analyses depict differences across the individual Regions, the combined Regions, and NERC. T-tests and ANOVA were used to identify statistically significant differences.

In this analysis, the calculated, "Overall Average" of all items (the 21 items contained in these Topic Areas), identified a slight difference between NERC (3.70) and the Regions (3.74). Individual Region Overall means ranged from 3.40 to 4.02.

The 4 Topic Area analyses reflected little variation between the Regions (combined) and NERC, with differences ranging only from .01 to .16. Conversely, means between Regions varied both in the ranking order of Regions across Topic Areas, and in within-Topic differences (ranging up to .79).

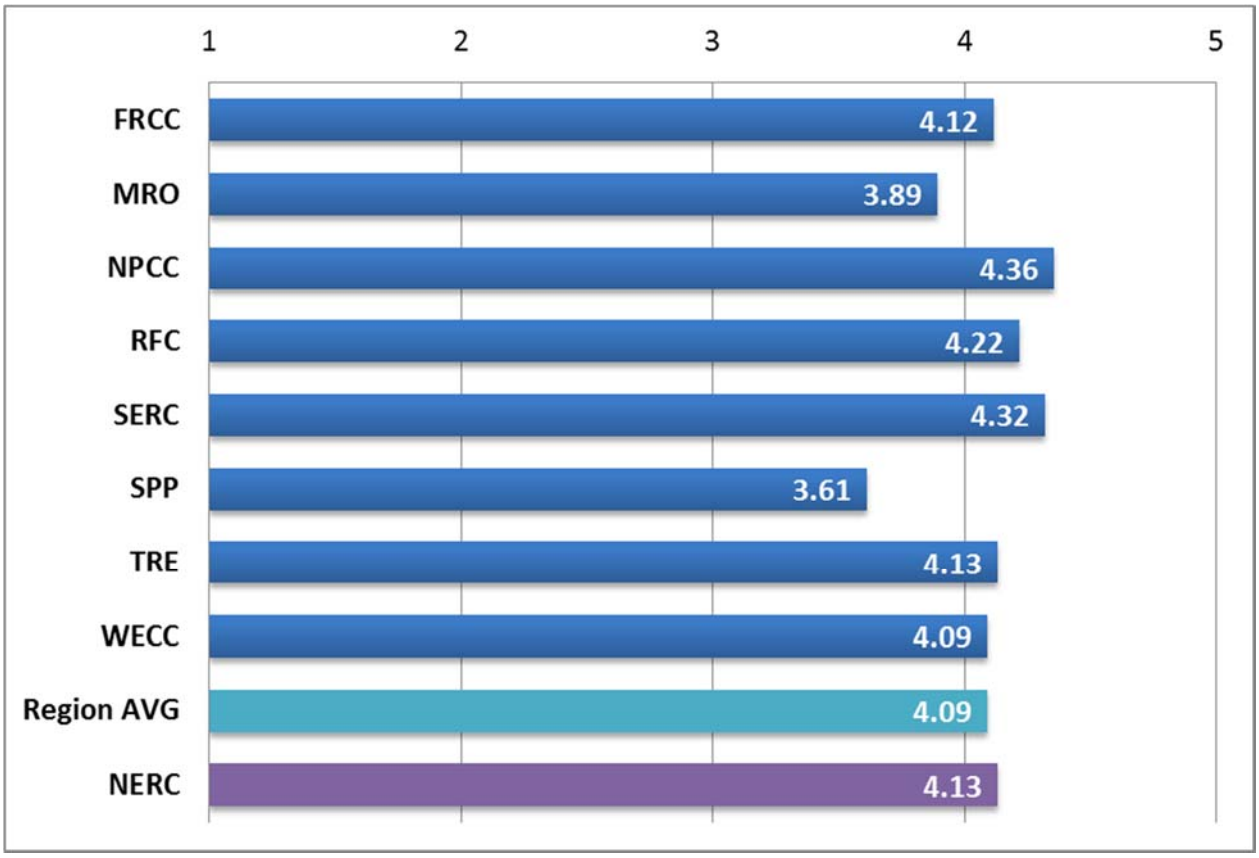
Overall Averages

Between the Regions, a .62 difference exists between the highest mean (4.02, NPCC) and the lowest mean (3.40, SPP), with statistically significant differences found between SPP and NPCC ($p < .05$).



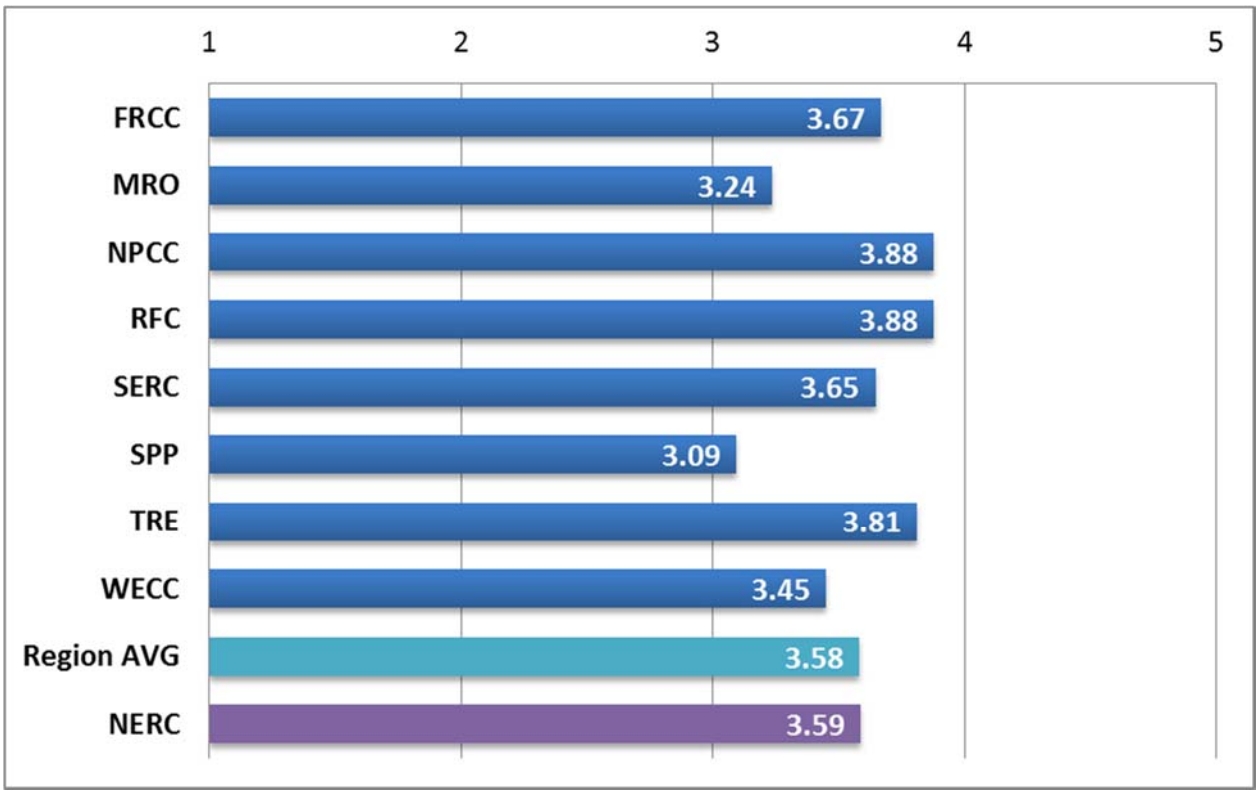
Compliance Monitoring

Individual Region averages ranged from 3.61 (SPP) to 4.36 (NPCC) within Compliance Monitoring, and significant differences were found between SPP and NPCC, MRO and NPCC, and FRCC and NPCC (all at p <.05).



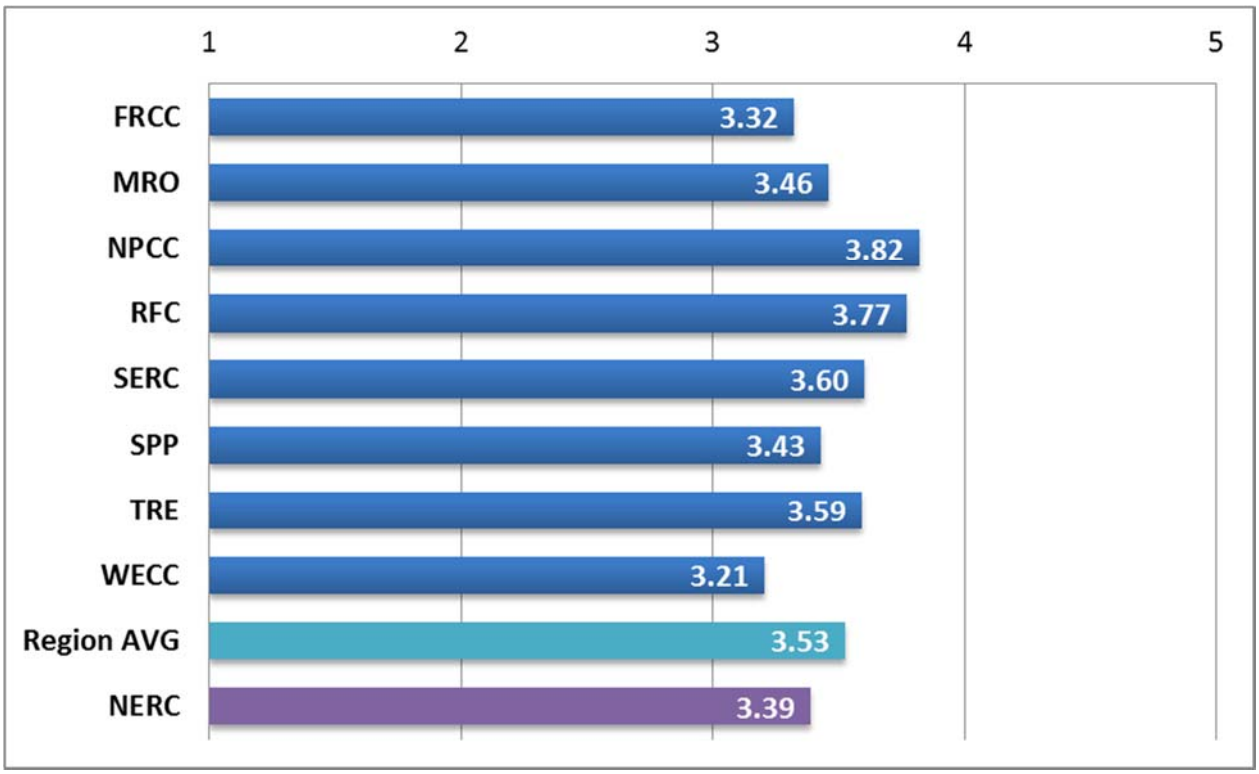
Enforcement Actions

Individual Region averages ranged from 3.09 (SPP) to 3.88 (NPCC and RFC) with significant differences found in SPP and NPCC, and SPP and RFC (p<.05).



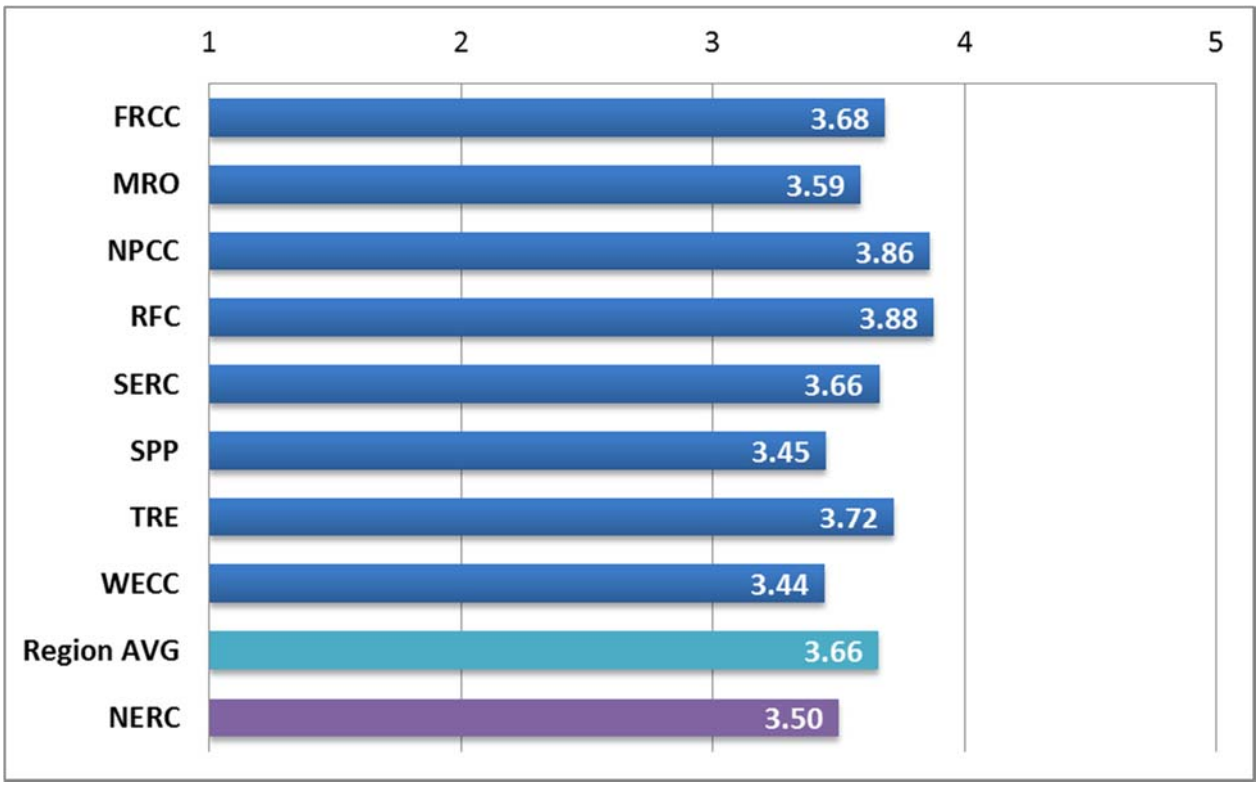
Organization Registration

Individual Region averages ranged from 3.21 (WECC) to 3.82 (NPCC) with a significant difference present between WECC and NPCC ($p < .05$).



Organization Certification

Individual Region averages ranged from 3.44 (WECC) to 3.88 (RFC) with a significant difference present between WECC and RFC ($p < .05$).

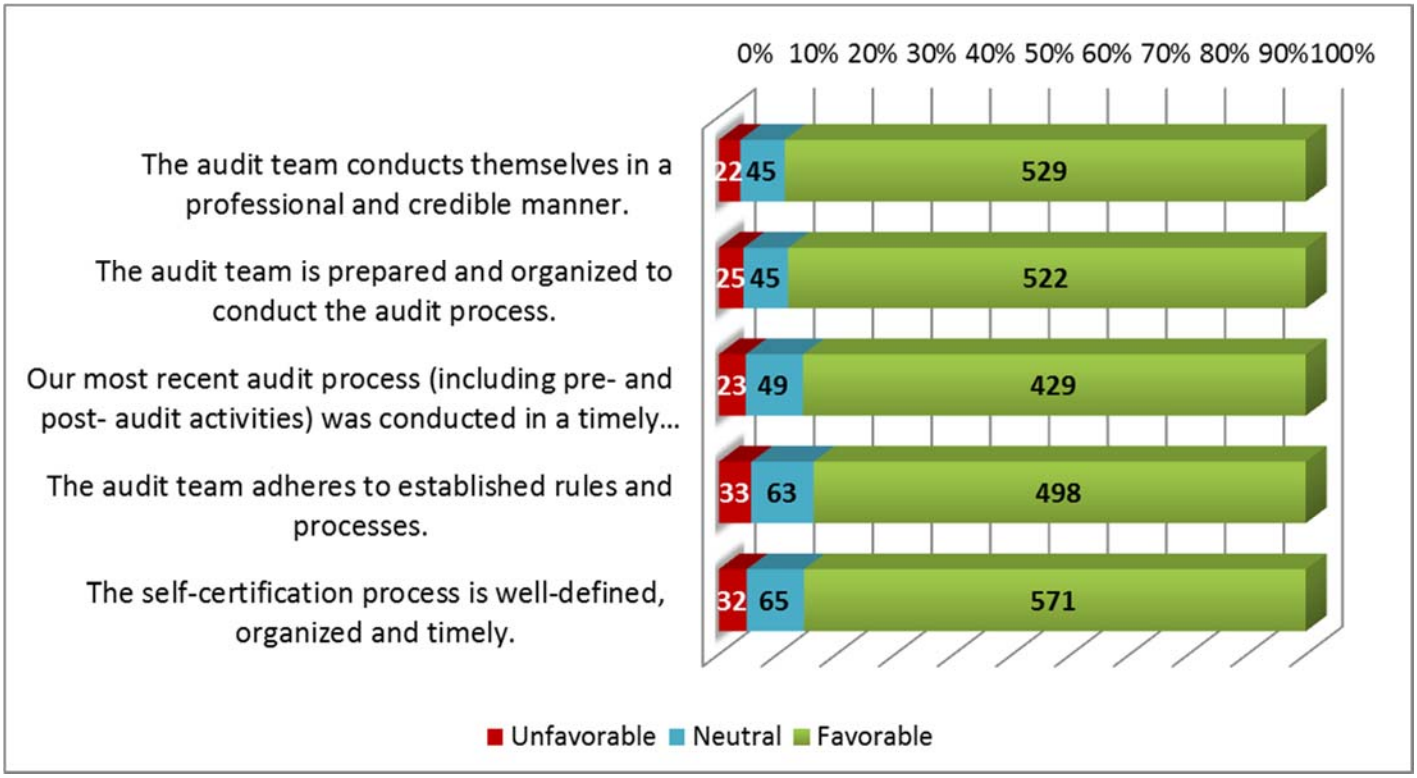


Favorability Analyses

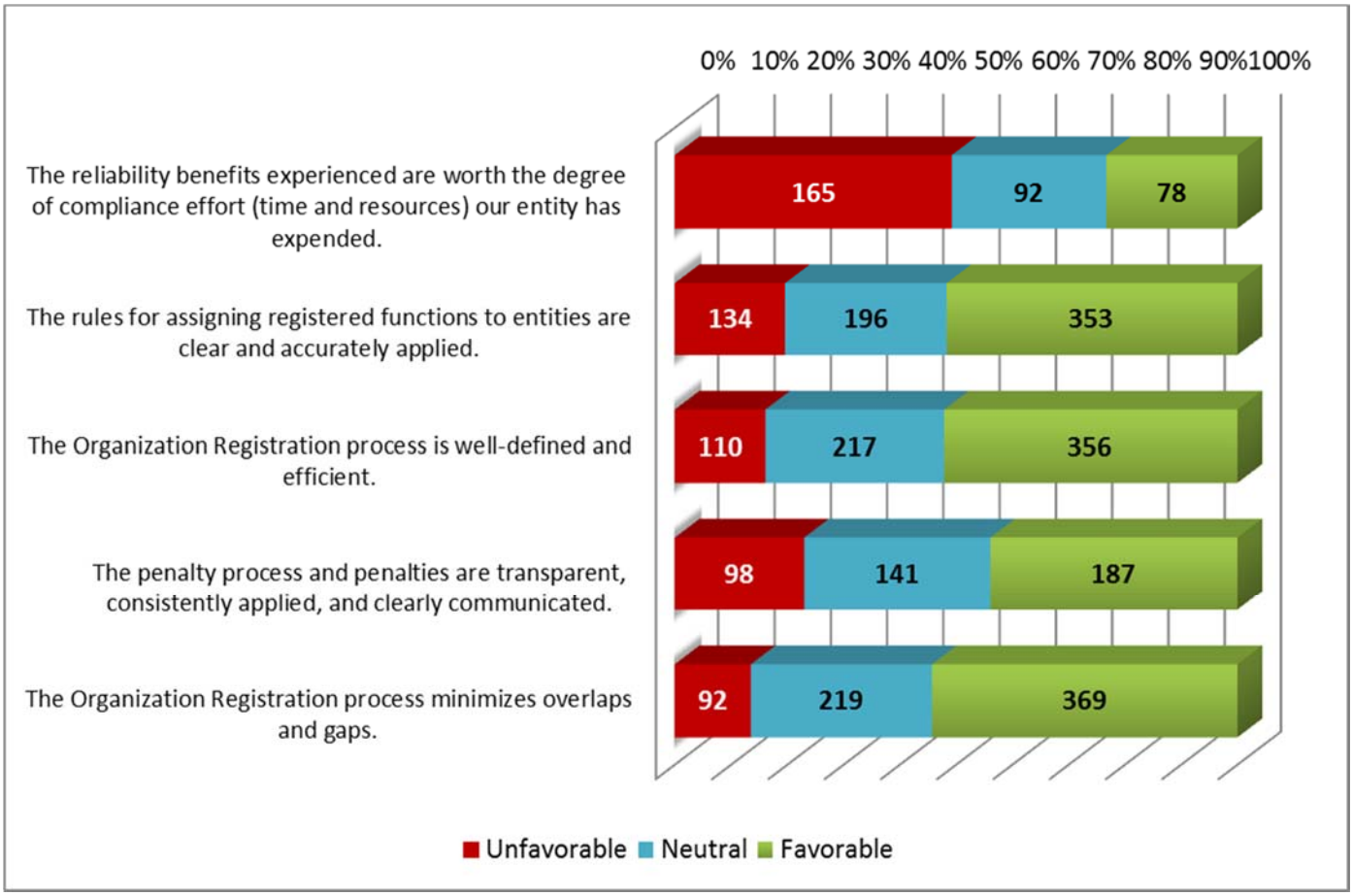
Favorability analysis allowed for additional insight into the strength of stakeholder perception through examination of the rating distribution. Responses across all Regions and NERC were re-coded as "Unfavorable" (rating of 1 – Strongly Disagree or 2 – Disagree), "Neutral" (rating of 3 – Neither Disagree Nor Agree), and "Favorable" (rating of 4 – Agree or 5 – Strongly Agree). Rank ordering of all items by those "Most Favorable," and by those "Least Favorable," highlighted items for further interpretation.

Across all Regions, the five items with the greatest number of favorable ratings (ranging from 84-89 percent) were in the Compliance Monitoring Topic Area. Conversely, the 5 items with the greatest number of unfavorable ratings (ranging from 14-49 percent) were in the Topic Areas of Compliance and Reliability Impact, Other, Enforcement Actions, and Organization Registration.

Most Favorable



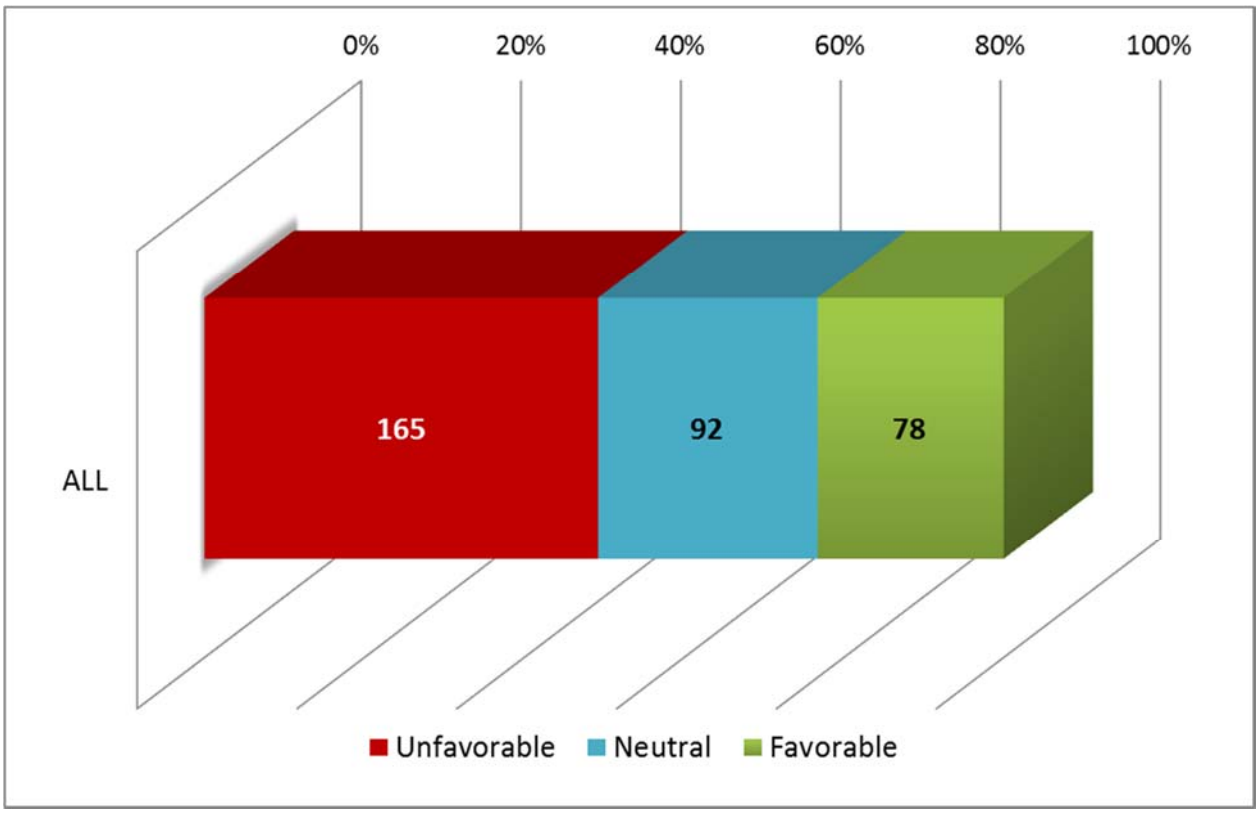
Least Favorable



Regional Favorability Analysis

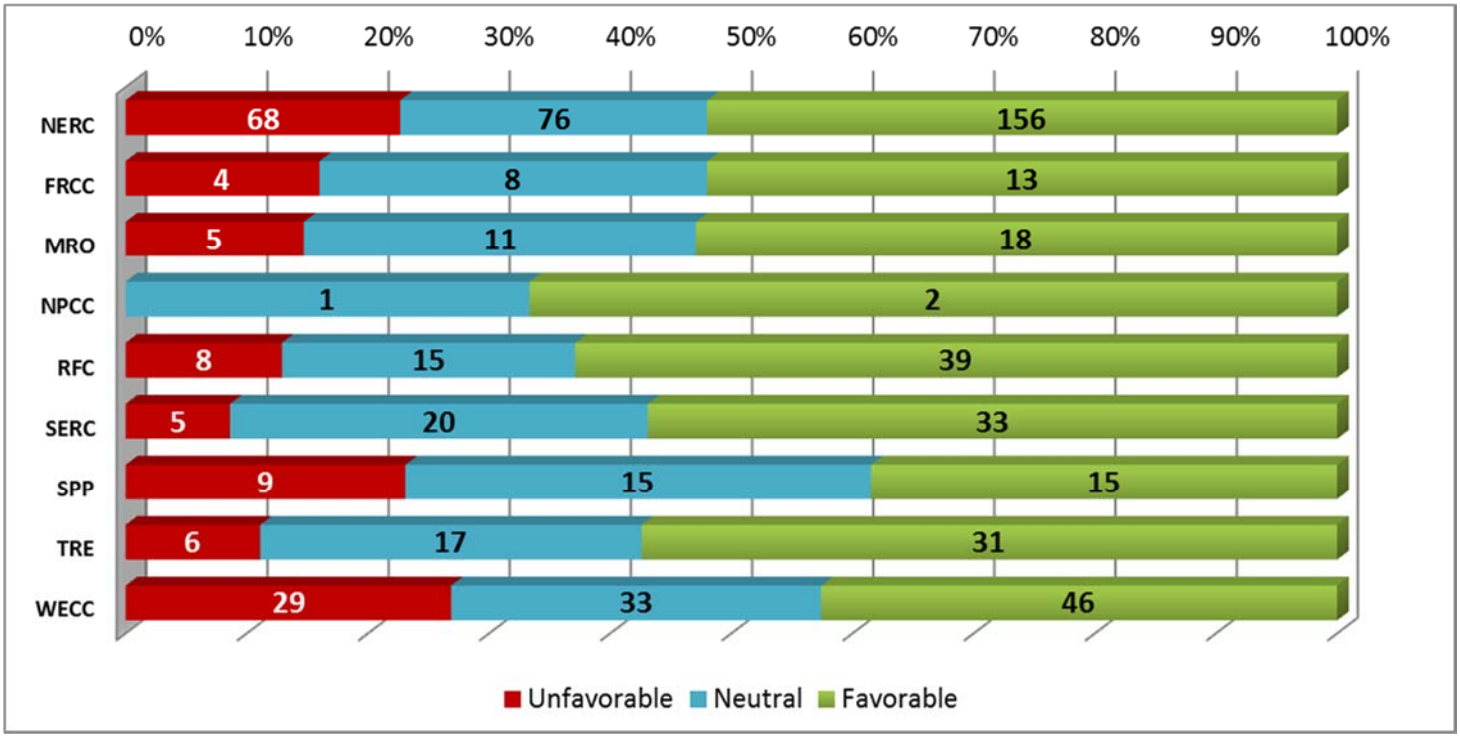
For the 5 least favorable items, a Region breakdown (where applicable) identified further variation.

"The reliability benefits experienced are worth the degree of compliance effort (time and resources) our entity has expended:"



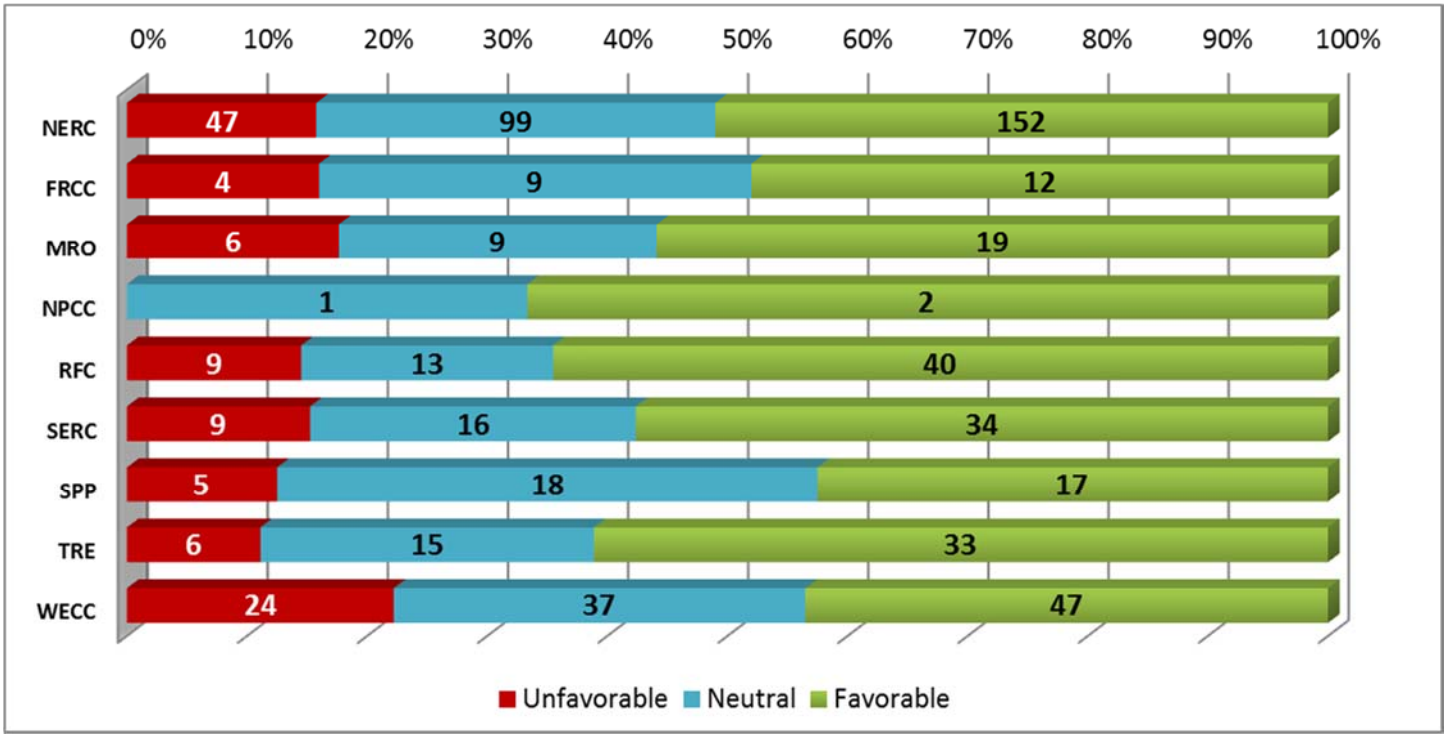
For this item, the average overall unfavorability is 49 percent.

"The rules for assigning registered functions to entities are clear and accurately applied:"



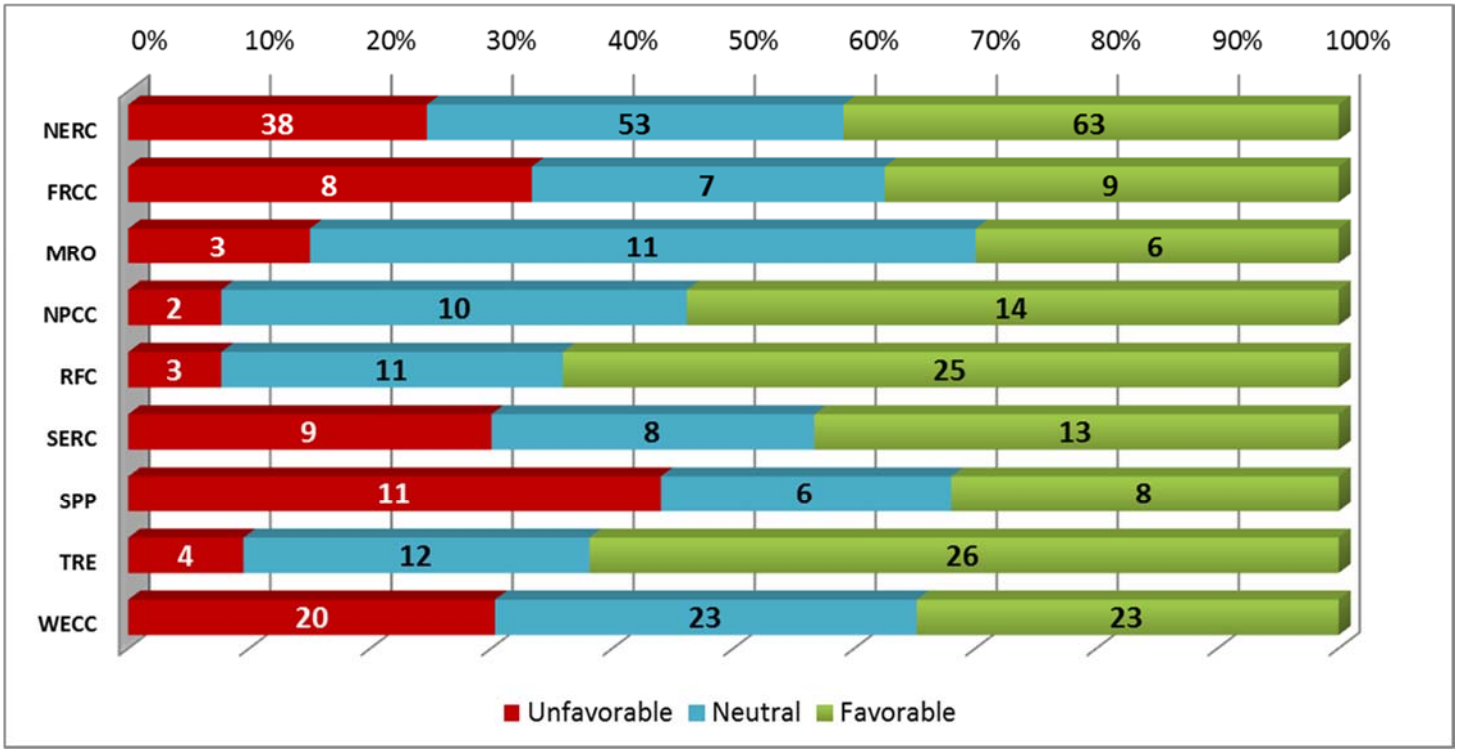
For this item, Regional comparisons identify WECC's 27 percent unfavorability the highest and NPCC's 0 percent unfavorability the lowest. Average overall unfavorability is 15.10 percent.

"The Organization Registration process is well-defined and efficient:"



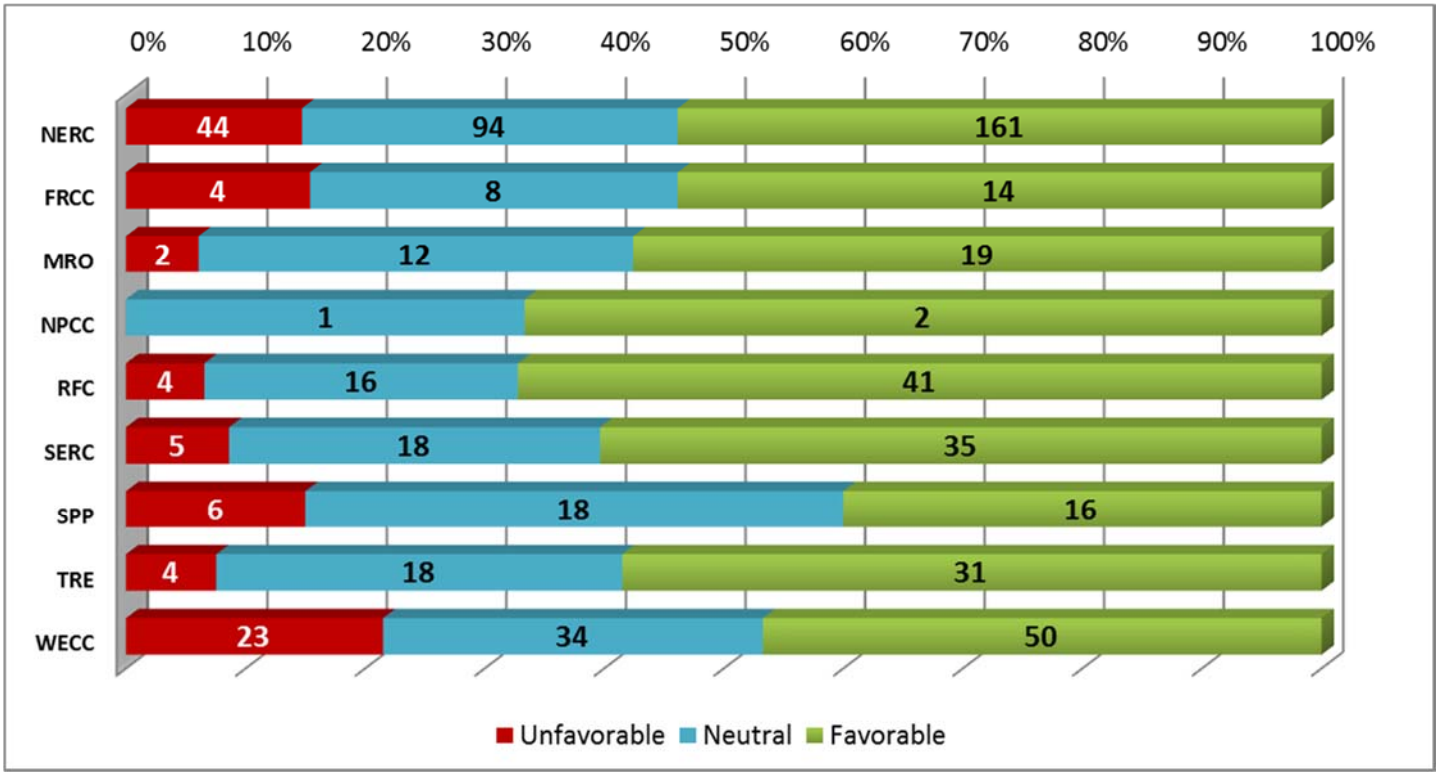
For this item, Regional comparisons identify WECC's 22 percent unfavorability the highest and NPCC's 0 percent unfavorability the lowest. Average overall unfavorability is 14 percent.

"The penalty process and penalties are transparent, consistently applied, and clearly communicated:"



For this item, Regional comparisons identify SPP's 44 percent unfavorability the highest and NPCC's and RFC's 8 percent unfavorability the lowest. Average overall unfavorability is 22 percent.

"The Organization Registration process minimizes overlaps and gaps:"

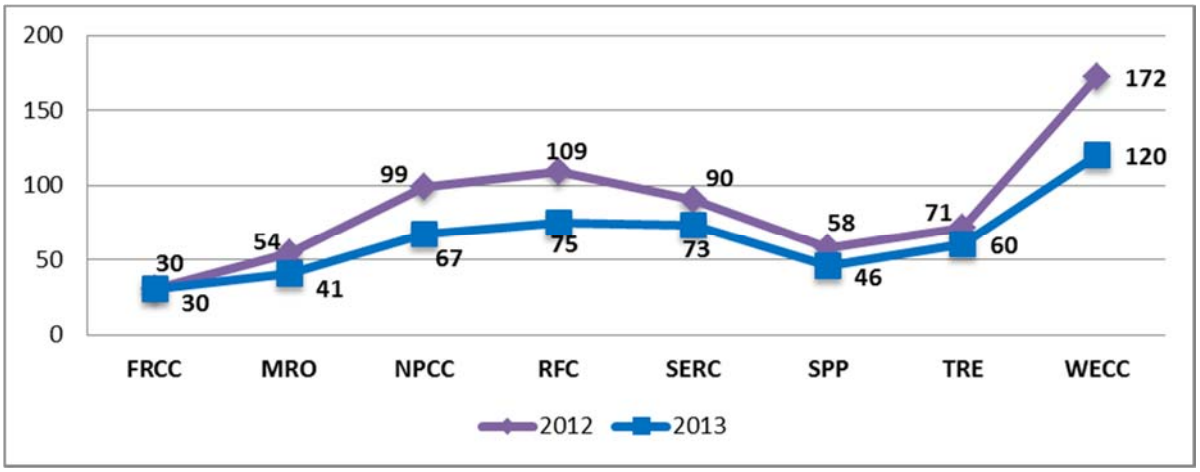


For this item, Regional comparisons identify WECC's 22 percent unfavorability the highest and NPCC's 0 percent unfavorability the lowest. Average overall unfavorability is 11 percent.

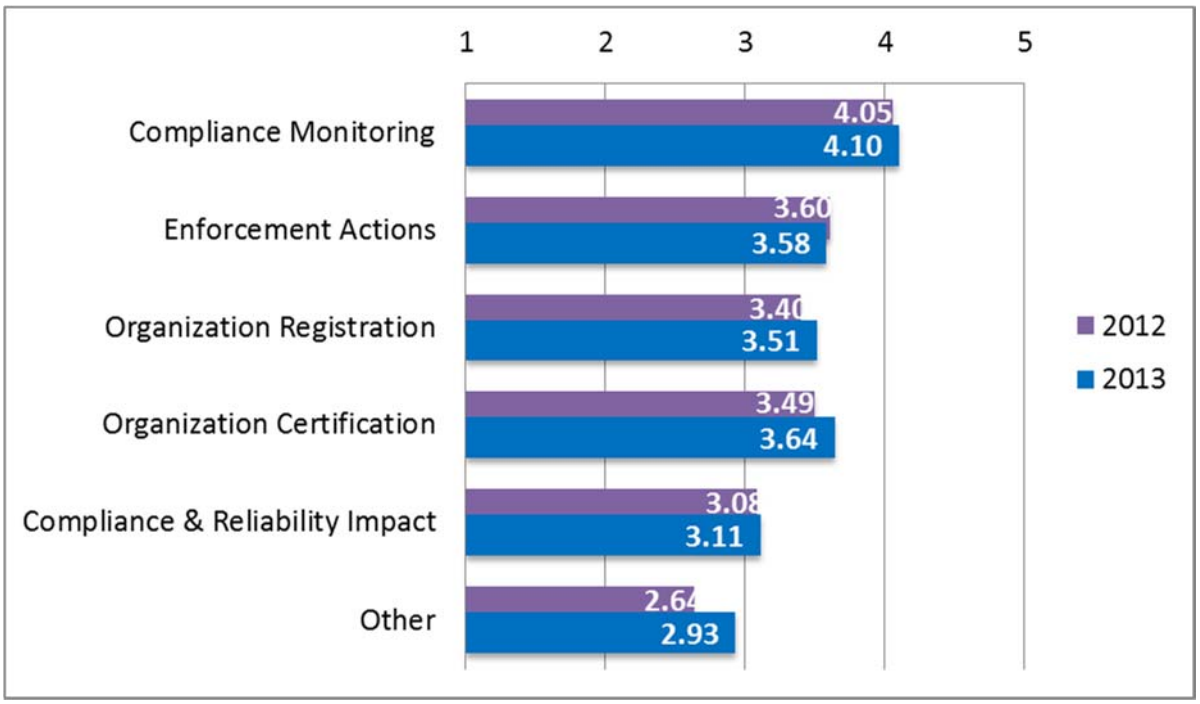
Year-over-year Analyses

New rating scale descriptors and extensive survey item updates in 2012 have previously constrained year-over-year analyses. However, 2013 survey items are an exact match from 2012 survey items, allowing a comparative year-over-year exploration of stakeholder perception.

Response Demographics: Region



Overall Averages by Topic Area

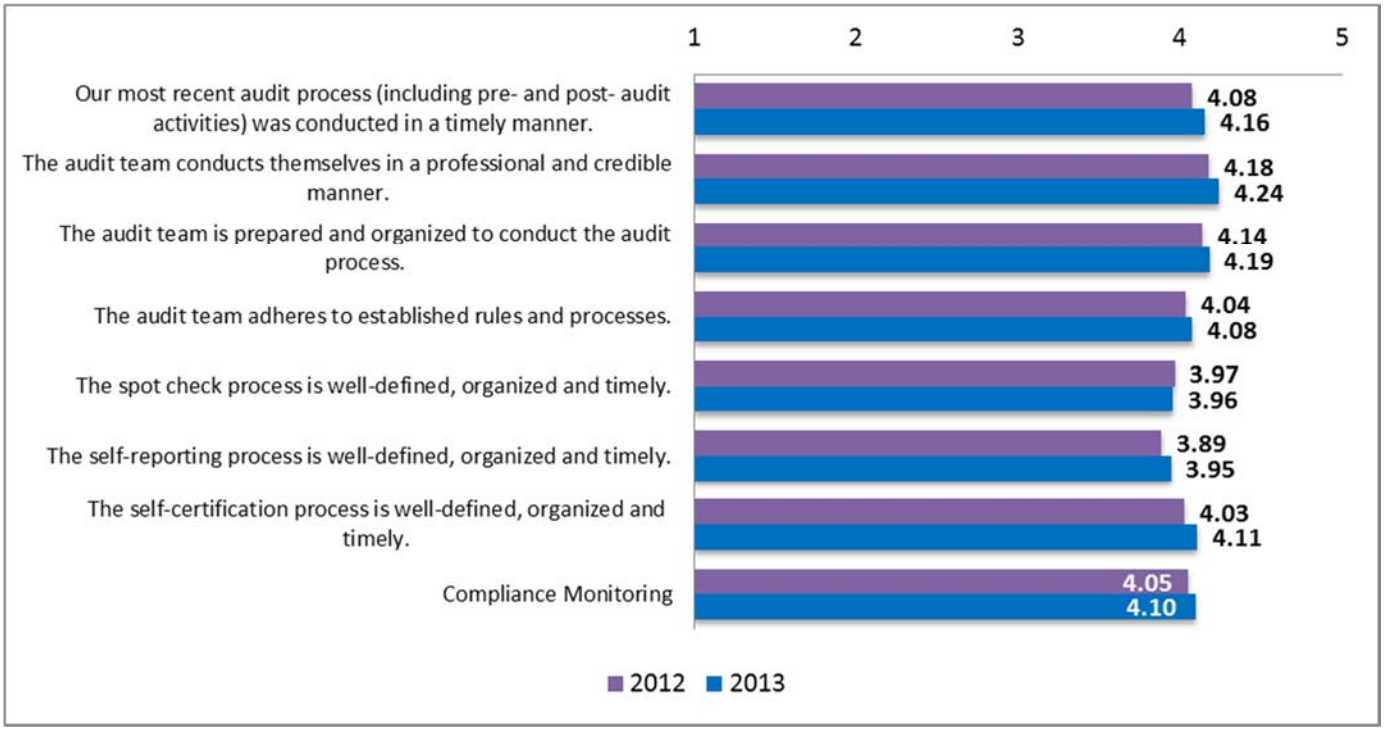


Consistent with 2012, Compliance Monitoring remains the highest rated Topic Area (4.10), increasing by .05. "Other" remains the lowest rated Topic Area (2.93), increasing by .29 as compared to 2012.

Year-Over-Year analysis did not yield any statistically significant differences between topic areas (p>.05).

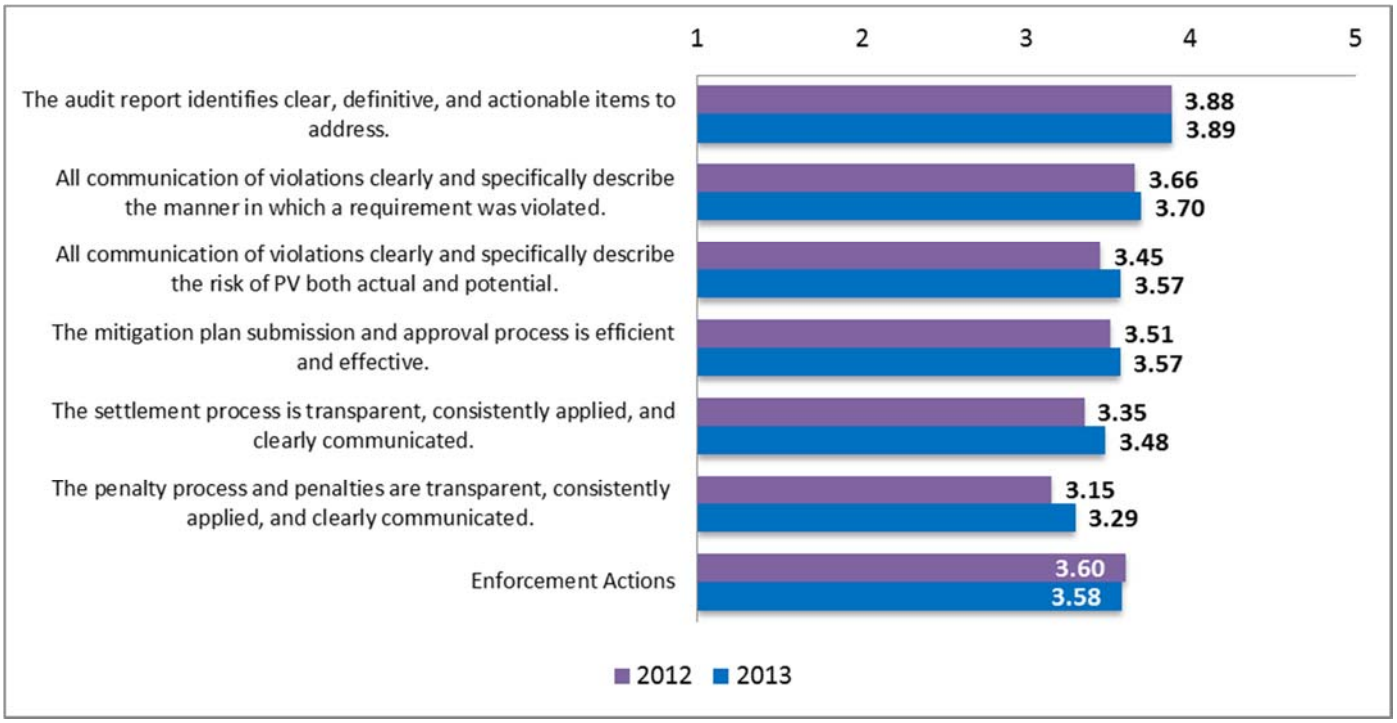
Compliance Monitoring

**Differences are not statistically significant (p>.05)*



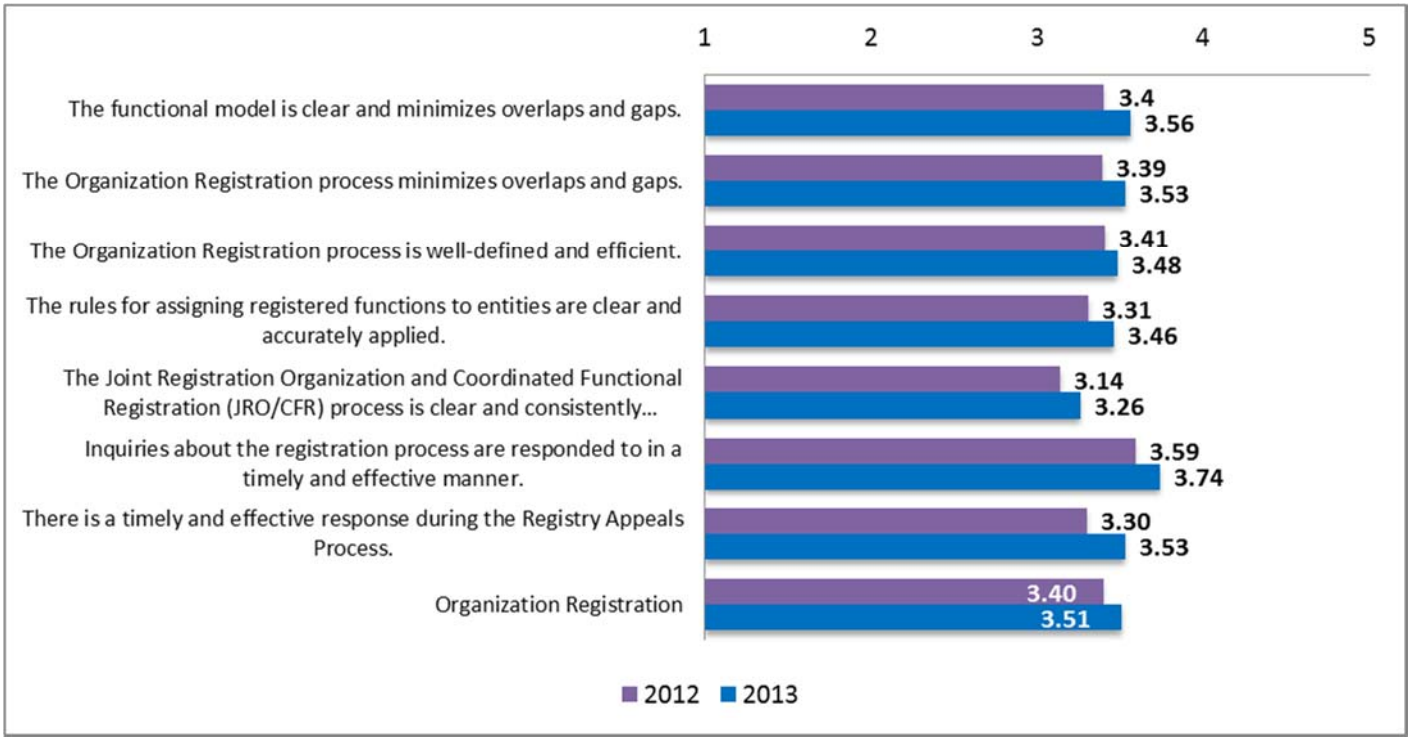
Enforcement Actions

**Differences are not statistically significant (p>.05)*



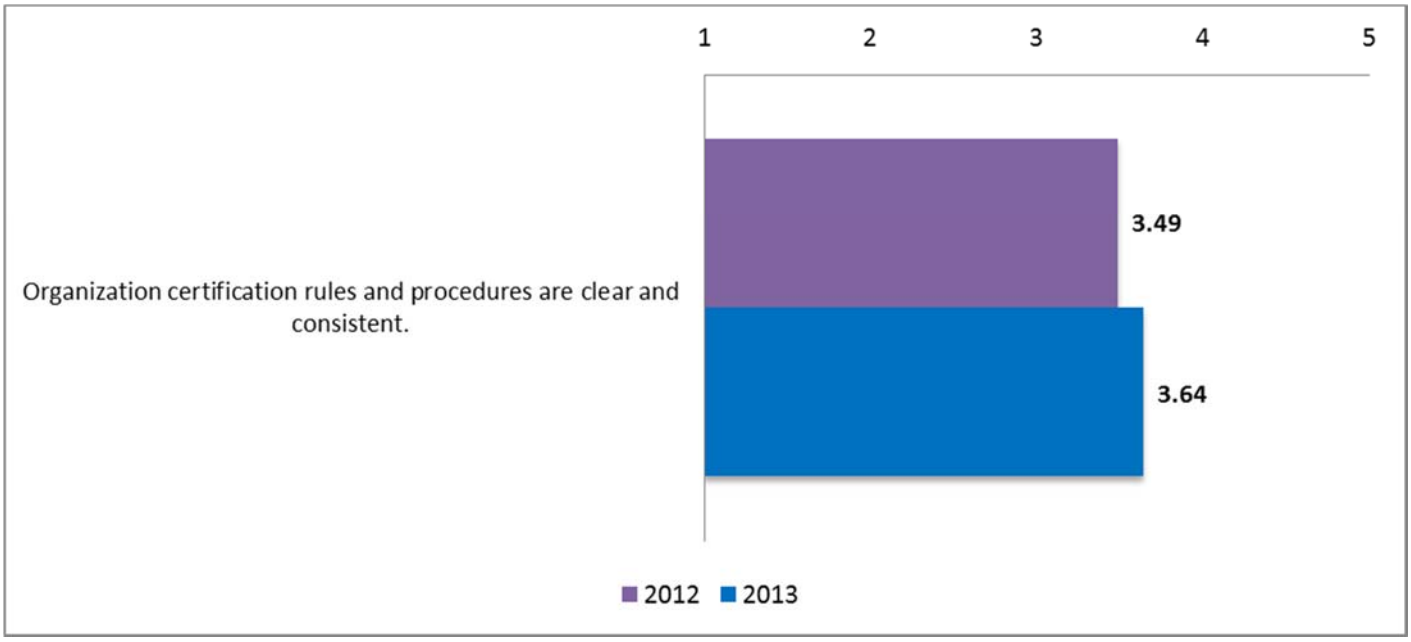
Organization Registration

**Differences are not statistically significant (p>.05)*



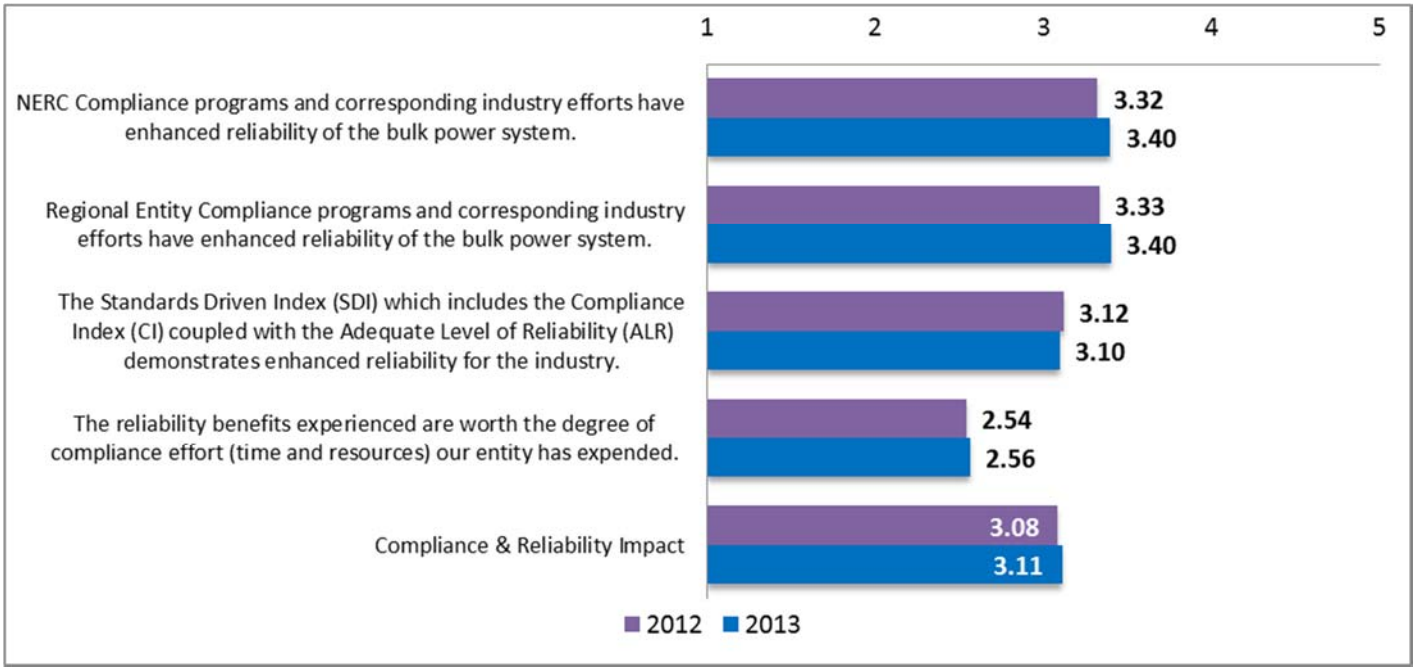
Organization Certification

**Differences are not statistically significant (p>.05)*



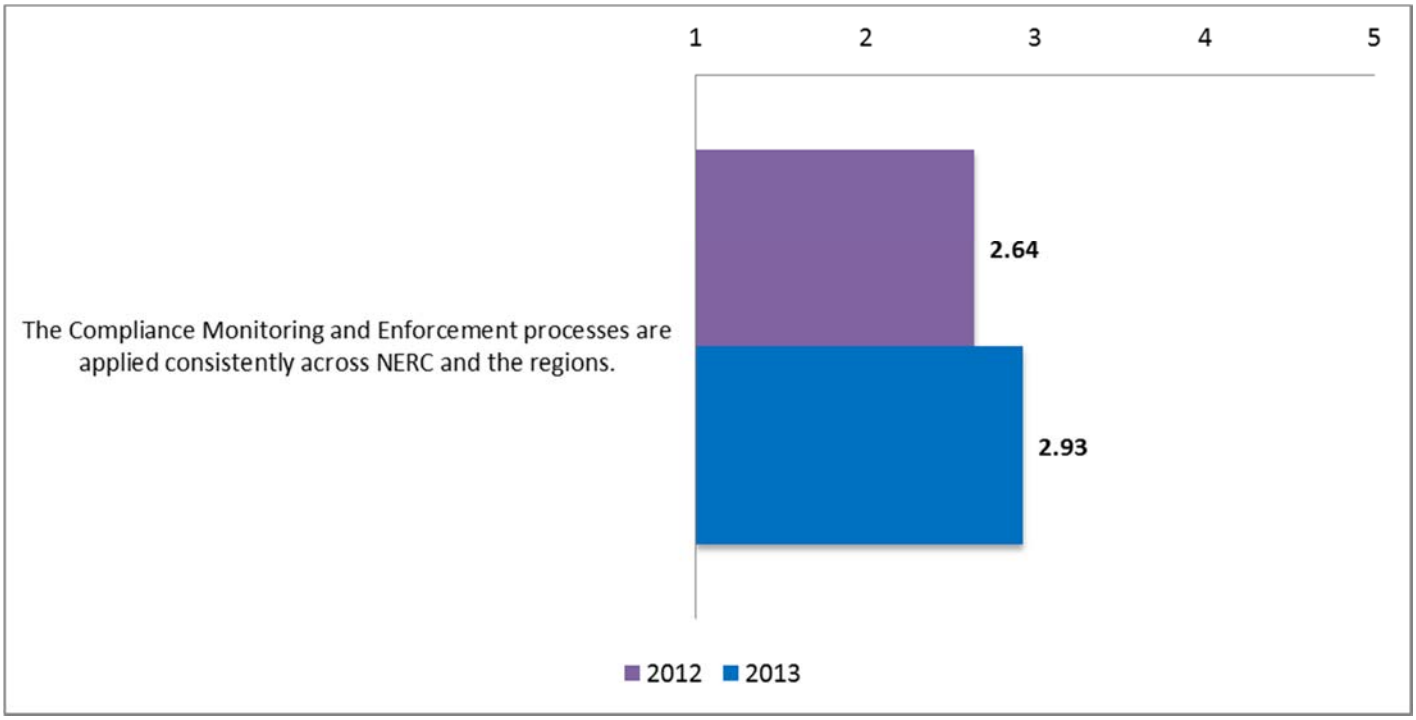
Compliance and Reliability Impact

**Differences are not statistically significant (p>.05)*



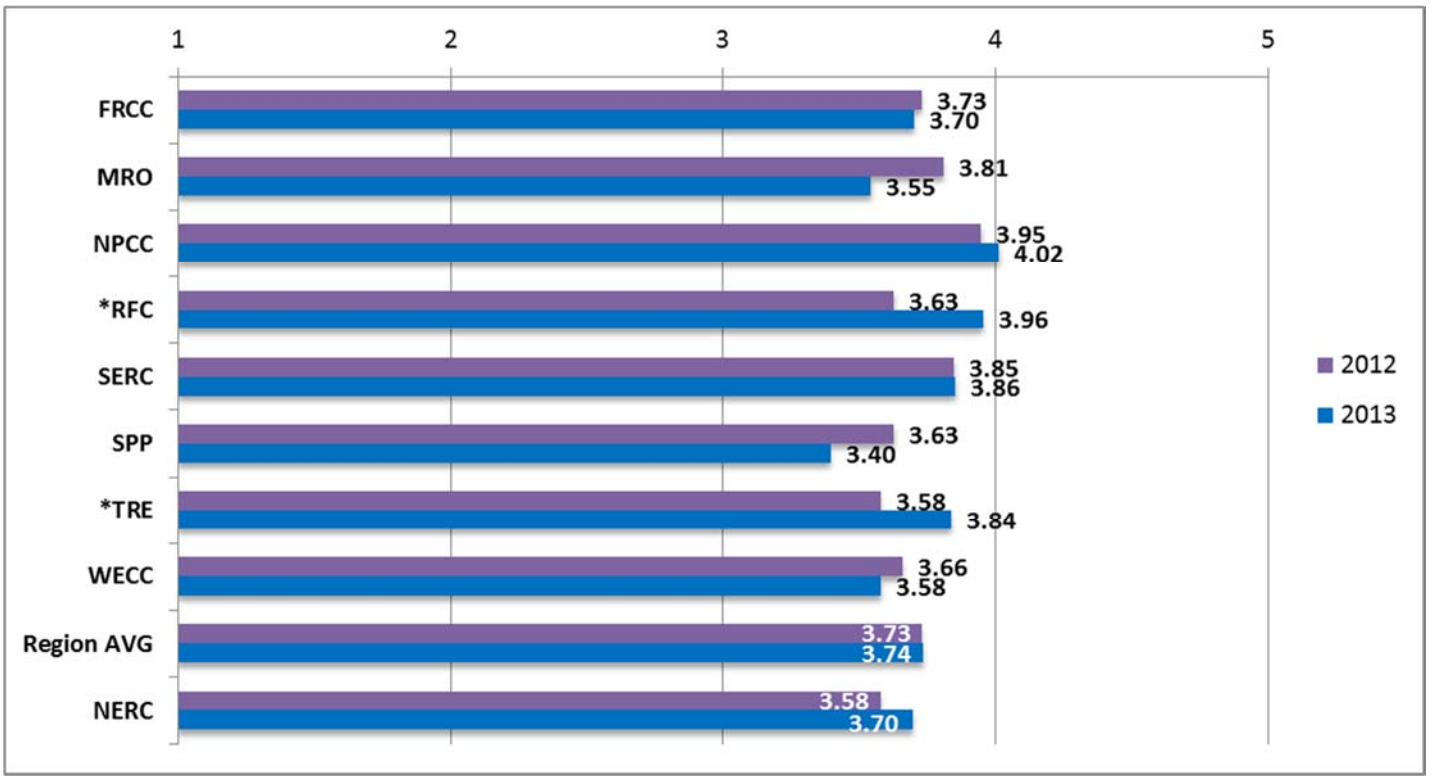
Other

**Difference in means are not statistically significant (p>.05)*



Overall Averages by Region

**Statistically significant difference (p<.05)*

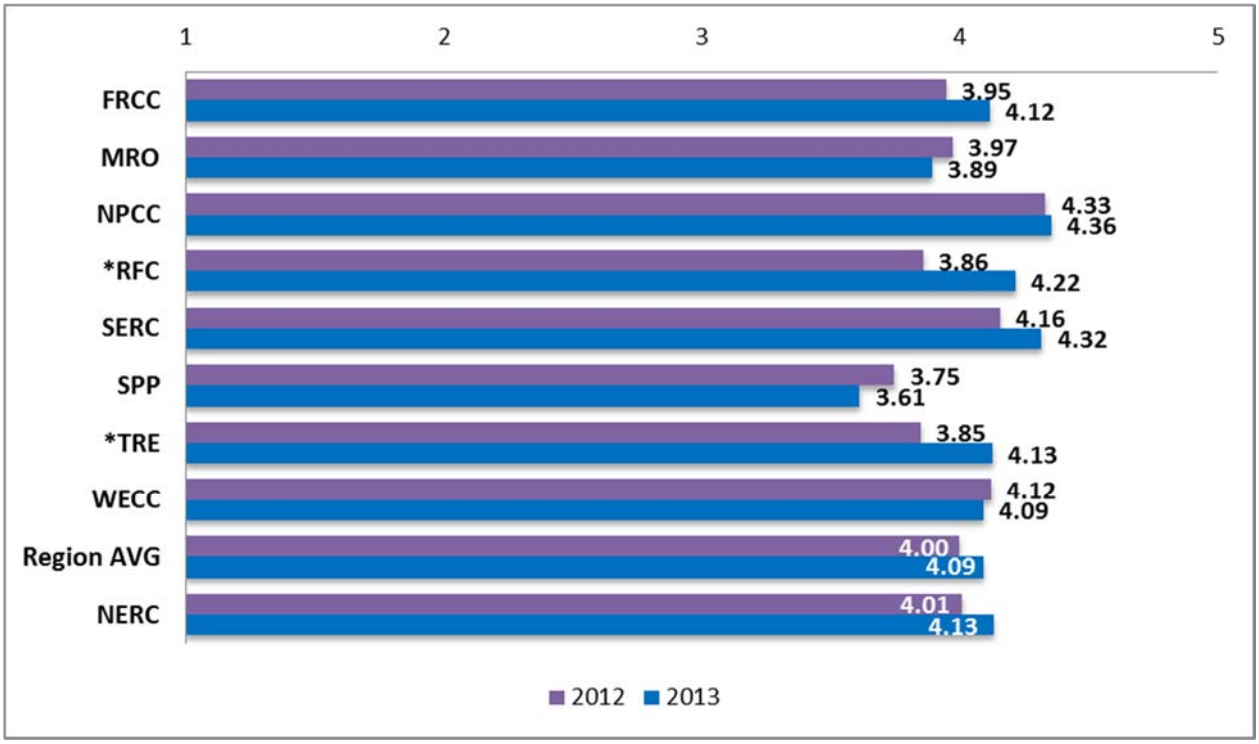


At the Regional level, 4 of the 8 Regions (NPCC, RFC, SERC, and TRE) averaged higher ratings overall as compared to 2012 with differences ranging from .01 to .33. Similarly, NERC as compared to the Regions, received .08 higher ratings than reflected in 2012. However, the overall Regional average remains consistent, reflecting only a slight increase of .01 when compared to 2012 ratings.

The RFC and TRE Regions both show statistically significant differences in their year-over-year overall response averages (p<.05).

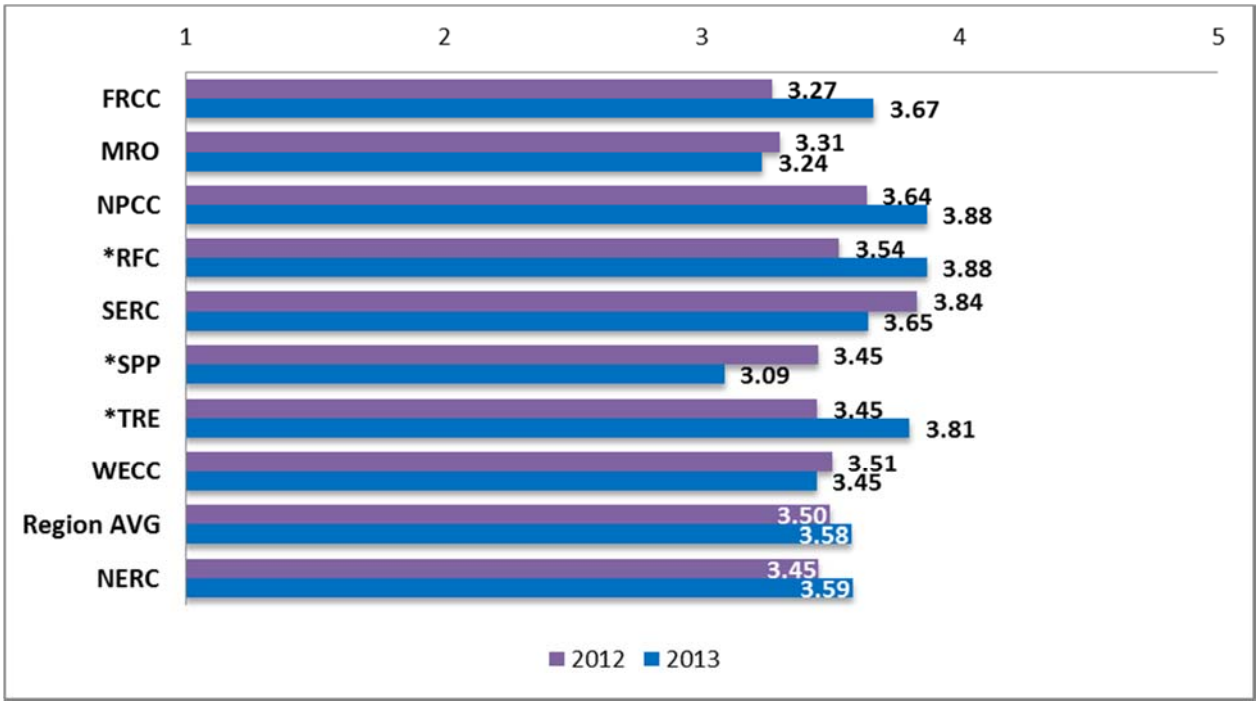
Compliance Monitoring

**Statistically significant difference (p<.05)*



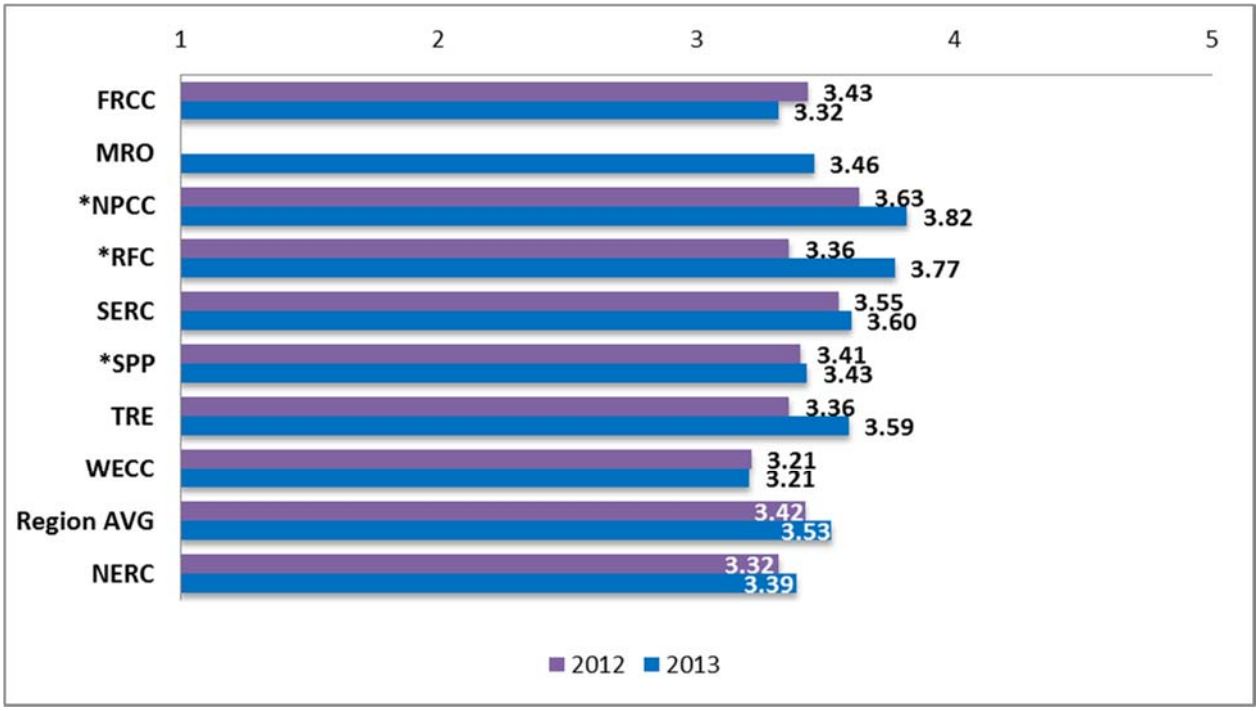
Enforcement Actions

**Statistically significant difference (p<.05)*



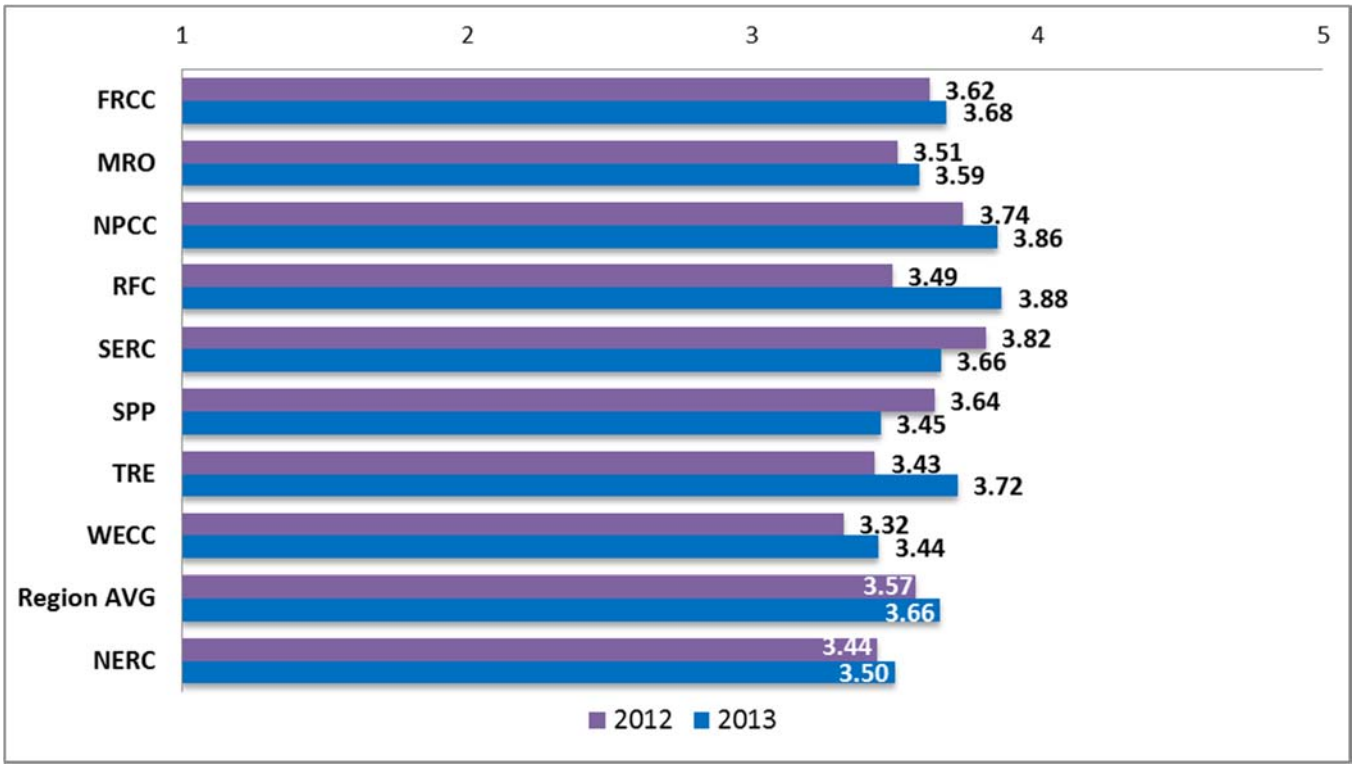
Organization Registration

**Statistically significant difference (p<.05)*



Organization Certification

**Statistically significant difference (p<.05)*



Comment Analysis

In the 2013 survey, open-ended responses underwent thematic qualitative analysis, creating objective output for interpretation. For each Topic Area and for the directed open-ended questions, all comments were coded thematically.

Stakeholder feedback focused on the following themes:

- Increased Consistency and Standardization:
  - In processes across Regions (Audit, Self-Reporting and Certification, Mitigation, the Functional Model, etc.)
  - In penalty application and the settlement process
  - In communications from NERC and RE's (portals, web links, etc.)
- Communication of Clearer, More Applicable Definitions:
  - In recertification processes
  - In JRO and CFR processes
  - In the BES
  - In valid reliability measure
- Greater Efficiencies via:
  - Increased process timeliness and feedback
  - Increased return on investment of compliance program
  - Continued streamlining of standards
  - Increased transparency

Compliance Monitoring

In both NERC and the Regions, leading themes in Compliance Monitoring referenced Auditor Inconsistencies and Self-Reporting/Certification.

THEME	NERC	RE
*Audit Inconsistencies	10	36
*Self-Reporting/Certification	15	23
Positive and Professional	2	11
Untimely Audits	2	9
Audit Feedback	2	4
Inappropriate and Unprofessional	1	3
Petty Fines	2	3
Standard Inconsistencies	2	3
Compliance Monitoring		2
Portal Consistency	2	2

THEME	NERC	RE
Process Inefficacies		2
Accountability		1
Limited to Regional Entity	1	1
Standards Development Process	1	1
Unjustified Costs	1	1
Contribution Clarity -WECC		1
Evidence Statements	1	
Increased Transparency and Consistency	2	
NERC Audit Guidance	1	

Auditor Inconsistencies – Sample Comments:

- "Overall our audit experiences have been favorable; however, in the past we have found inconsistencies, even within the same Region from auditor to auditor. We are in hopes that this will be eliminated by the auditor handbook."
- "This question will vary, depending on audit type. The 693 audits are well organized, well planned, and well executed. The CIP audits are not well organized, seemed to lack sufficient planning, and resulted in a somewhat chaotic environment. Also, the ever-changing CIP interpretations made compliance challenging."

Self-Reporting/Certification – Sample Comments:

- "The self-reporting process should be organized as a learning process for others instead of a punitive process."
- "The self-certification process has improved slightly, but needs to focus more on the BES that has a valid potential risk."
- "Recommend consideration of less frequent Self-Certifications and Data Submittals for smaller entities."

Enforcement Actions

In both NERC and the Regions, leading themes in Enforcement Actions referenced Settlement and Penalty Process and Consistency/Standardization.

THEME	NERC	RE
*Settlement and Penalty Process	17	37
*Consistency/Standardization	12	22
Mitigation	8	17
Transparency	5	16
Communications	4	11
FFT/FFR Implementation	3	1
Untimely Approval	1	7
Feedback		5
Positive and Professional		2
Accountability		1
Audit Report		1
Compliance		1

Settlement and Penalty Process – Sample Comments:

- "The settlement and penalty processes are not transparent. When more than one requirement is included in the settlement agreement, the penalty assessment is not defined and the calculation is not clear."
- "The audit report is overloaded with legal boilerplate, which may obscure improvement opportunities. Rules of Procedure are clear on mitigations, but mitigation of the immediate problem vs the underlying causes is variable. Settlements on the surface are transparent and end up being well documented, but never sure how they are going to turn out. Penalties seem to drift between the NERC VSL/VRF Penalty Table, and the FERC Sanction Guidelines; never sure which way an issue is going to lean, but prefer the structured approach of the FERC guidelines."

Consistency/Standardization – Sample Comments:

- "Audit team findings are not necessarily identical to Enforcement team findings."
- "Enforcement varies from Region to Region. WECC has applied more penalties and stiffer fines than the other Regions."
- "The audit process should be an open book test. It should have clear expectations of compliance. If I don't have clear expectations of compliance, how can the enforcement process be fair and impartial? If I don't understand what I've violated, I can't fix it or prevent reoccurrence."

Organization Registration

In both NERC and the Regions, leading themes in Organization Registration referenced Definitions/Clarity, Functional Model and Consistency/Standardization.

THEME	NERC	RE
*Definitions/Clarity	16	10
*Functional Model	9	9
*Consistency/Standardization	10	5
Feedback	3	4
Deregistration	4	4
Clear and Efficient	1	3
Overlaps/Gaps	5	3
Burdensome	5	2
Communications	2	2
GO/GOP/TO/TOP	3	2
Accountability	1	1
Process Improvement	1	1
Applicability	2	
BES	2	

Definitions/Clarity – Sample Comments:

- "The Planning Authority, Planning Coordinator function is not well-defined. There are gaps in registration and smaller entities are registered but should not be as they should be included in a larger Planning Coordinator Area."
- "The rules for assigning registered functions are not clear with information sprinkled in various documents. It is difficult to discern what is needed. The only saving grace is that inquiries on the process are quickly responded to. Discussion with the Regional Entities is necessary to understand the rules."

Functional Model – Sample Comments:

- "We believe the functional model is clear; however, it can create some confusion when you begin to apply it to certain standards, particularly the earlier versions of the Standards."
- "The function model was created back in early 2000s. Needs revamping. The original effort was to develop functions that an entity could perform. However the standards cross so many of these functions, confusion occurs within a utility of which function is connected to which requirement."

Consistency/Standardization- Sample Comments:

- "Registration criteria is not consistently applied in comparing other Regions. Request for transfer of registration function from one entity to another has not been addressed after multiple contacts."
- "Inconsistencies by RE personnel in different Regions. Complicated processes make registered entities look for ways not to use ROP options for ORC."

Organization Certification

In both NERC and the Regions, the leading theme in Organization Registration referenced Definitions/Clarity.

THEME	NERC	RE
*Definitions/Clarity	6	7
Re-Certification	2	3
Feedback		2
Deregistration	1	1
Efficient	1	1
BES		1
Consistency/Standardization	1	
Functionality	2	
Process Improvements	1	

Definitions/Clarity- Sample Comments:

- "The re-certification efforts need to be defined. E.g., what is the criteria that NERC uses to conduct a re-certification of an RC, TOP, BA."
- "At a RRO meeting, the Organization Reorganization function gave global examples of when to notify the Organization Reorganization Department of changes applied by the entity. The examples were too broad, not clear and not concise. The group should provide a procedure/program defining for the entity when the Organization Registration Department should be contacted for changes in the entity's function."
- "The Certification process is seemingly unknown even to the Regional Entity. Re-certification triggered by the NERC Rules of Procedure has apparently been in place for years, so it is unclear why the Regional Entity has no more understanding of what is entailed than the registered entity seeking re-certification. Perhaps some more detailed guidance from NERC would be beneficial."

Compliance and Reliability Impact

Comments regarding Compliance and Reliability Impact were gathered at the aggregate level and leading themes included Return on Investment and Reliability Standards.

THEME	#
Return on Investment	38
Reliability Standards	18
Administrative Issues	8
Compliance and Enforcement	7
Small Entities	6
Reliability Assurance Initiative	5
Risk Based vs. Zero Tolerance	3
Reliability Improvements	3
CIP Standards/Auditing	3

THEME	#
Consistency Complications	2
Reliability Metrics	1
Quantitative Results	1
Penalties	1
Independent Reliability Monitor	1
Deregulation	1
Cultural Alignment	1
BPS Reliability	1
BES Reliability Metrics	1

Return on Investment- Sample Comments:

- "While we agree that reliability of the bulk electric system has been enhanced to some degree, the enormous effort and associated costs that have been expended on things with no incremental benefit to the BES has drained resources from areas that are resource poor to begin with."
- "Agencies are spending much more time on Compliance Documentation and it is taking time from operators actually performing reliable operations of the Bulk Electric System."
- "The effort to ensure adequate documentation is excessive for our entity. The reliability effort is the same but documenting such is a burden."

Reliability Standards – Sample Comments:

- "The main focus of most conversations around the Reliability Standards now are what are the compliance implications and how will compliance be measured and not what will the reliability benefit be from a particular standard."
- "Our entity has been pushed to some "best practices" that were not previously done, but the overall impact on reliability is negligible at best."
- "While there have been improvements with regard to the reliability benefits experienced overall, there is still much work to be done to ensure that the Standards in effect truly do (or may) have a material impact to the operations of the BES. Those Standards that do not have a material impact to the reliability of the BES should be eliminated."

Recommendations: ERO-CMEP

Recommendations regarding the ERO-CMEP were gathered at the aggregate level and leading themes included Reliability Assurance Initiative and Focus on Reliability/Security.

THEME	#
Reliability Assurance Initiative	9
Focus on Reliability/Security	5
Audit Efficiency	4
Consistency	4
Risk Based vs. Zero Tolerance	4
Compliance Monitoring/Transparency	3
Target Due-Date Consistency	2
FFT Processing	1
Focus on Compliance and Enforcement	1
Process Improvement	1
Reliability Standards Program	1
Reporting Efficiency	1
Identify, Assess, Correct	1
Training	1

Reliability Assurance Initiative- Sample Comments:

- "Recommend diligent completion of development and implementation of the Reliability Assurance Initiative (RAI), particularly with regard to the impact on smaller entities, since the RAI appears to be headed in the right direction."
- "The RAI should try to maintain the focus on managing/mitigating reliability risk, providing consistency across the N.A. footprint and distinguishing between the reliability standards that maximize reliability assurance from those that are not as critical to that assurance."
- "The concern is with the level of effort around implementation of the RAI, specifically the Internal Controls. The White Paper guidance and the Internal Controls Working Guide appear inconsistent with statements by NERC that the RAI process would be less onerous. A more clear direction needs to be provided."

Focus on Reliability/Security- Sample Comments:

- "We need to facilitate a culture of reliability/security excellence. Where we all work together to keep this machine and all its parts rolling."
- "The process is too punitive and not necessarily geared toward improving reliability. We can't openly share potential reliability gaps for fear of retribution."
- "Provide better information about cyber security violations in the form of lessons learned around specific compliance issues that will enhance reliability."

Recommendations: Regional Entities

Recommendations regarding the Regional Entities were gathered at the aggregate level and leading themes included Collaboration/Consistency and Audit Standardization.

THEME	#
Collaboration/Consistency	17
Audit Standardization	4
Transparency	1
SPP RE Trustee Effectiveness	1
Reporting Improvements	1
Region Principles	1
RE Understanding	1
RE Praise	1
Focus on Reliability/Security	1
FFT Improvements	1
CDAA Improvements	1
Board Expansion	1
Audit Training	1

Collaboration/Consistency – Sample Comments:

- "There should be more collaboration and consistency between the Regions."
- "The Regions need to be consistent regarding JRO's, audit practices, and compliance requirements relative to documentation required, method of submittal, etc. It would be helpful if the Regions settled on one portal."
- "Recommend continued emphasis on achieving uniformity across Regions under the direction of NERC."

Audit Standardization – Sample Comments:

- "More standardization in the 'audit approach' would be very welcome."
- "Regional entities should work to standardize expectations, timelines, and interpretations of standards. This will minimize the efforts for entities to 'prove compliance' verses focusing on what will make the system more reliable and safe for all customers of the bulk electric power system."
- "We would like to have a single audit where SERC is the lead to cover us for audits in RFC. Our last audit for RFC consisted of a single requirement that really didn't apply to us. Seemed extremely unnecessary."

Inconsistencies across Regions

Comments regarding inconsistencies across Regions were gathered at the aggregate level and leading themes included Regional Inconsistencies and Audit Inconsistencies.

THEME	#
Regional Inconsistencies	23
Audit Inconsistencies	15
Standards	4
Compliance Monitoring	3
Portal Inconsistencies	3
Self-Certification	3
CMEP Schedules	1
Interpretation Clarity	1
CIP	1
Department Inconsistencies	1
Settlement Process	1

Regional Inconsistencies – Sample Comments:

- "Hearing from other entities that operate in other Regions or multiple Regions, they indicate there is a definite inconsistency within the Regions regarding application of NERC Reliability Standards."
- "There continue to be inconsistencies across the Regions regarding the enforcement process."
- "Just look at PRC-005 and VAR-002 violations across the Regions. You will see varying amounts of penalties going back to 2007. In defense of the Regions, it is difficult to be consistent with some many variable to consider. Some degree on inconsistency is to be expected, but the gap is too wide today."

Audit Inconsistencies – Sample Comments:

- "There are significant differences in the way CIP audits are being conducted in the SPP Region versus other Regions. The SPP CIP audits are going above and beyond the purview of the Standards. The SPP CIP auditors are auditing to best practices and not auditing to the letter of the Standards."
- "We have been told during workshops and audits that different auditors may reach different conclusions. That is an admission of inconsistency."
- "While there are many areas of consistencies across the Regions, each audit takes on its own persona based on the makeup of the team and especially if there are NERC and FERC observers."

Conclusion and Recommendations

Conclusion

The 2013 Stakeholder Perception Survey illustrated positive trends in all year-over-year evaluations, indicating industry's view of continued enhancements to ERO Effectiveness. Industry's relative perceptions of program strengths and opportunity areas were delineated through quantitative and qualitative analysis.
Industry feedback of strengths included:

- Compliance Monitoring components involving audit teams, audit processes, and self-certification.
- Positive progress by NERC and the Regions between 2011 and 2012 across all program areas, with a 38 percent increase in perceptions of NERC around Compliance Monitoring and Enforcement Actions.

Industry feedback for improvement included the themes:

- Increased consistency and standardization (in processes across Regions, in penalty application and the settlement process, and in communications from NERC and REs).
- Communication of clearer, more applicable definitions (in the recertification processes, in JRO and CFR processes, in the BES, and in valid reliability measure).
- Greater efficiencies (via increased process timeliness and feedback, increased return on investment of compliance program, continued streamlining of standards, and increased transparency).

2013 Recommendations

Through analysis and interpretation of the 2013 Stakeholder Perception Survey, the CCC has decided to recommend that NERC continue to move forward with the 2012 recommendations which are tied to the three themes that have prevailed over the past three years the survey has been conducted.

1. ROI of compliance program;
2. Inconsistencies within and across Regions; and
3. Transparency of the enforcement and penalty processes. In addition to recommendations below, NERC should address the specific conduct concerns that were presented in some of the comments.

These concerns have been presented to NERC under separate cover.

1. The CCC should continue to work with NERC staff to communicate the survey results in a productive way to NERC and the Regions to facilitate performance improvement and positively impact stakeholder perceptions.
2. The recommendations provided in the 2011 Stakeholder Perceptions Survey specifically included items to address ROI (recommendation number one) and transparency (recommendation number four). NERC should compile a new list of action items based on this 2012 survey and those provided in the 2011 survey. The CCC should have a standing item on its agenda for the next year to review NERC's progress on its action plan, offer assistance where requested, and work with NERC to communicate its successes to improve the results of future surveys.
3. NERC should review key/identified post-audit processes (audit reports, mitigation plans and settlements) with the objective of standardizing the process across Regions, streamlining components, and reducing the total process time.
4. NERC staff should review the free form written responses to the survey to identify the predominant consistency issues and develop an action plan to address.
5. NERC should implement a Multi-Region Registered Entity (MRRE) process by the end of 2013 (this was also addressed in the 2011 survey recommendations).

The CCC thanks the industry for their participation and the feedback provided in the survey. The CCC also wants to recognize NERC's support in facilitation of the CCC Stakeholder Survey, and its provision of an outside consultant to drive survey enhancement. The CCC requests that the NERC Board consider releasing a public version of the report.

REMG
REGIONAL ENTITY MANAGEMENT GROUP

STACY DOCHODA – FRCC | ED SCHWERDT – NPCC | SCOTT HENRY – SERC | LANE LANFORD – TRE
DAN SKAAR – MRO | TIM GALLAGHER – RFC | RON CIESIEL – SPP | CONSTANCE WHITE – WECC

Date: April 7, 2014

To: NERC Board of Trustees

From: Carter B. Edge, Director of REMG Coordinated Activities

Cc: Regional Executives

Subj: Regional Entity Management Group (REMG) report for the May NERC Board Meeting

Dear Trustees:

The Regional Entities continue to believe that our individual success should be measured by our collective success. To that end, leading up to the 2014 ERO Enterprise Metrics, we have been collaborating together and with NERC staff to complete work necessary to:

- File the 5-year ERO assessment
- Implement reforms under the Reliability Assurance Initiative (RAI) in a coordinated and consistent manner
- Conduct ERO-wide staff training on the Compliance Auditor Manual

Some efforts and accomplishments in these areas include:

- Development of a joint regional self-assessment as Attachment 2 to the *Five-Year Electric Reliability Organization Performance Assessment Report*. This assessment, with appendixes describing the Regional Entities' responses to specific concerns raised in the Commission's September 16, 2010 order on the Three-Year ERO Performance Assessment, as well as, how each region satisfies the applicable statutory and regulatory criteria for continued certification as part of the ERO, shows how NERC and the Regional Entities have coordinated over the period into an ERO Enterprise. Efforts, going forward, to improve enterprise operations with NERC will be around (1) clarifying and refining roles and responsibilities; (2) coordinating strategic planning and operational decision-making; (3) continuing to improve consistency; (4) sharing tools and infrastructure for delegated functions; and (5) coordinating communications.
- Preparation for execution of reforms under RAI began last year with the development of the 2014 ERO Compliance Monitoring and Enforcement Program required under the NERC Rules of Procedure. The 2014 ERO CMEP Implementation Plan is now a single, consolidated plan that aligns with the RAI and supports efforts toward a risk-based approach to compliance monitoring. It is important to note that 2014 is a transition year and that modifications to CMEP processes will occur across the ERO Enterprise to capture ongoing RAI efforts and project results that affect CMEP activities during the implementation year in a coordinated and consistent manner. The convergence of RAI pilot activity is an example. Specific guidance on CMEP activities will be provided throughout the 2014 implementation year and it is anticipated that more consistent, standardized processes will be implemented during the 2015 cycle.

- An ERO audit checklist and associated auditor handbook as a basis for enhancing Regional Entity audit practices, audit consistency, and auditor skills was developed late last year. A training program around these tools has started for ERO audit staff with specific auditor capabilities and competencies supporting the sustainment of ERO staff skills on a going forward basis.

BES Implementation

With the Commission approval of a revised Bulk Electric System definition, reliability will be improved by focusing activities on core facilities that are necessary for operating the interconnected transmission network. The definition provides clarity (when applied consistently) to those who are responsible for performance under the Reliability Standards around what is considered Bulk Electric System.

While the majority of the industry's effort should be focused on applying the revised definition to their asset inventory, the Regional Entities and NERC have developed corresponding enterprise-wide practices and an online application called the BES Notifications and Exceptions tool (BESnet) to support requests for exceptions to the definition. The BESnet provides a consistent way for entities to make notifications of changes to Bulk Electric System assets that affect their responsibilities for compliance with the Reliability Standards and to submit requests for a case-by-case determination of exception. The BESnet allows the ERO Enterprise to manage this workflow in an efficient and effective manner. Regional Entity staff will be the initial reviewers of notifications and exception requests and all eight regions have been actively engaged in developing consistent practices for these reviews.

Reference documents and training will continue to be developed and delivered leading up to the July 1, 2014 effective date to assist industry with the transition and ERO staff in consistently applying the definition and processes across the regions. These materials and schedules for training and outreach activities can be found on the NERC website.

OPEN DISTRIBUTION

April 7, 2014

NATF Report for NERC Board of Trustees (BOT) – May 2014

- NATF / NERC Coordination Progress:
  - 345 kV Breaker Performance (see attached)
  - Protection System Mis-operation
  - Sharing of NATF Modeling Documents
  - EMS (Situational Awareness) Performance
  - FAC Rating Alert – Best Practices for ongoing ROW Maintenance
  - Security / Physical and CIP V5 Practices

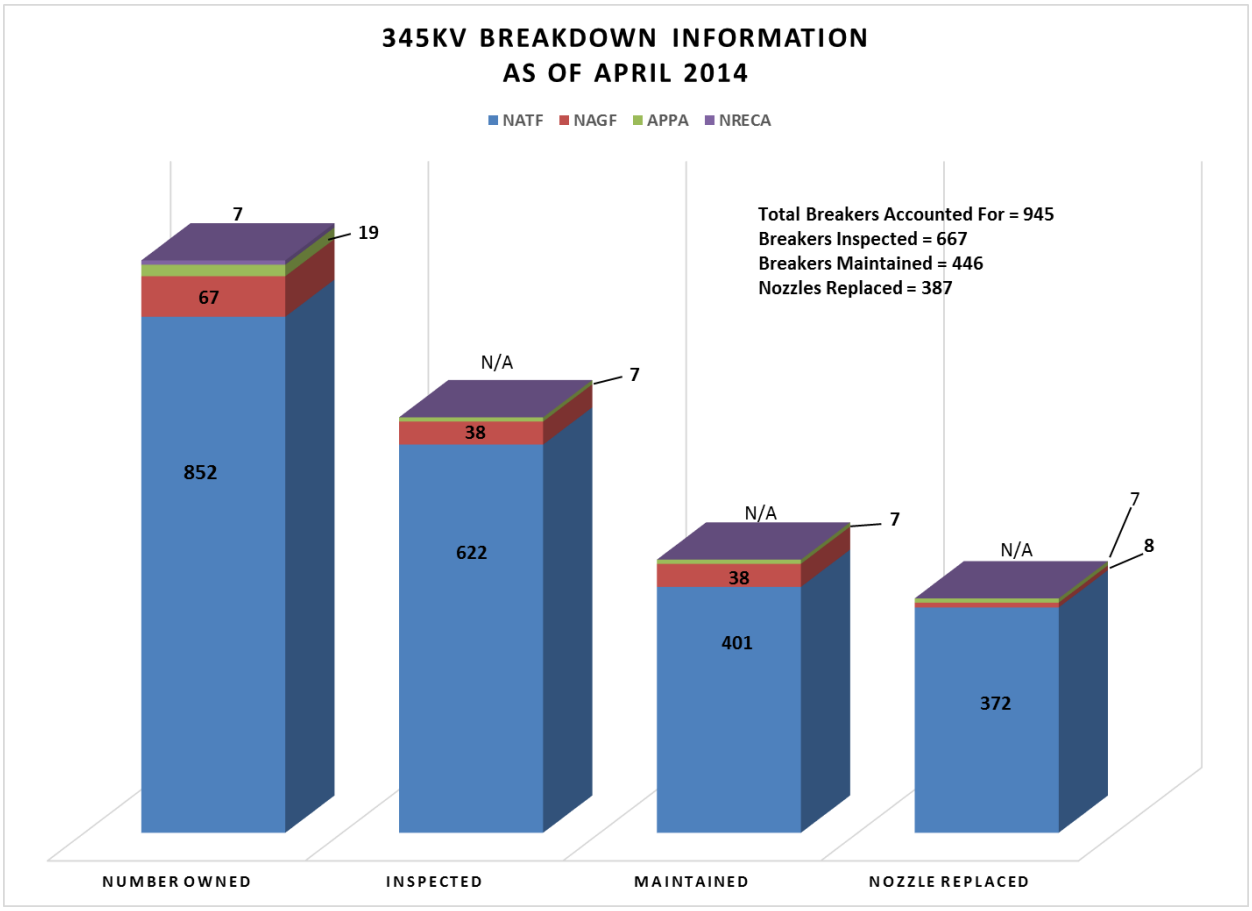
- Systematic Interaction with Members / ERO on Reliability Assurance Initiative (RAI)
  - Sharing of Key Principles and Lessons Learned
  - Risk / Controls focus in Peer Reviews
  - Preparing Members for Risk-focused Audits
  - Interacting with ERO Staff (workshops, etc.)

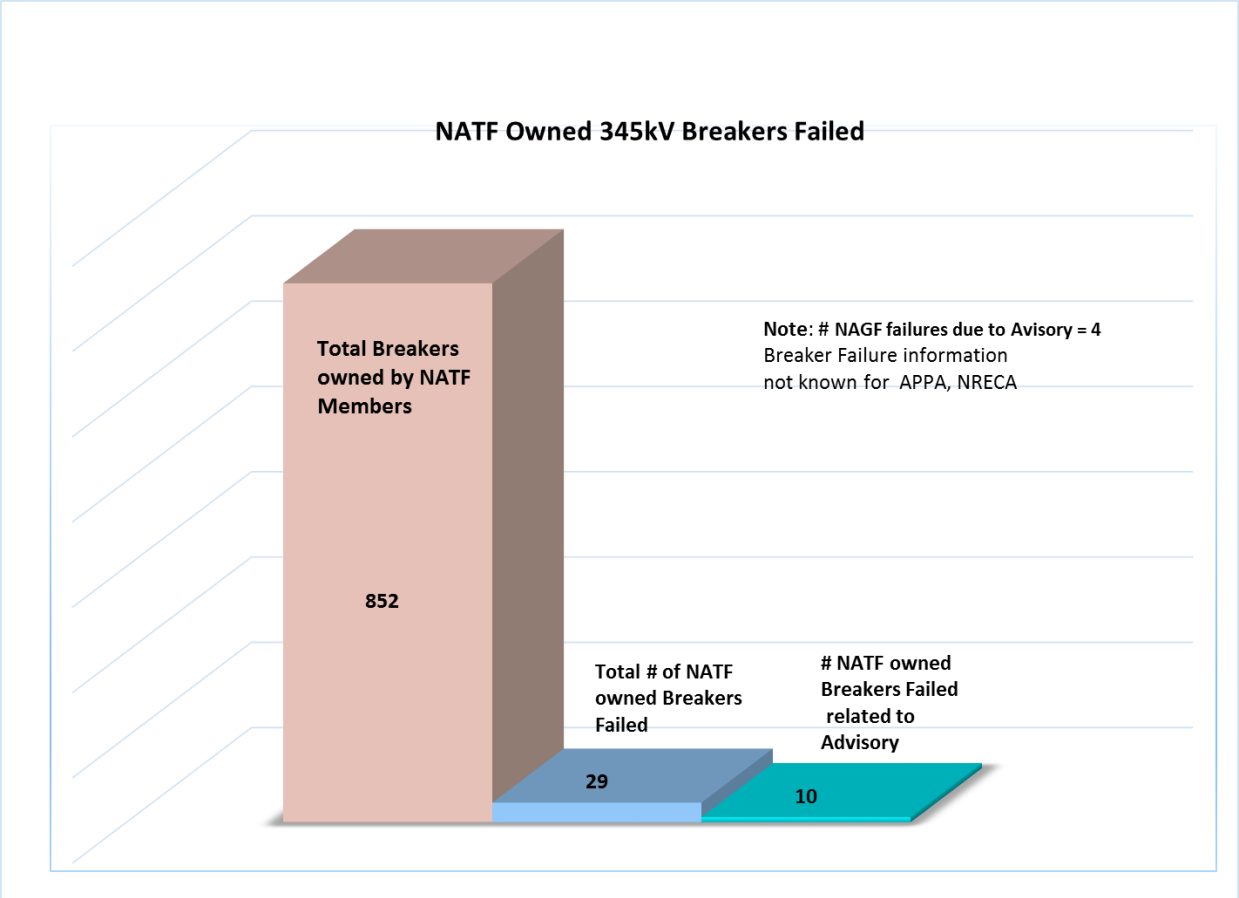
- EPRI Collaborations
  - Resiliency:
    - Physical Security
    - GMD Workshop(s)
    - EMP Workshop
    - Severe Weather
  - Equipment Performance and Maintenance Issues
  - Strategy Sessions Regarding Grid Operations and Planning Synergies

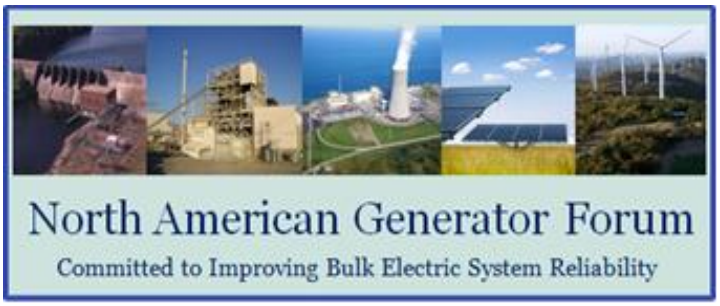
- INPO Collaborations - Operating Experience / LOOP Reductions (IER 13-53) / Blackstart

- NATF 2014 Peer Review Program Fully Integrates:
  - Risk Assessment and Internal Controls
  - Human Performance Error Reduction
  - Operating Experience Exchange
  - Physical Security

- Other Recently Completed / Near Term Activities
  - Compliance Practices Workshop (focus on Risk / Controls)
  - Human Performance Symposium
  - System Operations – EMS focus


345KV BREAKDOWN INFORMATION
AS OF APRIL 2014
NATF
NAGF
APPA
NRECA
Total Breakers Accounted For = 945
Breakers Inspected = 667
Breakers Maintained = 446
Nozzles Replaced = 387
7
19
67
852
N/A
7
38
622
N/A
7
38
401
N/A
7
8
372
NUMBER OWNED
INSPECTED
MAINTAINED
NOZZLE REPLACED


NATF Owned 345kV Breakers Failed
Total Breakers owned by NATF Members
852
Total # of NATF owned Breakers Failed
29
NATF owned Breakers Failed related to Advisory
10
Note: # NAGF failures due to Avisory = 4
Breaker Failure information not known for APPA, NRECA



TO: NERC Board of Trustees
Gerry Cauley, NERC President and CEO

FROM: Allen D. Schriver
Chair, North American Generator Forum (NAGF)

DATE: April 7, 2014

SUBJECT: NAGF 2014 Spring Report

---

1. The NAGF Standards Review Team collaborated with the VAR-002 Standards Drafting Team to first review generator comments from the last posting and then to develop and propose compromise language to the SDT, most of which was incorporated into the Standard. The NAGF strongly encouraged its members to review and evaluate the proposed Standard from the perspective that the new iteration was an improvement, was a compromise with TO/TOP's and was produced through what the NAGF leadership believes will be the first of many collaborative projects.

2. The NAGF Standards Review Team at the request of Mr. James Castle, NYISO and Chairman of the Operating Committee reviewed and submitted comments on the **Reliability Guideline: Generating Unit Operations During Complete Loss of Communications.**

3. On Wednesday April 2, 2014, the NAGF Security Practices Group held an NAGF conference call to update the membership on the status of **Project 2014-02 CIP Version 5 Revisions**. The call covered discussions on the overall plan, the changes to be worked on, the subgroup breakout and expected direction, the proposed schedule and the possibility for the NAGF to collaborate on the development of RSAW's.

4. Friday April 25, 2014, the NAGF is sponsoring a **BES Definition Workshop** to be held at the NextEra Energy Inc. Office in Juno Beach Florida. Mr. Thomas Burgess, NERC Vice President and Director, Reliability Assessment and Performance Analysis and Mr. Peter Heidrich, FRCC Manager of Reliability Standards have been kind enough to volunteer to lead the Workshop. The goal of the Workshop is to exchange information on the revised definition and to discuss impacts to GO/GOP's due to the change.

5. The NAGF continues to work on collaborative efforts as follows:
    A. With Mr. Troy Blalock, SCE&G, on the Eastern Interconnection Frequency Response Initiative. The NAGF is working to develop tuning guidelines for older GE mechanical governors.
    B. With Mr. Scott Barfield-McGinnis, NERC on opportunities to update and engage the NAGF on two specific NERC projects that affect generation entities. The projects are 2010-05.1 – Protection Systems: Misoperations (PRC-004-3) and 2010-13.3 – Relay Loadability: Stable Power Swings (PRC-026-1, new).
    C. With Mr. Mark Lauby, NERC as a member of the Reliability Based Registration Advisory Group (RBRAG)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Board of Trustees Meeting

May 7, 2014 | 8:30 a.m. - Noon Eastern
Hyatt Regency Philadelphia at Penn's Landing
201 S. Columbus Blvd.
Philadelphia, PA 19106

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consent Agenda

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Regular Agenda

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Opening Remarks by Board Chair

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Remarks by FERC Commissioner Cheryl LaFleur

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Remarks by FERC Commissioner Tony Clark

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Remarks by Mr. Denis O'Brien CEO, Exelon Utilities

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

President's Report

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards

Mark Lauby, Senior Vice President and Chief Reliability Officer
Board of Trustees Meeting
May 7, 2014

RELIABILITY | ACCOUNTABILITY

Demand Data (MOD C) – MOD-031-1

- Reliability benefits
  - Establishes consistency in data requirements and reporting procedures
  - Provides the authority to collect data necessary for reliability
  - Identifies responsible entities
- Action
  - Adopt MOD-031-1 Demand and Energy Data and associated documents

Voltage and Reactive Control – VAR-002-3

- Reliability benefits
  - Ensures Generator Operators (GOPs) provide reactive and voltage support
  - Enable GOPs to operate in controlling voltage or other mode as instructed by the Transmission Operator (TOP)
  - Requires GOPs to follow notification requirements established by the TOPs

- Action
  - Adopt VAR-002-3-Generator Operation for Maintaining Network Voltage Schedules and associated documents

Communication Protocols COM-002-4

- Reliability Benefits
  - Reliability-related information for Emergency and non-Emergency Operating Instructions is conveyed effectively, accurately, and consistently, in a timely manner towards mutual understanding by all key parties
- Action
  - Adopt COM-002-4—Operating Personnel Communication Protocols and associated documents
  - Rescind approval of Interpretation of COM-002-2, effective upon implementation of COM-002-4 in substantially the form adopted by the Board

Modify VRFs and VSLs as directed by FERC

- Background
  - FERC directed modification of Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) in 11 Reliability Standards
- Action
  - Adopt Violation Risk Factor/Violation Severity Level Revisions:
    - TPL-001-4
    - CIP Version 5 (CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-008-5, CIP-009-5)
    - MOD-026-1 and MOD-027-1
    - PRC-005-2 and PRC-005-3
    - BAL-003-1

Physical Security Standard

- Background
  - FERC order issued on March 7, 2014, directed NERC to submit Reliability Standard(s) that require steps to address physical security risks and vulnerabilities within 90 days
- Final ballot update

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Amendments to SERC Bylaws

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

State of Reliability Report

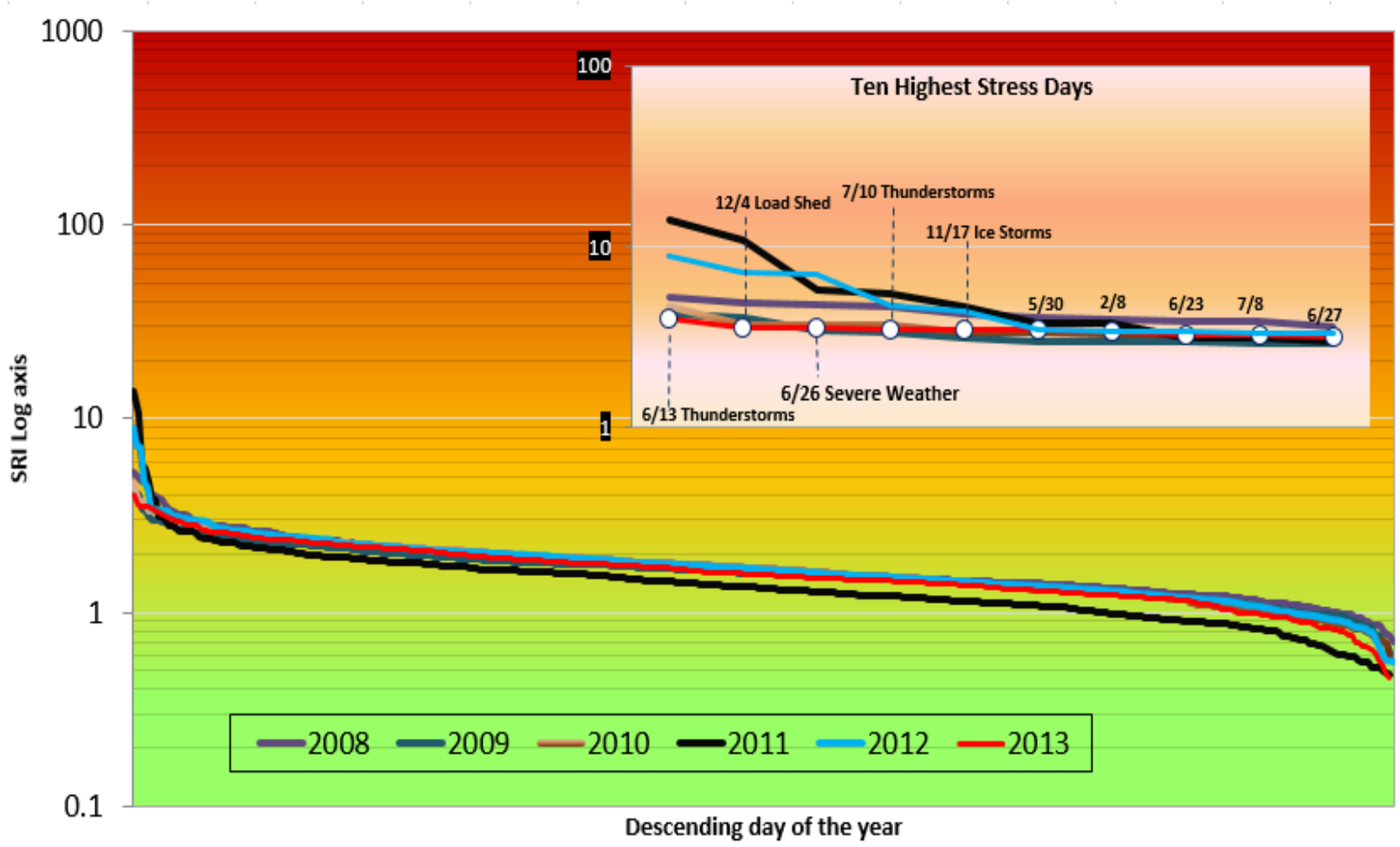
Howard Gugel, Director, Performance Analysis
Board of Trustees
May 7, 2014

RELIABILITY | ACCOUNTABILITY

State of Reliability

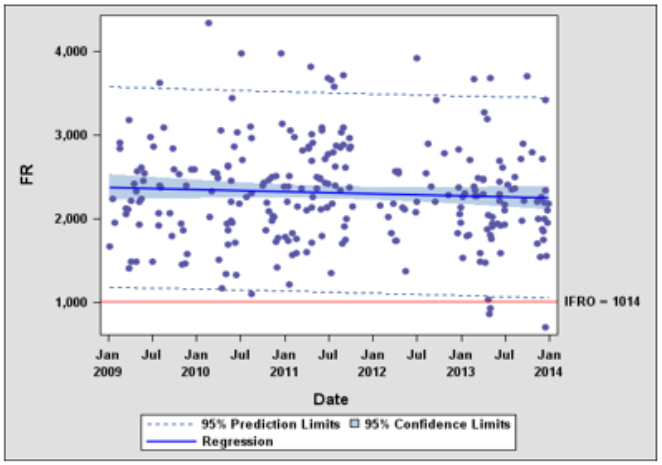
- Purpose – independent view of performance
- Identify trends and risks to reliability
- Provide recommendations
- Serve as risk-informed input to:
  - Reliability Issues Steering Committee (RISC) project prioritization
  - Standards projects
  - Reliability assurance initiatives
  - Event analysis reliability assessment, and critical infrastructure protection

Sustained High BPS Performance

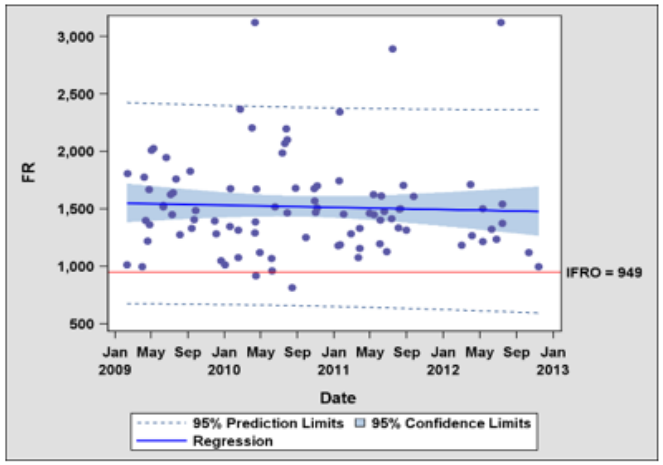


Frequency Response Remains Stable

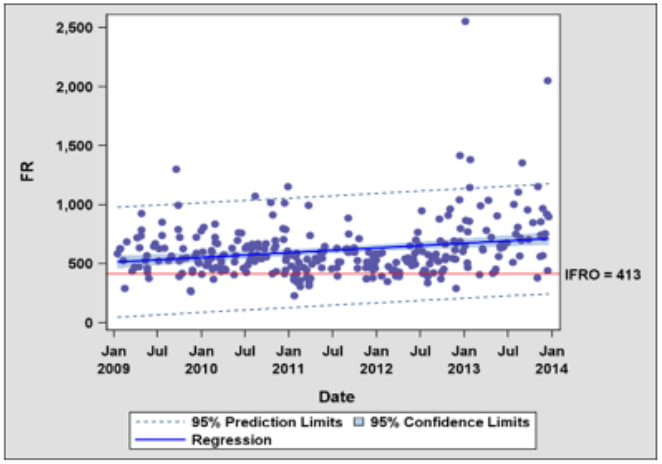
Eastern Interconnection



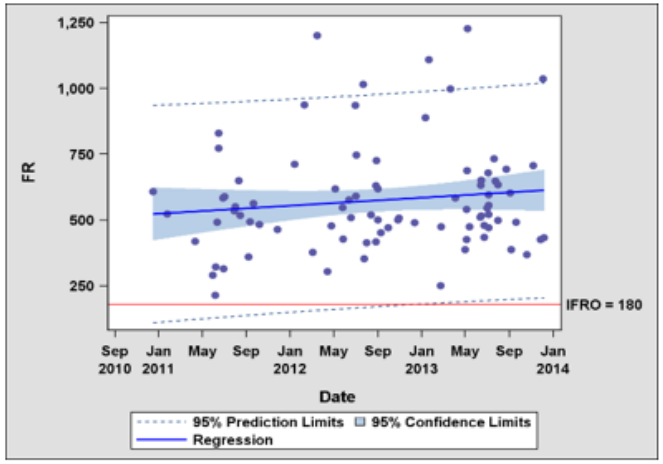
Western Interconnection



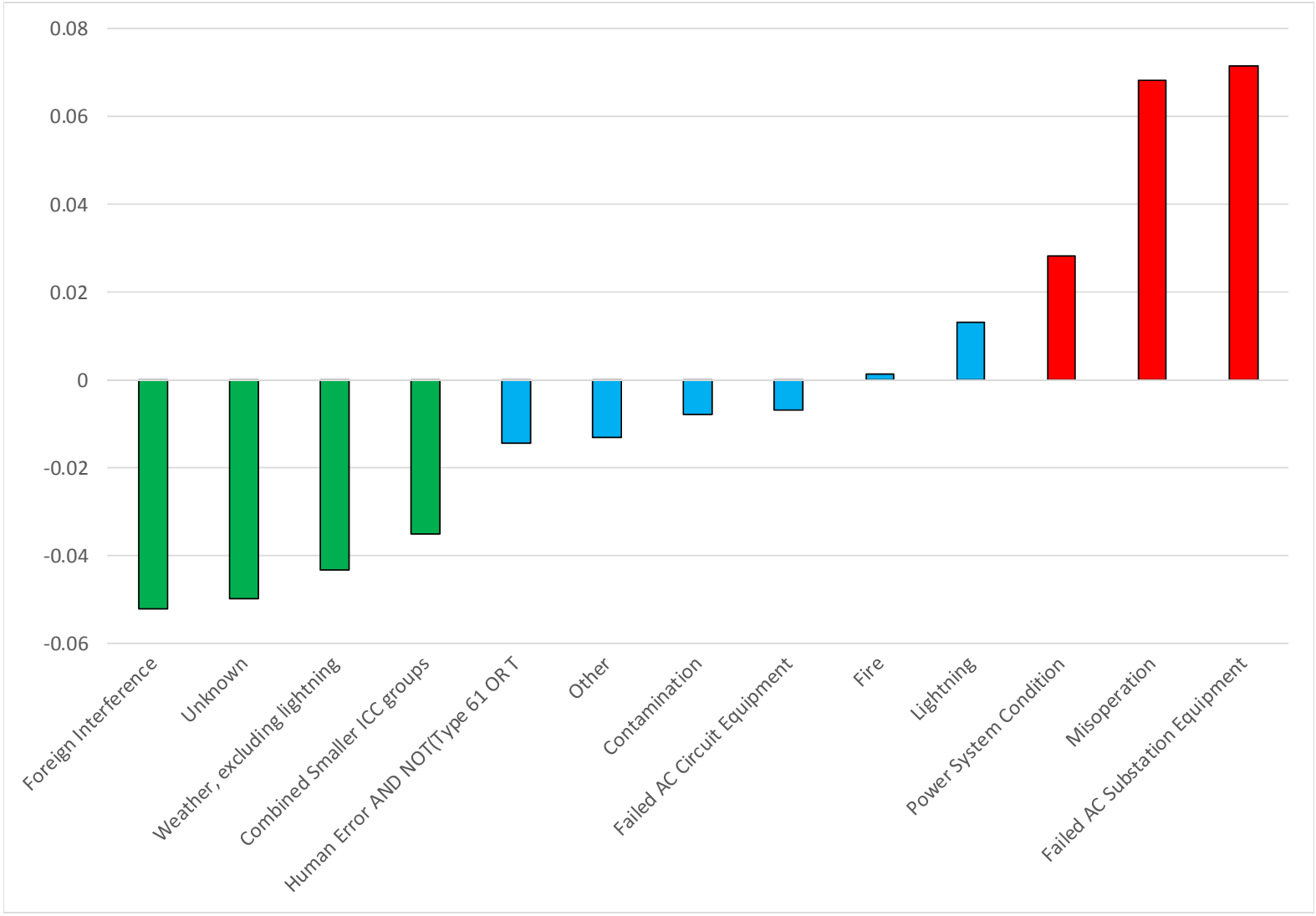
ERCOT Interconnection



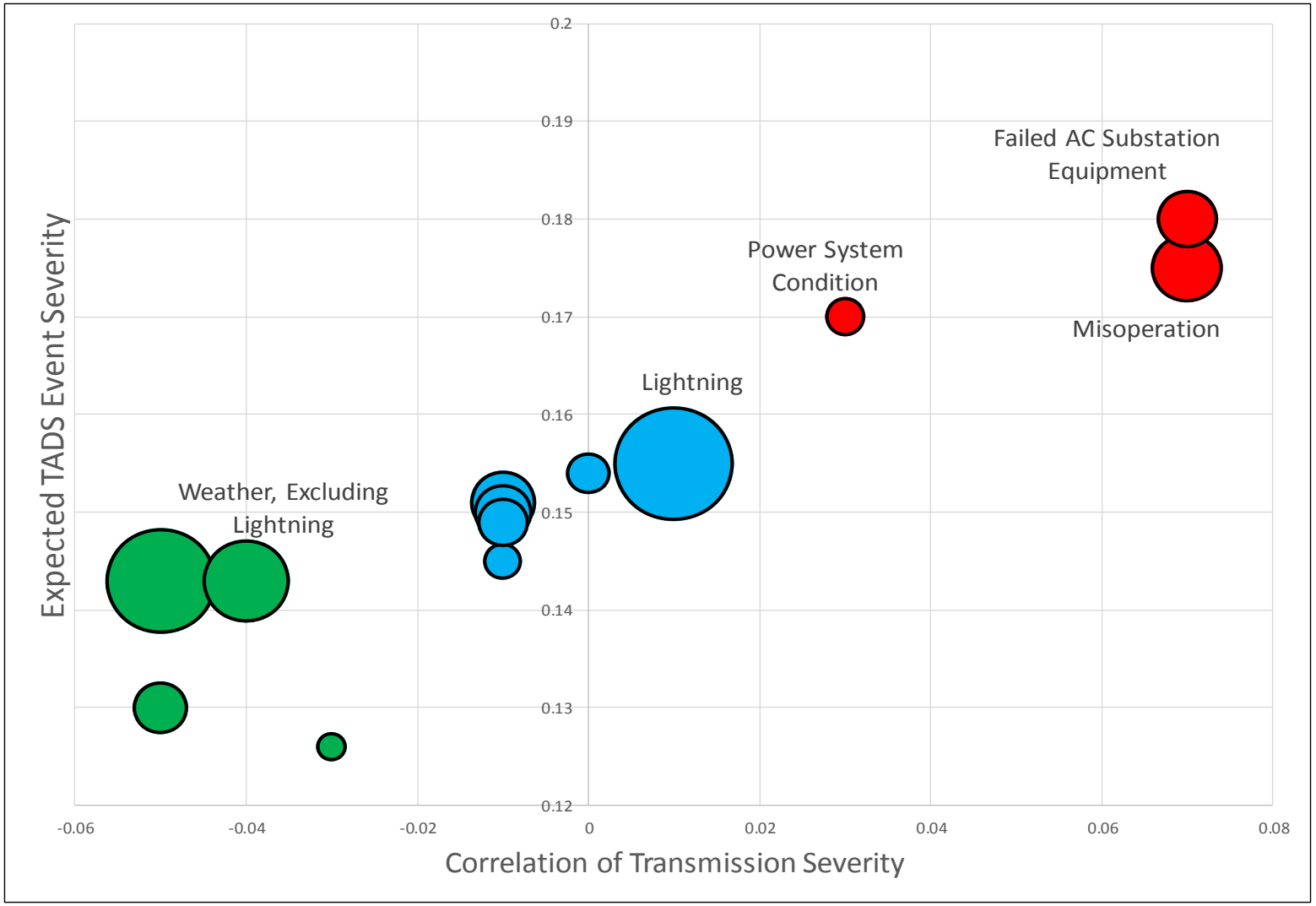
Québec Interconnection



Protection System Misoperations and Failed AC Substation Equipment



Transmission Outage Severity Correlation



Use of EEA Level 3 Declines

Number of Events	Year							
	2006	2007	2008	2009	2010	2011	2012	2013
NERC	7	23	12	41	11	23	15	7
FRCC	0	0	0	0	0	0	0	1
MRO	0	0	0	0	0	0	0	0
NPCC	0	0	1	1	0	0	0	0
RFC	0	3	1	0	2	0	1	0
SERC	4	14	2	3	4	2	7	0
SPP	1	5	3	35	4	15	6	2
TRE	0	0	0	0	0	1	0	0
WECC	2	1	5	2	1	5	1	4

Focus on Reliability Risks

- Integrate RISC control projects
- Physical and cyber security
  - Develop security performance metrics
- Integrating variable resources
  - Solar
  - Wind
- Changes in historical resource mix
  - Gas/coal
  - Demand as a resource
- Validate analyses using Events Analysis insights

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2014 Summer Reliability Assessment

John Moura, Director of Reliability Assessments
Board of Trustees
May 7, 2014

RELIABILITY | ACCOUNTABILITY

Key Findings - Summary

1. All Regions Meet Summer Reference Margin

- **ERCOT**: sufficient margins dependent on in-service dates of new generation
- **MISO**: retirements, derates, mothballing

2. Gas-Electric Interdependencies – Considerations for Summer

- Year-on-year increasing dependence on gas-fired generation
- Pipeline maintenance
- Natural gas storage

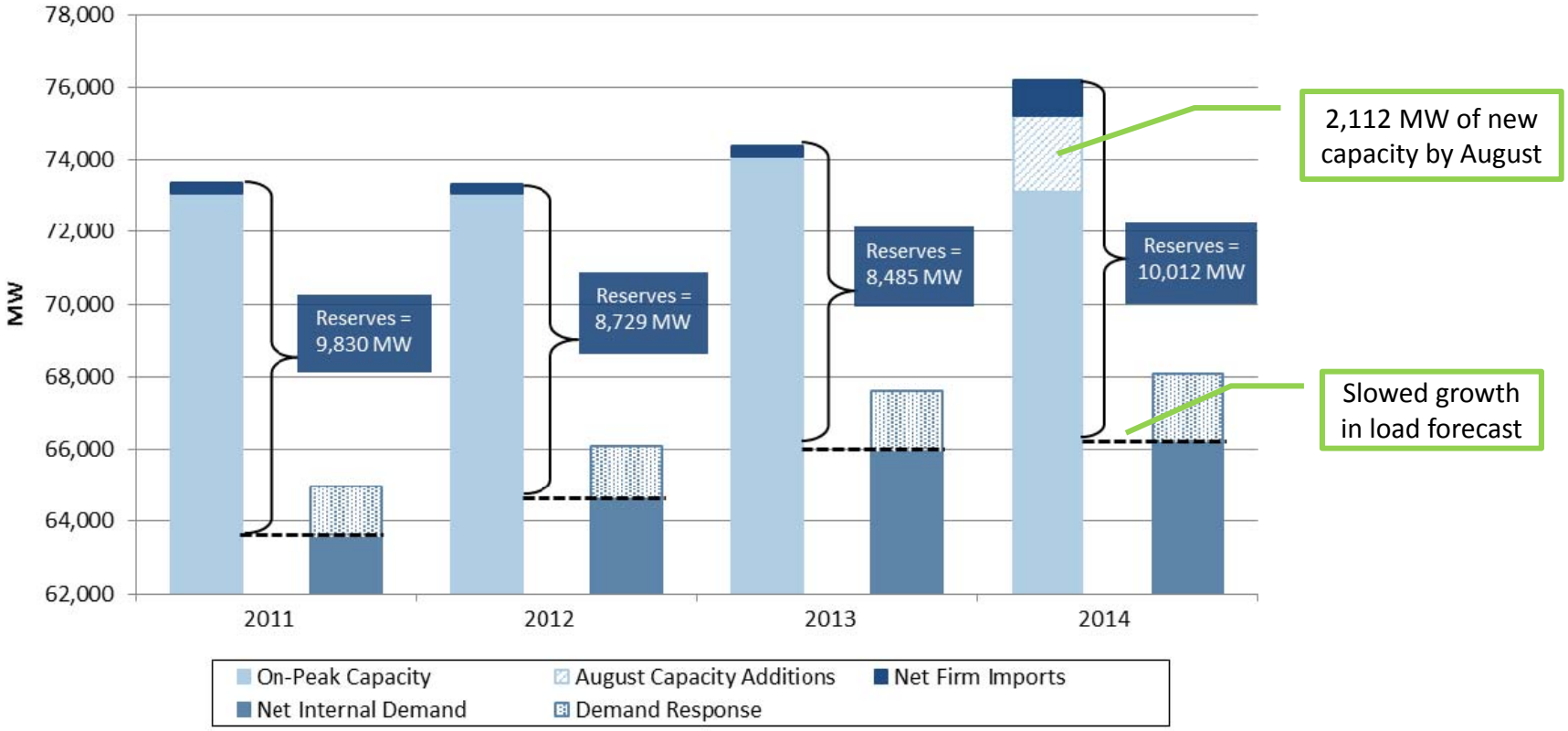
3. Continued Impacts of Baseload Retirements

- Contribute to tighter reserve margins
- Ontario retired last coal plant in April
- Localized reliability issues identified in operational planning

Other Summer Season Highlights

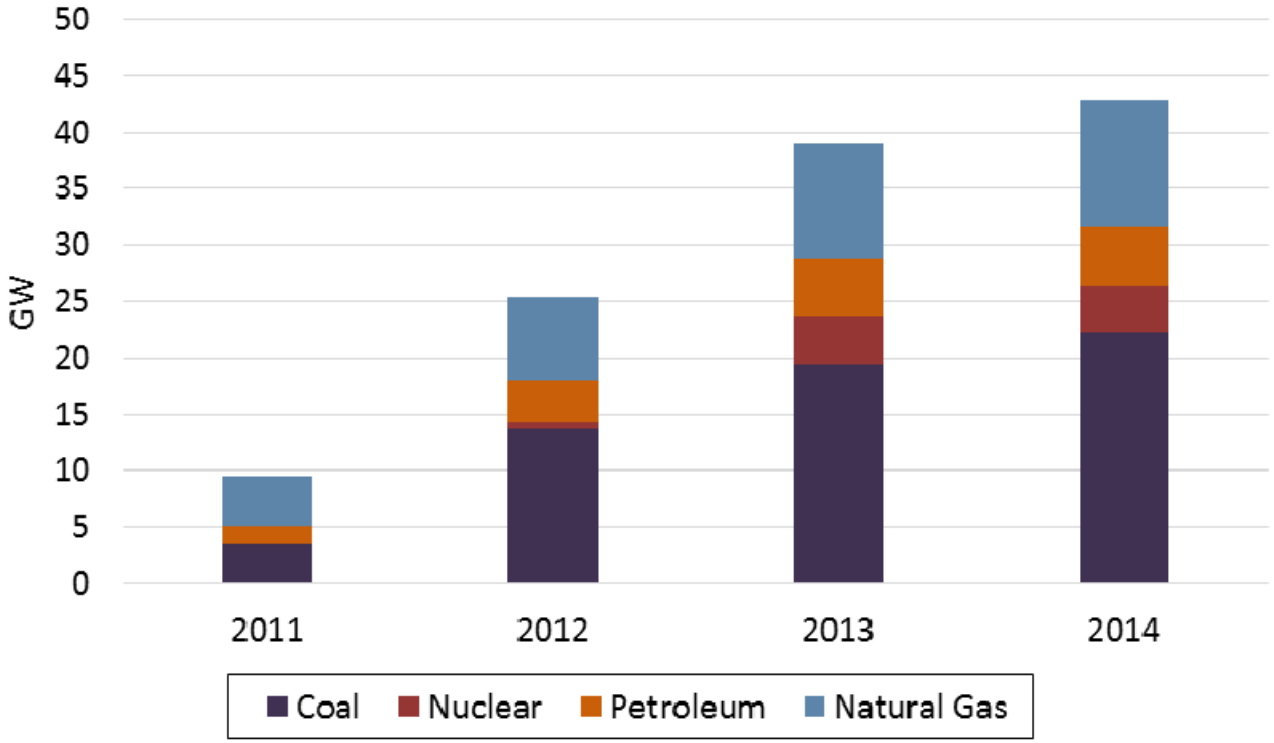
- **MISO-South integration**
  - North-south transmission constraints
- **California drought impacts**
  - Conditions have improved since March
  - “Extreme Drought” for most of California; some parts “Exceptional"
- **Rail shipments of coal in the Midwest**
  - Generation impacts unlikely for summer peak
  - Further evaluations warranted for longer-term challenge

New Capacity in ERCOT Strengthening Reserve Margins



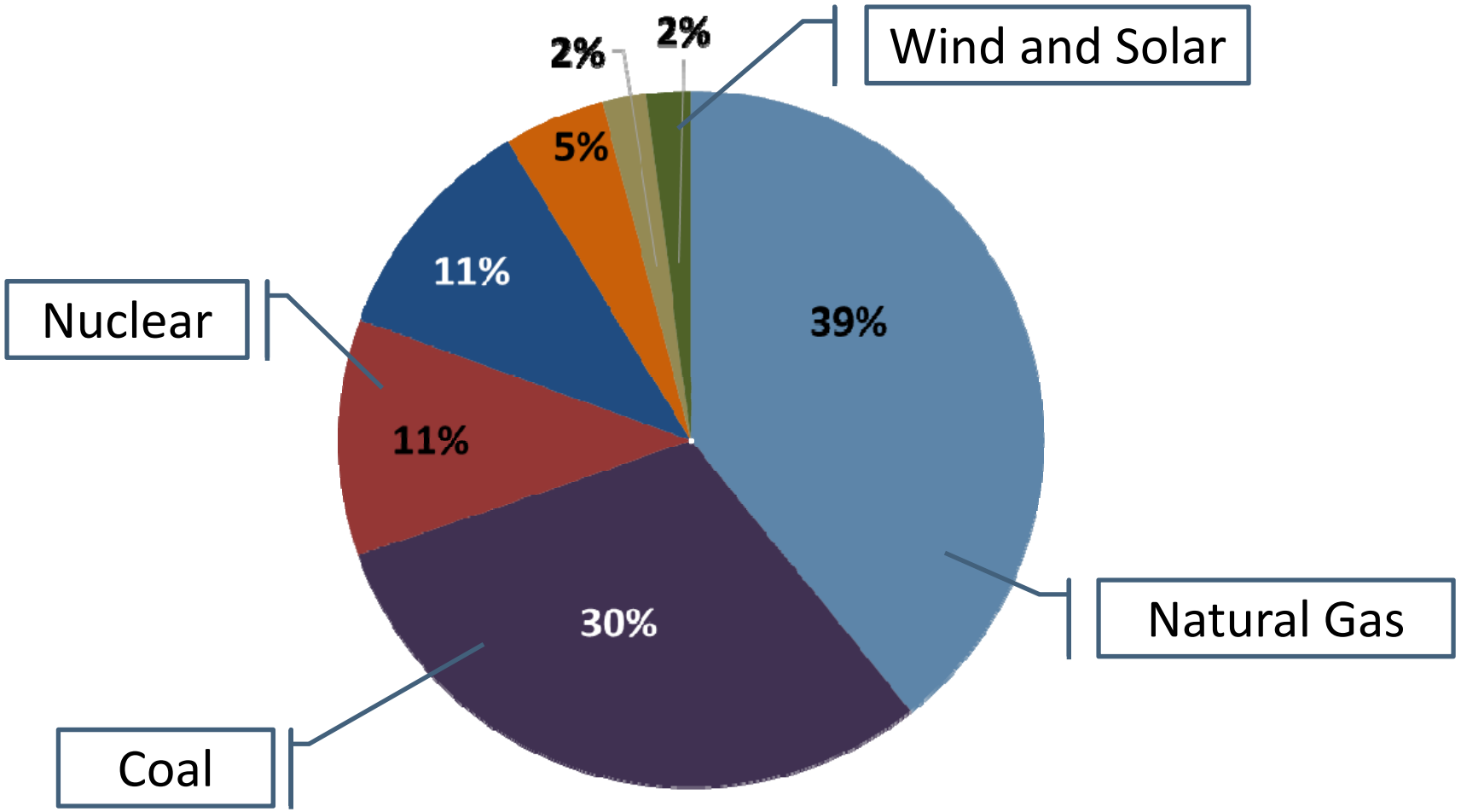
- August in-service date for needed capacity
- Growth in Demand Response programs
- Slower load growth projected, based on modified forecasting methodology

Generator Retirements On-Pace with NERC Projections



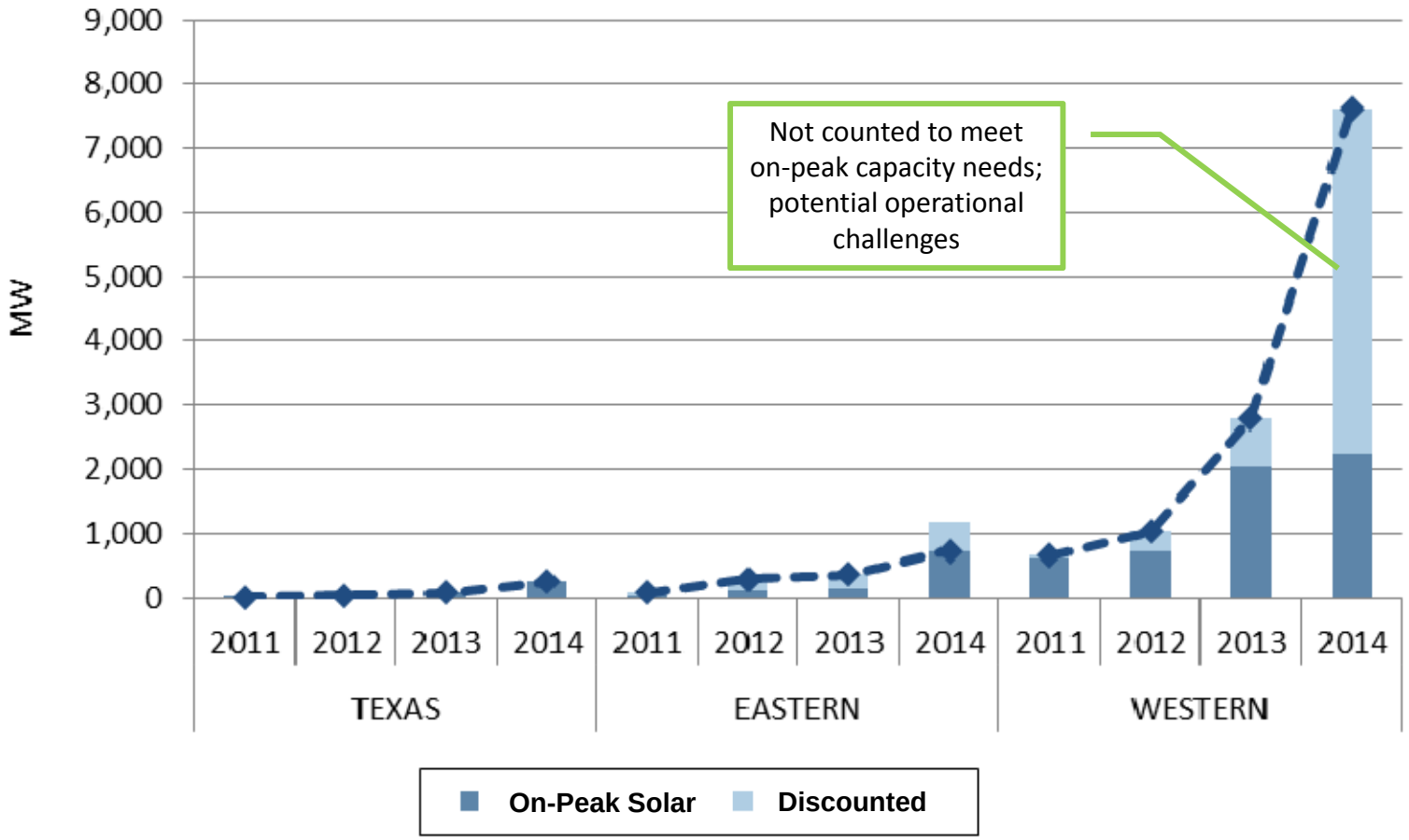
- **Retirements:** 43 GW of capacity since 2011
- Significant capacity reductions in Ontario and MISO
- Continue to track long-term impacts in the *Long-Term Reliability Assessment*

An Evolving Resource Mix



Substantial Growth in Solar Resources

Solar Energy in WECC (primarily California)



Approval and Publishing Schedule

Date	Deliverables
Tuesday, April 29	Report Sent to PC, OC, and MRC for Review
Monday, May 5	Planning Committee Review & Vote to Approve Report
Tuesday, May 6	Send Report to Board of Trustees for Review
Tuesday, May 13	BOT Teleconference and Vote to Approve Report
Thursday, May 15	Target Release

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Strategic Plan Metrics

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

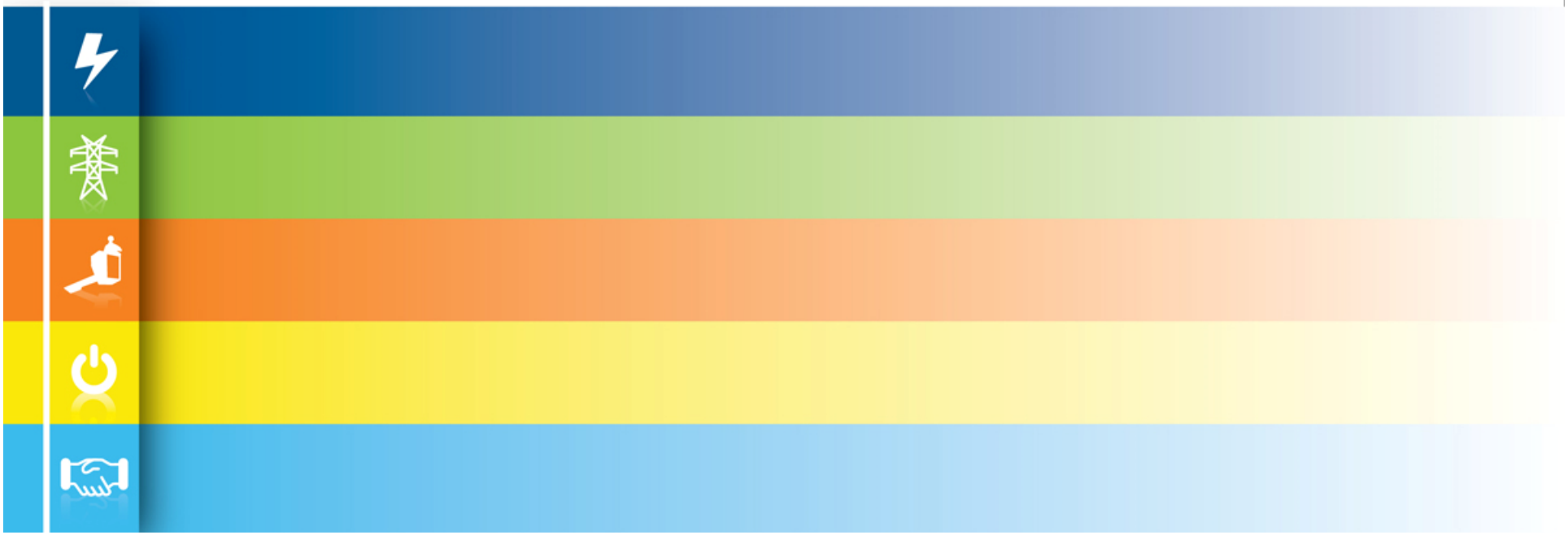
Canadian Affairs

RELIABILITY | ACCOUNTABILITY

Canadian Electricity Association | Association canadienne de l'électricité

Canadian Affairs Update

Jim Burpee
President & CEO, Canadian Electricity Association
NERC Board Meeting – Philadelphia, Pennsylvania
May 7, 2014



Overview

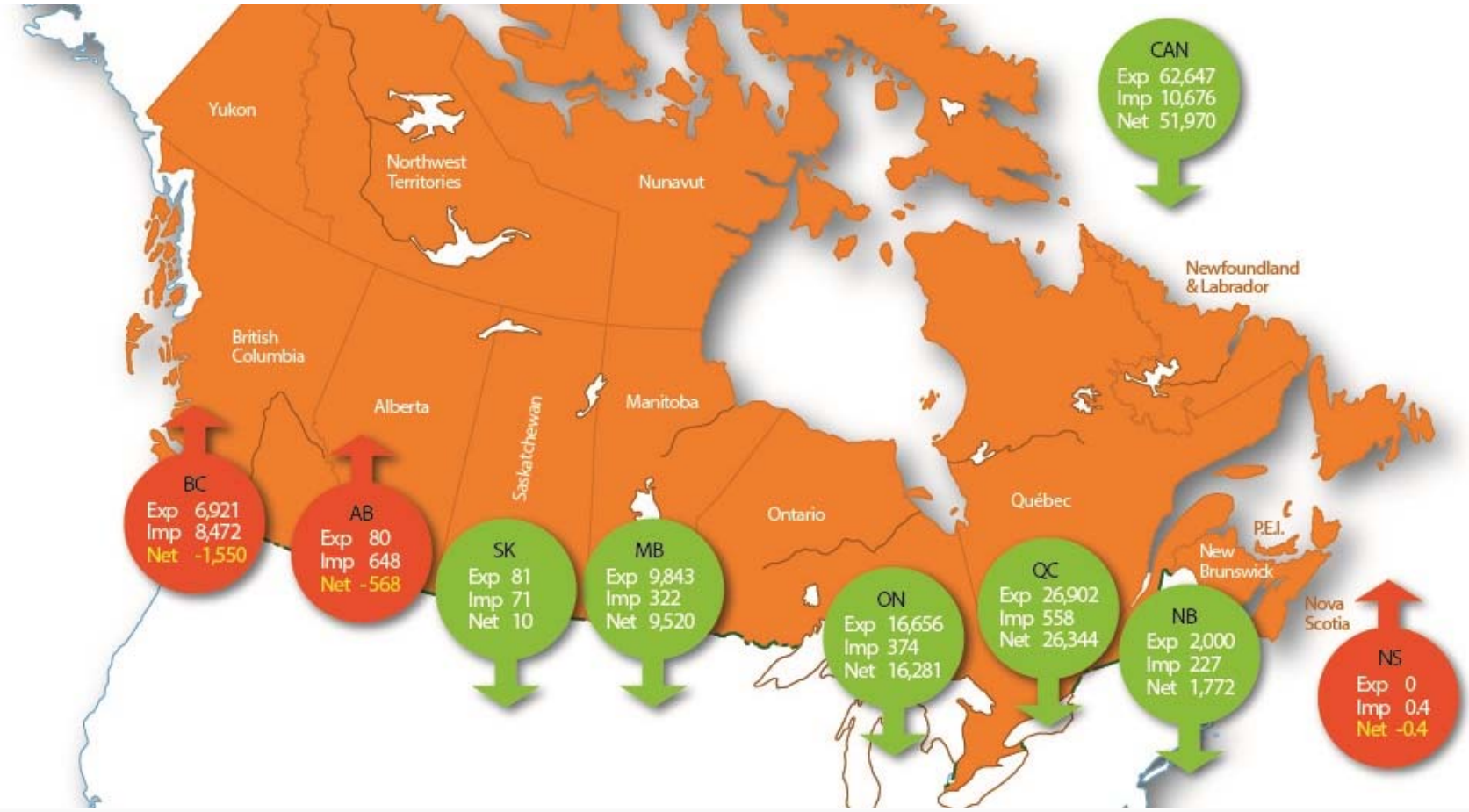
1. The Evolving Bilateral Electricity Relationship – Recent Events
   - 2013 data on Canada-U.S. electricity trade
   - New Minnesota-Manitoba transmission interconnection

2. CEA Policy Initiatives & Engagements – Recent Highlights
   - *Vision 2050: The Future of Canada's Electricity System*
   - EPA GHG Guidelines, Quadrennial Energy Review
   - Bipartisan Policy Center Electric Grid Cybersecurity Initiative

3. Comments on Major NERC Projects & Initiatives
   - Physical security standard
   - Risk-based registration

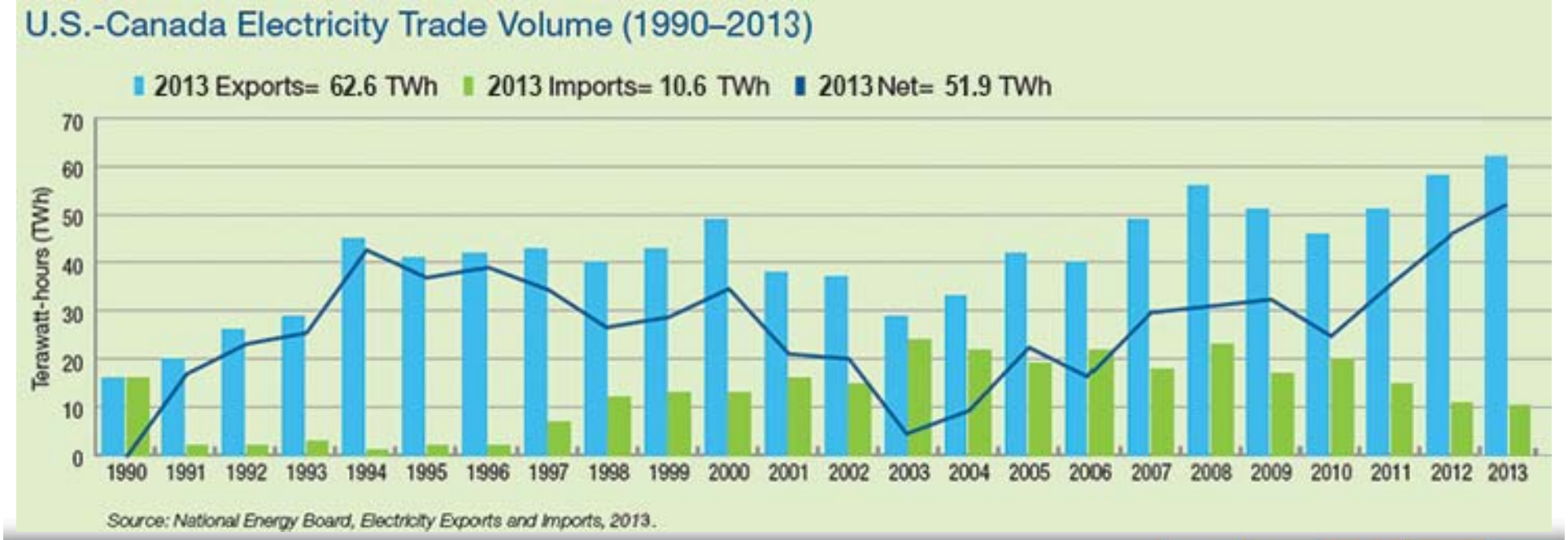
1. Evolving Bilateral Electricity Relationship – Recent Events

- Feb. 2014 – publication of 2013 NEB data on cross-border trade.



Data displayed are in gigawatt-hours. Source: National Energy Board, Electricity Exports and Imports, 2013.

- Key take-aways:
  - Exports from Canada rose 8% over 2012. U.S. exports remained even.
  - 2013 continued the recent trend of increased exports from Canada.
  - Most trading is transacted through the spot market (in 2013, 75%+). Long-term contracts represent <25% (and continue to decline).
  - Historically, Canada has been a net exporter (exports = 5-10% of generation).

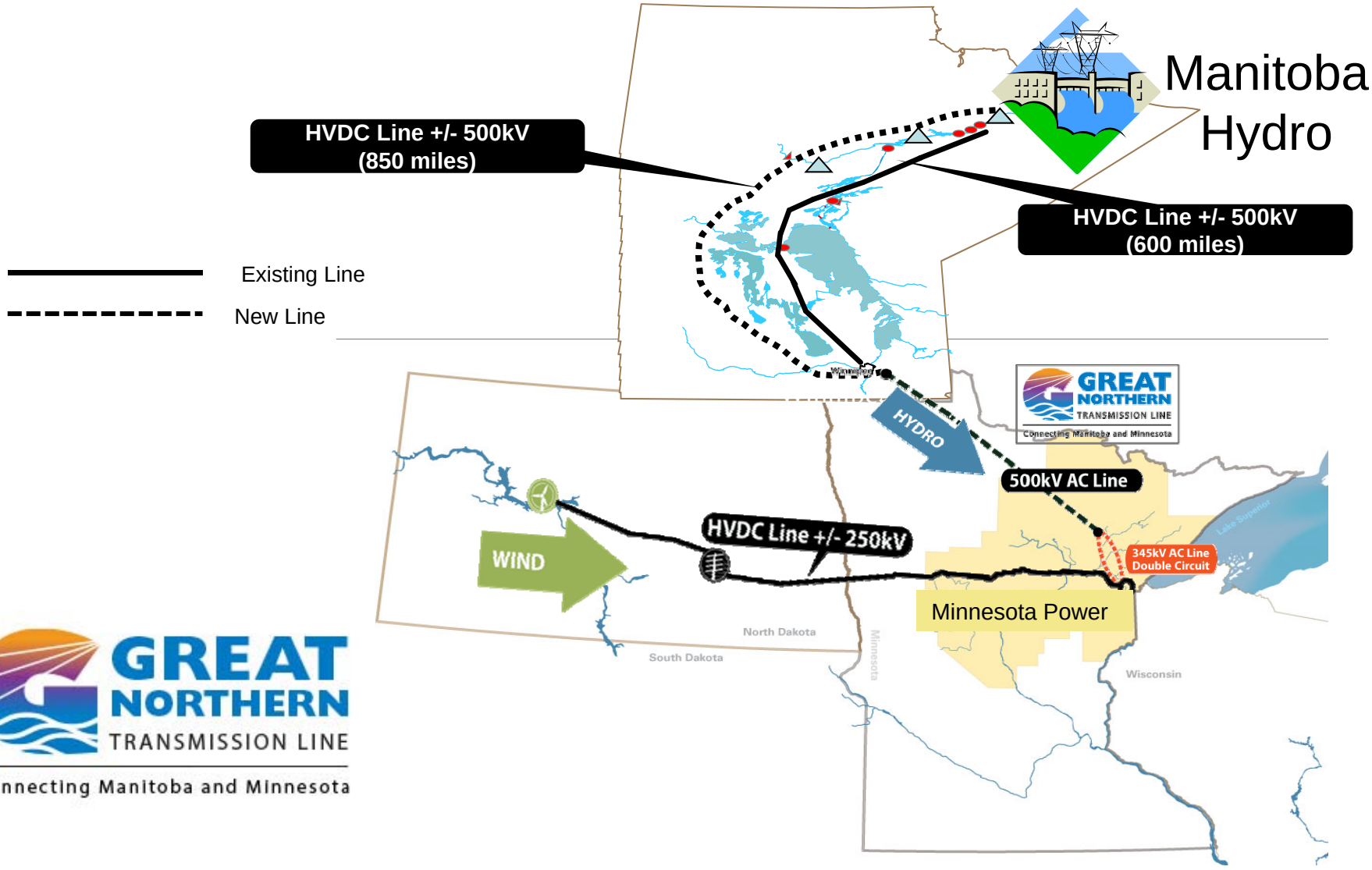


Great Northern Transmission Line

- Apr. 16, 2014 – Minnesota Power applies for state and federal permits for U.S. segment of new interconnection with Manitoba.
- Project being developed in partnership with Manitoba Hydro.
- 500 kV line from border to Iron Range; 750 MW transfer capacity.
- “Hydro by wire” from Manitoba enables “wind by wire” from North Dakota.
- Further diversifies Minnesota Power’s energy mix.
- Hydropower’s “load-following” capability and the unique “wind storage” provision add value to both wind and water assets.
- Overall project (energy + transmission line) enhances regional reliability and provides energy market benefits.
- Public engagement is ongoing for Manitoba’s segment of the line.

Hydropower + Windpower: A Perfect Marriage

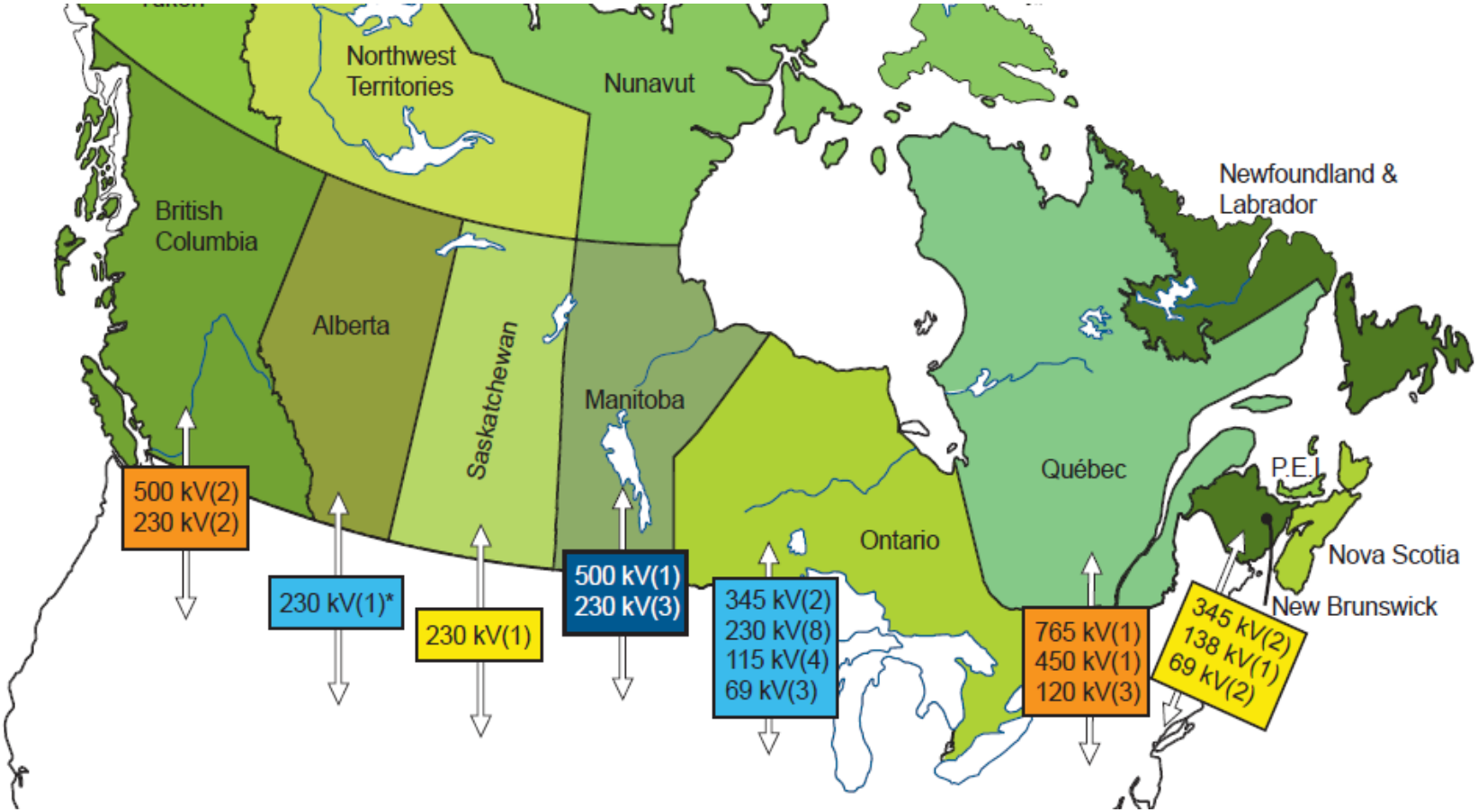
Manitoba Hydropower Facilitates North Dakota Windpower



GREAT NORTHERN TRANSMISSION LINE

Connecting Manitoba and Minnesota

Canada-U.S. Transmission Interconnections (Existing)

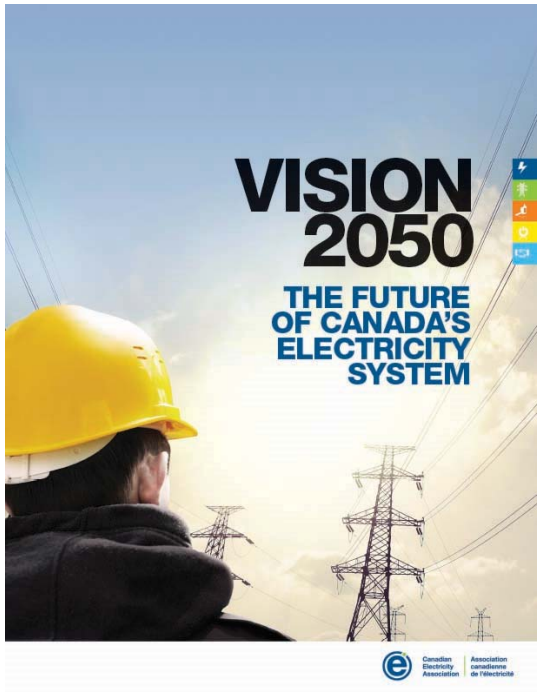


Source: National Energy Board

2. CEA Policy Initiatives & Engagements – Recent Highlights

Vision 2050: The Future of Canada's Electricity System

- Sheds light on the urgent need for informed decision-making – in policy development and infrastructure investment – if Canada is to maintain a reliable, sustainable and affordable system.
- Frames context for decisions about electricity, including drivers of change, in next 5-10 years.
- Offers recommendations in areas most likely to produce the greatest transformations:
  - Accelerating innovation and customer management.
  - Implementing financial instruments for CO_2 reduction.
  - Enabling electric vehicles.
  - Expanding collaboration across borders.
- Serves as basis for all CEA work going forward.



EPA GHG Guidelines, Quadrennial Energy Review

- CEA is engaging in both initiatives. Similar key messages:
  - Both should recognize & seek to expand benefits of U.S.-Canada integration:
    - Enhanced reliability and affordability; and
    - Reduced emissions (thru access to & support for low-carbon resources).
  - More integration will help maximize North America's clean energy potential.
- CEA appreciates the N. American scope to NERC's QER comments.

Bipartisan Policy Center Cyber Security Report

- Offers recommendations in four areas:
  - Standards and best practices; info sharing; responding to a cyber attack; and paying for cybersecurity.
- CEA participated in advisory board.
- Report's ideas are thoughtful; a few, contentious.

3. Comments on Major NERC Projects & Initiatives

Physical Security Standard

- CEA was concerned about language in FERC Order signaling an active role for regulatory authorities wrt to critical facilities lists.
- Draft standard has addressed this well and alleviated concerns.
- However, challenges look set to arise with 3rd-party verification:
  - What exactly does “verification” mean? How will verification be audited?
  - How can or should compliance be linked to activities or recommendations of a 3rd-party, which falls outside of NERC and governmental oversight?

Risk-based Registration

- Registration varies across Canada. Approaches build upon/are modelled upon NERC’s program. (*See CEA policy input).*
- Different approaches; same goals, focus (w/positive outcomes).

Questions?

For more information:

- **Jim Burpee**
  President and Chief Executive Officer
  (613) 230-4762
  Burpee@electricity.ca

- **Patrick Brown**
  Director, U.S. Affairs
  (613) 627-4124
  Brown@electricity.ca

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Committee Reports

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Operating Committee

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Planning Committee

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Critical Infrastructure Protection Committee

RELIABILITY | ACCOUNTABILITY

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Member Representatives Committee

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Personnel Certification Governance Committee

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Committee

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Issues Steering Committee Update

Bob Schaffeld, Chair, NERC Reliability Issues Steering Committee

NERC Board of Trustees Meeting

May 7, 2014

RELIABILITY | ACCOUNTABILITY

RISC Update

- Process-oriented Activities Completed
  - Charter Changes and Triage Process
  - Committee Interactions and ERO Planning Process Integration
- Membership Adjustments
  - RISC Nominating Committee Process
  - Extensions to Support Staggering and Continuity
  - New Members
- Risk Management Activities Underway
  - Execution in 2014
  - Business Planning and Budgeting for 2015
  - Analysis and Planning for the Future

Charter Changes

- Consistency
  - Reviewed Standards Process Input Group (SPIG) recommendations and ensured alignment with original intent of committee creation
- Formatting
  - Transfers charter to common NERC template
- Streamlining
  - Moves “how” elements to member handbook, keeps “what” elements in charter
  - Clarifies how members are appointed to the RISC
  - Removes MRC obligation to review charter every three years

Reliability Risk Management Process Status

- Execution in 2014
  - Triage and other process clarifications underway
  - Reliability Leadership Summit scheduled
  - Risk and action prioritization on schedule
- 2015 Business Plan and Budget Preparation
  - BP&B in development, with discussion of activities linked to Reliability Risk Management
  - **Goal**: Ensure 2015 activities are aligned with Reliability Risk priorities
- Longer-Term
  - Detailed Risk Analyses and Strategic Planning underway
  - **Goal:** Sustainable process, provides strategy and BP&B influence

Requested Actions

- Approve new Charter
- Approve membership adjustments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance and Certification Committee

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Electricity Sub-Sector Coordinating Council

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Forum and Group Reports

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

North American Energy Standards Board

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Regional Entity Management Group

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

North American Transmission Forum

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

North American Generator Forum

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Board Committee Reports

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Corporate Governance and Human Resources Committee

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Committee

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Finance and Audit Committee

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Enterprise-Wide Risk Committee

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Oversight and Technology Committee

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Minutes
Board of Trustees

May 7, 2014 | 8:30 a.m.-12:00 p.m. Eastern

Hyatt Regency Philadelphia at Penn's Landing
201 S. Columbus Blvd.
Philadelphia, PA 19106

Call to Order and Chair's Remarks

Mr. Frederick W. Gorbet, chair, called to order the duly noticed open meeting of the Board of Trustees ("Board") of the North American Electric Reliability Corporation ("NERC") on May 7, 2014, at 8:30 a.m. Eastern, and a quorum was declared present. The agenda is attached as **Exhibit A**.

Present at the meeting were:

Board Members:
Frederick W. Gorbet, Chair
Paul F. Barber
Janice B. Case
Gerald W. Cauley, President and Chief Executive Officer
Robert G. Clarke
David Goulding
Douglas Jaeger
Kenneth G. Peterson
Bruce A. Scherr
Jan Schori
Roy Thilly

NERC Staff
Charles A. Berardesco, Senior Vice President, General Counsel, and Corporate Secretary
Thomas Burgess, Vice President and Director of Reliability Assessment and Performance Analysis
Howard Gugel, Director of Performance Analysis
Mark G. Lauby, Senior Vice President and Chief Reliability Officer
John Moura, Director of Reliability Assessment
Steven Noess, Associate Director of Standards Development
Janet Sena, Senior Vice President and Director of Policy and External Affairs
Brady Walker, Associate Counsel
Michael Walker, Senior Vice President, Chief Financial and Administrative Officer, and Corporate Treasurer

A listing of industry attendees is attached as **Exhibit B.**

Mr. Gorbet acknowledged and welcomed Mr. John R. Norris, Commissioner, Federal Energy Regulatory Commission ("FERC"), and Mr. Denis O'Brien, Chief Executive Officer of Exelon Utilities. He expressed regrets on behalf of Mr. Ken Quesnelle, Chair of the Canadian Association of Members of Public Utility Tribunals, who was not able to attend the meeting.

NERC Antitrust Compliance Guidelines

Mr. Berardesco directed the participants' attention to the NERC Antitrust Compliance Guidelines included in the agenda, and offered to answer any additional questions the participants had at any time regarding antitrust compliance or other matters.

Consent Agenda

Upon motion duly made and seconded, the Board approved the consent agenda as follows:

Minutes

The draft minutes for the February 6, 2014 Board meeting were approved in the form as presented to the Board at the meeting.

Compliance Processes and Procedures Subcommittee Formation

RESOLVED, that the Board hereby approves the elimination of the Compliance and Certification Committee's Standards Interface Subcommittee and Procedures Subcommittee.

FURTHER RESOLVED, that the Board hereby approves the formation of the Compliance Processes and Procedures Subcommittee.

Committee Membership Appointments

Critical Infrastructure Protection Committee

RESOLVED, that the Board hereby approves the appointment of the following individuals to the Critical Infrastructure Protection Committee ("CIPC") for a term of at least two years:

- Gary Mayfield of the Western Area Power Administration
- Ed Goff of Duke Energy

RESOLVED, that the Board hereby approves the election of the following individual to the Executive Committee of the CIPC for a term commencing May 7, 2014 and concluding December 31, 2015:

- David Revill of Georgia Transmission

Compliance and Certification Committee

RESOLVED, that the Board hereby appoints the following individuals to the Compliance and Certification Committee, each for a term of three years, effective May 7, 2014:

- Rick Terrill of Luminant Mining
- Caroline Dupuis of Hydro-Québec TransÉnergie
- William Temple of Northeast Utilities
- Jennifer Flandermeyer of Kansas City Power & Light

FURTHER RESOLVED, that the Board hereby appoints the following individuals as officers, each for a term of two years, effective July 1, 2014.

- Patti Metro of the National Rural Electric Cooperative Association, chair
- Jennifer Flandermeyer of Kansas City Power & Light, vice chair

Personnel Certification Governance Committee

RESOLVED, that the Board hereby appoints the following individual to the Personnel Certification Governance Committee for a term beginning May 7, 2014 and concluding December 31, 2015:

- Michael Hoke of PJM Interconnection

Executive Session

Mr. Gorbet reported that before the open meeting, as is its custom, the Board met in closed session with NERC management, and subsequently in executive session without NERC management, to review NERC management activities.

Mr. Gorbet also reported that on Monday, May 5, 2014, the Board met with the leadership of the Boards of the Regional Entities with Regional Entity chief executive officers present, and then without the CEOs in a subsequent executive session. Mr. Gorbet summarized the discussion and reported that these meetings have helped to improve communication at the governance level within the ERO Enterprise.

Welcoming Remarks

Mr. Gorbet welcomed and introduced Mr. Norris and Mr. O'Brien.

Remarks by John R. Norris

Mr. Norris remarked on the evolution of the relationship between FERC and NERC and stated he believed interactions between the two organizations had improved significantly. He praised the quality of NERC's work and commented on the overall positive direction of the organization. Mr. Norris thanked NERC leadership and staff for their response to and work on the Physical Security Order and the related proposed Reliability Standard. He noted that caution should be exercised when responding to political pressures to act, both now and in the future, and encouraged NERC to continue to take

action in the interest of reliability. Mr. Norris stated he was looking forward to continuing a productive working relationship with NERC.

Remarks by Denis O'Brien

Mr. Cauley provided a brief introduction of Mr. O'Brien.

Mr. O'Brien provided the Board with an overview of Exelon's investments in infrastructure and commitment to reliability. He highlighted the positive effects of NERC's outreach to and collaboration with the electric industry.

President's Report

Mr. Cauley provided comments on the evolution of the standards development process. He stated that the process has matured over the years and has benefitted from the high quality of FERC orders that allow industry to work collaboratively to arrive at the best and most efficient solutions for reliability. Mr. Cauley highlighted the flexibility and adaptability of the standards development process and cited the development of the proposed Physical Security Reliability Standard as an example of NERC's and industry's ability to respond to urgent issues. He praised the hard work of the standard drafting team members.

Mr. Cauley stated that the standards development process is working as it was envisioned with broad oversight from FERC, leadership from NERC's Board, and the effective application of technical expertise that leads to improved reliability, avoids undue compliance burdens, and serves the public interest.

Standards

Mr. Lauby provided an overview of the Reliability Standards program and presented the following items for Board action. After discussion, and upon motions duly made and seconded, the Board approved the following resolutions:

Demand Data (MOD C)—MOD-031-1

RESOLVED, that the Board hereby adopts proposed Reliability Standard MOD-031-1, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the associated implementation plan, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the revised and new NERC Glossary definitions, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Violation Risk Factors and Violation Severity Levels for the proposed Reliability Standard, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Reliability Standards proposed for retirement, as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities and take such further actions and make such further filings as are necessary and appropriate to effectuate the intent of the foregoing resolutions.

Voltage and Reactive Control—VAR-002-3

RESOLVED, that the Board hereby adopts proposed Reliability Standard VAR-002-3, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the associated implementation plan, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Violation Risk Factors and Violation Severity Levels for the proposed Reliability Standard, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Reliability Standard proposed for retirement, as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities and take such further actions and make such further filings as are necessary and appropriate to effectuate the intent of the foregoing resolutions.

Operating Personnel Communications Protocols—COM-002-4

RESOLVED, that the Board hereby adopts proposed Reliability Standard COM-002-4, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the associated implementation plan, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the new NERC Glossary definition, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Violation Risk Factors and Violation Severity Levels for the proposed Reliability Standard, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Requirement and Reliability Standards proposed for retirement, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby rescinds its February 9, 2012 approval of the Interpretation of COM-002-2, effective (i) for U.S. registered entities upon implementation of COM-002-4 in substantially the form approved by the Board and (ii) for Canadian entities, effective upon implementation of COM-002-4 in substantially the form approved by the Board.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities and take such further actions and make such further filings as are necessary and appropriate to effectuate the intent of the foregoing resolutions.

Violation Risk Factor/Violation Severity Level Revisions

RESOLVED, that the Board hereby adopts proposed Violation Risk Factor and Violation Severity Level Modifications for the following Reliability Standards, as presented to the Board at this meeting:

- TPL-001-4—Transmission System Planning Performance Requirements
- CIP-003-5—Cyber Security—System Management Controls
- CIP-004-5.1—Cyber Security—Personnel and Training
- CIP-006-5—Cyber Security—Physical Security of BES Cyber Systems
- CIP-008-5—Cyber Security—Incident Reporting and Response Planning
- CIP-009-5—Cyber Security—Recovery Plans for BES Cyber Systems
- MOD-026-1—Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions
- MOD-027-1—Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions
- PRC-005-2—Protection System Maintenance
- PRC-005-3—Protection System and Automatic Reclosing Maintenance
- BAL-003-1—Frequency Response and Frequency Bias Setting

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities and take such further actions and make such further filings as are necessary and appropriate to effectuate the intent of the foregoing resolutions.

Physical Security Reliability Standard Development

Mr. Lauby introduced Mr. Noess who announced that the proposed Physical Security Reliability Standard had received final industry approval. He thanked the standard drafting team, the Standards Committee, and industry stakeholders for their collaborative efforts on this project. Mr. Noess indicated that NERC staff would begin to prepare the proposed Reliability Standard for approval by the NERC Board at a future meeting.

Mr. Brian Murphy, chair of the Standards Committee ("SC"), praised the collaborative nature of the development process and stated that the approach to development on this project could benefit all future standards development projects.

Amendments to SERC Bylaws

Mr. Berardesco presented a set of proposed amendments to the SERC Reliability Corporation Bylaws. He stated that the amendments reflect a decision made by SERC regarding its tax status and that these changes do not impact SERC's ability to operate as a Regional Entity. Mr. Berardesco indicated Board approval was required because the Bylaws are an exhibit to the delegation agreement and noted that FERC will also need to approve the amendments.

Upon motion duly made and seconded, the Board approved the following resolution:

WHEREAS, the SERC Board of Directors has proposed amendments to the Delegation Agreement between NERC and SERC ("Delegation Agreement") by amending Exhibit B – the SERC Bylaws.

WHEREAS, the proposed amendments do not affect SERC's Regional Entity functions.

WHEREAS, the proposed amendments continue to satisfy the governance criteria specified in the Delegation Agreement.

RESOLVED, that the Board hereby approves the proposed amendments to NERC's Delegation Agreement with SERC, consisting of amendments to Exhibit B – the SERC Bylaws, in the form as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities.

State of Reliability Report

Mr. Burgess provided an introduction to the State of Reliability Report ("SORR"). He explained that the SORR is developed by NERC's Reliability Assessment and Performance Analysis group, stakeholders, and regional assessment groups. Mr. Burgess stated the SORR utilizes a variety of data, event analyses, and historical performance information to identify trends and indicators related to Bulk-Power System performance and reliability. With that information, NERC and stakeholders are able to take proactive steps to focus on key areas of reliability performance.

Mr. Gugel provided an overview of the 2014 SORR. He stated the SORR represents NERC's independent view of ongoing Bulk-Power System trends through an objective analysis of the state of reliability. The SORR's key findings serve as guide to risk assessment, reliability standards development project prioritization, compliance and enforcement process improvement, event analysis, and critical infrastructure protection. Mr. Gugel presented a summary of the keys findings and recommendations, a copy of which was included with the advance meeting materials.

Summer Reliability Assessment

Mr. Burgess provided an overview of the Summer Reliability Assessment. He indicated that NERC provides seasonal assessments that describe anticipated conditions and key areas for focus and

attention during upcoming summer seasonal conditions. Mr. Moura presented a summary of the key findings and recommendations, a copy of which was included with the advance meeting materials.

ERO Strategic Plan Metrics

Mr. Cauley provided an overview of the Three-Year ERO Strategic Plan approval process. He noted that the Board approved the Strategic Plan without the plan metrics at its February 2014 meeting, so as to allow management to refine a few of the metrics to reflect industry comments. Mr. Cauley presented a summary of the revisions and indicated that the metrics are intended to provide guidance for achieving the goals outlined in the Strategic Plan. He stated that both the Strategic Plan and metrics will be updated as necessary.

Upon motion duly made and seconded, the Board approved the following resolution:

RESOLVED, that the Board hereby approves the metrics for use with the ERO Strategic Plan, as presented to the Board at this meeting.

Canadian Affairs

Mr. James Burpee, President and CEO of the Canadian Electricity Association, presented an update on current Canadian reliability-related initiatives.

Standing Committee Reports

Representatives of the Standing Committees provided reports to the Board highlighting items from their written reports as contained within the agenda package.

Operating Committee

Mr. James D. Castle, chair, highlighted some of the Operating Committee's ("OC") activities since the last Board meeting. He thanked Trustees Jaeger and Barber for their attendance at the OC's March meeting and stated the OC is looking forward to welcoming Ms. Case and Mr. Gorbet at future meetings. Mr. Castle praised the Board for their commitment to engaging with the OC. He also provided updates on the OC's work on (i) the Essential Reliability Services Taskforce, (ii) the cold weather preparedness reliability guideline, (iii) the independent experts' report, and (iv) improvements to the organization and structure of the OC.

Planning Committee

Mr. Benjamin Crisp, chair, reviewed progress on some of the Planning Committee's ("PC") key initiatives. He outlined the PC's work in helping to develop the Summer Reliability Assessment and State of Reliability Report. Mr. Crisp also summarized the PC's work with the GMD taskforce and efforts to provide technical basis and justification to that project's standard drafting team. He provided an overview of the PC's process changes which are intended to allow for more feedback from the regions and an increased ability to reprioritize projects within the PC as necessary. Mr. Crisp thanked the Trustees for their active participation with the PC.

Critical Infrastructure Protection Committee

Mr. Charles F. Abell, chair, briefly summarized the ongoing work of the CIPC. He highlighted the issuance of two reports related to NERC's GridEx II, one for the distributed play exercise and one for the executive table top exercise. Mr. Abell stated that the CIPC was actively engaged in implementing the recommendations and addressing the concerns identified in the reports. He also highlighted the strong attendance at and feedback from the CIPC technical workshops and stated that planning was underway for another workshop in June focusing on physical security issues.

Member Representatives Committee

Mr. John A. Anderson, chair, thanked Mr. Gorbet and the Board for the continued use of the Member Representatives Committee's ("MRC") policy input, and summarized the issues that had been discussed at the MRC meeting the previous day. He stated he was appreciative of new meeting structure and recognized MRC members for attending Board Committee meetings.

Personnel Certification Governance Committee

Mr. Brett Hallborg, chair, was not in attendance. Mr. Gorbet referred the meeting participants to the written report of the Personnel Certification and Governance Committee, located in the agenda package.

Standards Committee

Mr. Murphy expressed his gratitude for the good working relationship between the SC and the Board, NERC staff, industry, and the staff of FERC. He outlined work that was ongoing on a number of projects and initiatives including (i) coordination between the SC and the Reliability Issues Steering Committee ("RISC"), (ii) the Reliability Standards Development Plan and its relation to the newly approved ERO Strategic Plan metrics, and (iii) the development of an evaluation framework to be used in conjunction with the metrics.

Reliability Issues Steering Committee

Mr. Robert A. Schaffeld, chair, outlined some of the recent activities of the Reliability Issues Steering Committee ("RISC") including (i) several process improvements intended to assist with the delivery of clear recommendations to Board, (ii) revisions to the RISC charter that are intended to provide clarity on the role of the RISC, and (iii) the completion of an effort to extend and expand committee membership. Mr. Schaffeld also made mention of the RISC's upcoming Reliability Leadership Summit, scheduled to take place in September 2014. He thanked the Board for their continued involvement with RISC activities.

Upon motions duly made and seconded, the Board approved the following resolutions:

RISC Charter Amendments

RESOLVED, that the Board hereby approves the amended Reliability Issues Steering Committee (RISC) Charter, substantially in the form presented to the Board at this meeting, to replace the RISC Charter approved by the Board on August 16, 2012.

RISC Committee Membership Appointments

RESOLVED, that the Board hereby approves extensions to the current Reliability Issues Steering Committee (RISC) members' terms, as follows:

- MRC representative Scott Helyer, through May 2015
- MRC representative Jason Marshall, through May 2015
- At-large member and RISC chair Bob Schaffeld, through May 2016
- MRC representative John Twitty, through May 2015

FURTHER RESOLVED, that the Board hereby approves the following new members to the RISC:

Name	Title	Type of Membership	Term
Daniel Froetscher	Senior Vice President, Transmission, Distribution, and Customers, Arizona Public Service Company	At-Large Member	Two-year term ending May 2016
Ray Gorman	Chairman, New Brunswick Energy and Utilities Board	At-Large Member	Two-year term ending May 2016
Scot Hathaway	Vice President – Transmission, Dominion Virginia Power	At-Large Member	Two-year term ending May 2016
Duane Highley	President and CEO, Arkansas Electric Cooperative	At-Large Member	Two-year term ending May 2016
Nabil Hitti	Vice President, Transmission Network Operations, National Grid	Member Representatives Committee member to the RISC	Two-year term ending May 2016
Steve Whitley	President and CEO, New York ISO	At-Large Member	Two-year term ending May 2016
Terry Bilke	Consulting Advisor, Compliance Services, Midcontinent ISO	Compliance and Certification Committee member to the RISC	Two-year term ending May 2016

Compliance and Certification Committee

Mr. Terry Bilke, chair, reported on the activities of the three Compliance and Certification Committee ("CCC") subcommittees which included (i) involvement in the upcoming independent audit process, (ii) participation in the development of the Reliability Assurance Initiative ("RAI"), and (iii) monitoring of the ongoing risk-based registration project. He also thanked FERC staff for their involvement with the enforcement report. Mr. Bilke presented the 2014-2016 CCC Work Plan for Board approval, as well as the 2013 Stakeholder Perception Survey Report for Board acceptance.

Mr. Gorbet recognized that this is Mr. Bilke's last report to the Board as chair of the CCC and thanked him for his work. Mr. Gorbet welcomed the incoming CCC chair, Ms. Patti Metro.

Upon motions duly made and seconded, the Board approved the following resolutions:

CCC 2014-2016 Work Plan

RESOLVED, that the Board hereby approves the 2014-2016 Compliance and Certification Committee Work Plan, substantially in the form as presented to the Board at this meeting.

CCC 2013 Stakeholder Perception Survey Results and Report Recommendations

RESOLVED, that the Board hereby accepts the 2013 ERO Effectiveness and Stakeholder Perceptions Survey report, substantially in the form as presented to the Board at this meeting.

Electricity Sub-Sector Coordination Council

Mr. Cauley, executive committee member, reported on the recent activities of the Electricity Sub-Sector Coordination Council ("ESCC"), and some of its key focus areas. He described the committee's membership and structure, and stated that the committee is functioning as envisioned. Mr. Cauley also noted the involvement of Mr. Barber with the ESCC.

Forum and Group Reports

North American Energy Standards Board
Mr. Michael Desselle, chair, updated the Board on three matters: (i) the progress of the coordinated effort to retire Reliability Standards that contain commercial aspects, (ii) the development of the Parallel Flow Visualization Project, and (iii) the collaborative effort of North American Energy Standards Board ("NAESB") and NERC staff to support the implementation of the NAESB Electric Industry Registry.

Regional Entity Management Group
Mr. Scott Henry, chair, summarized the current key focus areas for the Regional Entity Management Group: (i) the Five-Year ERO assessment, (ii) the implementation of reforms to RAI and the associated training, (iii) work to fully implement the compliance auditor manual, and (iv) implementation of the new Bulk Electric System ("BES") definition and BES exception processes. Mr. Henry also stated that he appreciates the collaborative process that resulted in the successful development of common metrics but that more work must be done to track and trend their effectiveness. He noted that the joint meeting of the leadership of the regional Boards, the regional CEOs, and the NERC trustees was a success, and thanked Mr. Gorbet for hosting the joint meeting.

North American Transmission Forum
Mr. Galloway, president and CEO, summarized key collaborative efforts between NERC and the North American Transmission Forum, including an update on the 345kV breaker inspection, maintenance, and tracking process and preliminary work on the development of best practices regarding protection system misoperations. He also noted progress on ongoing work with the Electric Power Research

Institute on resiliency and with an effort to promote improved reliability of off-site power sources for nuclear power plants.

North American Generator Forum
Mr. Allen D. Schriver, chair, stated that in addition to the North American Generator Forum's ("NAGF") written report, the increased interactions between NAGF, NERC Staff, and the regions had led to the strengthening of processes and an increase in the quality of feedback received.

Board Committee Reports

Corporate Governance and Human Resources Committee
Ms. Schori, chair, summarized the recent meetings of the Corporate Governance and Human Resources Committee ("CGHRC"). She stated that the CGHRC met in closed session on April 23, 2014 to review management compensation and benefits, and to consider a deferred compensation plan for certain executives and other key employees. Ms. Schori noted that no action had been taken at the meeting and that the committee would continue to consider such a plan.

She reported also that the CGHRC met in open session on May 1, 2014. At that meeting, the committee reviewed a draft of the IRS Form 990, and received updates on both the 2014 corporate goals and NERC staffing. In addition, the committee recommended Board approval of proposed revisions to the Board of Trustees Compliance Committee mandate.

Upon motion duly made and seconded, the Board approved the following resolution:

Compliance Committee Mandate Amendments

RESOLVED, that the Board, upon recommendation of the Corporate Governance and Human Resources Committee, hereby approves the Compliance Committee Mandate, as presented to the Board at this meeting, to replace the Compliance Committee Mandate approved by the Board on May 9, 2012.

Board of Trustees Compliance Committee
Mr. Scherr reported that the Compliance Committee met in executive session on May 5, 2014, and in subsequent open session on May 6, 2014. He reported on some of the issues covered during those meetings, including (i) progress on RAI, (ii) the new processes for revising existing Reliability Standard Audit Worksheets ("RSAW") and management's work to finalize the document, and (iii) consideration of Compliance caseload statistics.

Finance and Audit Committee
Mr. Thilly, chair, reported that on May 6, 2014, the Finance and Audit Committee met in closed and open sessions. He reported that the committee reviewed and recommended Board acceptance of both the 2013 Audit Financial Statements and the First Quarter 2014 Unaudited Statement of Activities for NERC and the Regions. Mr. Thilly also provided an update on the development of the 2015

Business Plans and Budgets for NERC and the Regions and stated that the process has been refined to allow more time for stakeholder review and comment.

Upon motions duly made and seconded, the Board approved the following resolutions:

2013 Audit Financial Statements

RESOLVED, that the Board, upon recommendation of the Finance and Audit Committee, hereby accepts the 2013 Audit Financial Statements, as presented to the Board at this meeting.

First Quarter Unaudited Statement of Activities

RESOLVED, that the Board, upon recommendation of the Finance and Audit Committee, hereby accepts the NERC First Quarter 2014 Unaudited Statement of Activities, as presented to the Board at this meeting.

Enterprise-wide Risk Committee
Mr. Goulding, chair, reported that the first meeting of the Enterprise-wide Risk Committee took place in closed session on May 5, 2014. He indicated that the committee reviewed the 2014 Audit Plan, received an update on risk management activities, and reviewed the CCC's 2014-2016 Work Plan.

Standards Oversight and Technology Committee
Mr. Peterson, chair, stated that the Standards Oversight and Technology Committee met in open session on May 6, 2014. He reported that the committee received an update on the CIP Version 5 transition and that committee members engaged in an active discussion of issues and concerns raised with regard to ERO Enterprise IT Applications. Mr. Peterson indicated that committee members had taken a more active oversight role on those projects. He noted also that he believes there has been a significant improvement in the quality of NERC's work with regard to standards development over the last several years.

Closing Remarks of Chair Gorbet

Mr. Gorbet expressed his appreciation on behalf of the Board to all of those individuals who had made the Board meeting successful. He again thanked Commissioner Norris for attending and offering supportive and encouraging comments. Mr. Gorbet stated that NERC has grappled with many difficult issues at once, has been able to come to a successful resolution to many, and is well positioned for success when confronted with the challenges that are ahead. He commended the work of the NERC standing committees and expressed his satisfaction that Board members have and are continuing to become more involved with the work of the standing committees. Mr. Gorbet reiterated the importance of the MRC policy input process and indicated that the process would continue to be used and refined.

Adjournment

There being no further business, and upon motion duly made and seconded, the meeting was adjourned at 11:42 a.m. Eastern.

Submitted by,

Charles A. Berardesco
Corporate Secretary

Exhibit A

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Board of Trustees

May 7, 2014 | 8:30 a.m. - Noon Eastern

Hyatt Regency Philadelphia at Penn's Landing
201 S. Columbus Blvd.
Philadelphia, PA 19106
215-928-1234

Call to Order

NERC Antitrust Compliance Guidelines and Public Announcement

Consent Agenda — Approve

1. **Minutes***
   a. February 6, 2014 Meeting
2. **Committee Membership and Charter Changes***
   a. Compliance and Certification Committee Membership
   b. Compliance Processes and Procedures Subcommittee Formation
   c. Critical Infrastructure Protection Committee Membership
   d. Personnel Certification Governance Committee Membership

Regular Agenda

3. **Opening Remarks by Board Chair**
4. **Remarks by FERC Commissioner Cheryl LaFleur**
5. **Remarks by FERC Commissioner Tony Clark**
6. **Remarks by Mr. Denis O'Brien, CEO, Exelon Utilities**
7. **President's Report**

8. **Standards***
    a. Demand Data (MOD C) – MOD 031-1 — **Adopt**
    b. Voltage and Reactive Control – VAR-002-3 – **Adopt**
    c. Operating Personnel Communictions Protocols – COM-002-4 – **Adopt**
    d. Violation Risk Factor/Violation Severity Level Revisions – **Adopt**
        - TPL-001-4
        - CIP Version 5 (CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-008-5, CIP-009-5)
        - MOD-026-1 and MOD-027-1
        - PRC-005-2 and PRC-005-3
        - BAL-003-1
    e. Physical Security Standard — **Information**
9. **Amendments to SERC Bylaws* – Approve**
10. **State of Reliability Report*— Information**
11. **Summer Assessment*— Information**
12. **ERO Strategic Plan Metrics – Approve**
13. **Canadian Affairs – Jim Burpee — Information**
14. **Committee Reports***
    a. Operating Committee
    b. Planning Committee
    c. Critical Infrastructure Protection Committee
    d. Member Representatives Committee
    e. Personnel Certification Governance Committee
    f. Standards Committee
    g. Reliability Issues Steering Committee
        i. Charter Amendments – **Approve**
        ii. Committee Membership Appointments – **Approve**
    h. Compliance and Certification Committee
        i. 2014-2016 Work Plan – **Approve**
        ii. 2013 Stakeholder Perception Survey Results and Report Recommendations – **Accept**
    i. Electricity Sub-Sector Coordinating Council

15. **Forum and Group Reports***
    a. North American Energy Standards Board
    b. Regional Entity Management Group
    c. North American Transmission Forum
    d. North American Generator Forum
16. **Board Committee Reports**
    a. Corporate Governance and Human Resources
        i. Compliance Committee Mandate Amendments – **Approve**
    b. Compliance
    c. Finance and Audit
        i. 2013 Audit Financial Statements – **Accept**
        ii. First Quarter Statement of Activities – **Accept**
    d. Enterprise-wide Risk
    e. Standards Oversight and Technology

***Background materials included.**

Exhibit B

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Minutes
Board of Trustees

May 7, 2014 | 8:30 a.m.-12:00 p.m. Eastern

Hyatt Regency Philadelphia at Penn's Landing
201 S. Columbus Blvd.
Philadelphia, PA 19106

Call to Order and Chair's Remarks

Mr. Frederick W. Gorbet, chair, called to order the duly noticed open meeting of the Board of Trustees ("Board") of the North American Electric Reliability Corporation ("NERC") on May 7, 2014, at 8:30 a.m. Eastern, and a quorum was declared present. The agenda is attached as **Exhibit A**.

Present at the meeting were:

Board Members:
Frederick W. Gorbet, Chair
Paul F. Barber
Janice B. Case
Gerald W. Cauley, President and Chief Executive Officer
Robert G. Clarke
David Goulding
Douglas Jaeger
Kenneth G. Peterson
Bruce A. Scherr
Jan Schori
Roy Thilly

NERC Staff
Charles A. Berardesco, Senior Vice President, General Counsel, and Corporate Secretary
Thomas Burgess, Vice President and Director of Reliability Assessment and Performance Analysis
Howard Gugel, Director of Performance Analysis
Mark G. Lauby, Senior Vice President and Chief Reliability Officer
John Moura, Director of Reliability Assessment
Steven Noess, Associate Director of Standards Development
Janet Sena, Senior Vice President and Director of Policy and External Affairs
Brady Walker, Associate Counsel
Michael Walker, Senior Vice President, Chief Financial and Administrative Officer, and Corporate Treasurer

A listing of industry attendees is attached as **Exhibit B.**

Mr. Gorbet acknowledged and welcomed Mr. John R. Norris, Commissioner, Federal Energy Regulatory Commission ("FERC"), and Mr. Denis O'Brien, Chief Executive Officer of Exelon Utilities. He expressed regrets on behalf of Mr. Ken Quesnelle, Chair of the Canadian Association of Members of Public Utility Tribunals, who was not able to attend the meeting.

NERC Antitrust Compliance Guidelines

Mr. Berardesco directed the participants' attention to the NERC Antitrust Compliance Guidelines included in the agenda, and offered to answer any additional questions the participants had at any time regarding antitrust compliance or other matters.

Consent Agenda

Upon motion duly made and seconded, the Board approved the consent agenda as follows:

Minutes

The draft minutes for the February 6, 2014 Board meeting were approved in the form as presented to the Board at the meeting.

Compliance Processes and Procedures Subcommittee Formation

RESOLVED, that the Board hereby approves the elimination of the Compliance and Certification Committee's Standards Interface Subcommittee and Procedures Subcommittee.

FURTHER RESOLVED, that the Board hereby approves the formation of the Compliance Processes and Procedures Subcommittee.

Committee Membership Appointments

Critical Infrastructure Protection Committee

RESOLVED, that the Board hereby approves the appointment of the following individuals to the Critical Infrastructure Protection Committee ("CIPC") for a term of at least two years:

- Gary Mayfield of the Western Area Power Administration
- Ed Goff of Duke Energy

RESOLVED, that the Board hereby approves the election of the following individual to the Executive Committee of the CIPC for a term commencing May 7, 2014 and concluding December 31, 2015:

- David Revill of Georgia Transmission

Compliance and Certification Committee

RESOLVED, that the Board hereby appoints the following individuals to the Compliance and Certification Committee, each for a term of three years, effective May 7, 2014:

- Rick Terrill of Luminant Mining
- Caroline Dupuis of Hydro-Québec TransÉnergie
- William Temple of Northeast Utilities
- Jennifer Flandermeyer of Kansas City Power & Light

FURTHER RESOLVED, that the Board hereby appoints the following individuals as officers, each for a term of two years, effective July 1, 2014.

- Patti Metro of the National Rural Electric Cooperative Association, chair
- Jennifer Flandermeyer of Kansas City Power & Light, vice chair

Personnel Certification Governance Committee

RESOLVED, that the Board hereby appoints the following individual to the Personnel Certification Governance Committee for a term beginning May 7, 2014 and concluding December 31, 2015:

- Michael Hoke of PJM Interconnection

Executive Session

Mr. Gorbet reported that before the open meeting, as is its custom, the Board met in closed session with NERC management, and subsequently in executive session without NERC management, to review NERC management activities.

Mr. Gorbet also reported that on Monday, May 5, 2014, the Board met with the leadership of the Boards of the Regional Entities with Regional Entity chief executive officers present, and then without the CEOs in a subsequent executive session. Mr. Gorbet summarized the discussion and reported that these meetings have helped to improve communication at the governance level within the ERO Enterprise.

Welcoming Remarks

Mr. Gorbet welcomed and introduced Mr. Norris and Mr. O'Brien.

Remarks by John R. Norris

Mr. Norris remarked on the evolution of the relationship between FERC and NERC and stated he believed interactions between the two organizations had improved significantly. He praised the quality of NERC's work and commented on the overall positive direction of the organization. Mr. Norris thanked NERC leadership and staff for their response to and work on the Physical Security Order and the related proposed Reliability Standard. He noted that caution should be exercised when responding to political pressures to act, both now and in the future, and encouraged NERC to continue to take

action in the interest of reliability. Mr. Norris stated he was looking forward to continuing a productive working relationship with NERC.

Remarks by Denis O'Brien

Mr. Cauley provided a brief introduction of Mr. O'Brien.

Mr. O'Brien provided the Board with an overview of Exelon's investments in infrastructure and commitment to reliability. He highlighted the positive effects of NERC's outreach to and collaboration with the electric industry.

President's Report

Mr. Cauley provided comments on the evolution of the standards development process. He stated that the process has matured over the years and has benefitted from the high quality of FERC orders that allow industry to work collaboratively to arrive at the best and most efficient solutions for reliability. Mr. Cauley highlighted the flexibility and adaptability of the standards development process and cited the development of the proposed Physical Security Reliability Standard as an example of NERC's and industry's ability to respond to urgent issues. He praised the hard work of the standard drafting team members.

Mr. Cauley stated that the standards development process is working as it was envisioned with broad oversight from FERC, leadership from NERC's Board, and the effective application of technical expertise that leads to improved reliability, avoids undue compliance burdens, and serves the public interest.

Standards

Mr. Lauby provided an overview of the Reliability Standards program and presented the following items for Board action. After discussion, and upon motions duly made and seconded, the Board approved the following resolutions:

Demand Data (MOD C)—MOD-031-1

RESOLVED, that the Board hereby adopts proposed Reliability Standard MOD-031-1, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the associated implementation plan, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the revised and new NERC Glossary definitions, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Violation Risk Factors and Violation Severity Levels for the proposed Reliability Standard, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Reliability Standards proposed for retirement, as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities and take such further actions and make such further filings as are necessary and appropriate to effectuate the intent of the foregoing resolutions.

Voltage and Reactive Control—VAR-002-3

RESOLVED, that the Board hereby adopts proposed Reliability Standard VAR-002-3, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the associated implementation plan, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Violation Risk Factors and Violation Severity Levels for the proposed Reliability Standard, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Reliability Standard proposed for retirement, as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities and take such further actions and make such further filings as are necessary and appropriate to effectuate the intent of the foregoing resolutions.

Operating Personnel Communications Protocols—COM-002-4

RESOLVED, that the Board hereby adopts proposed Reliability Standard COM-002-4, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the associated implementation plan, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the new NERC Glossary definition, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Violation Risk Factors and Violation Severity Levels for the proposed Reliability Standard, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby approves the Requirement and Reliability Standards proposed for retirement, as presented to the Board at this meeting.

FURTHER RESOLVED, that the Board hereby rescinds its February 9, 2012 approval of the Interpretation of COM-002-2, effective (i) for U.S. registered entities upon implementation of COM-002-4 in substantially the form approved by the Board and (ii) for Canadian entities, effective upon implementation of COM-002-4 in substantially the form approved by the Board.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities and take such further actions and make such further filings as are necessary and appropriate to effectuate the intent of the foregoing resolutions.

Violation Risk Factor/Violation Severity Level Revisions

RESOLVED, that the Board hereby adopts proposed Violation Risk Factor and Violation Severity Level Modifications for the following Reliability Standards, as presented to the Board at this meeting:

- TPL-001-4—Transmission System Planning Performance Requirements
- CIP-003-5—Cyber Security—System Management Controls
- CIP-004-5.1—Cyber Security—Personnel and Training
- CIP-006-5—Cyber Security—Physical Security of BES Cyber Systems
- CIP-008-5—Cyber Security—Incident Reporting and Response Planning
- CIP-009-5—Cyber Security—Recovery Plans for BES Cyber Systems
- MOD-026-1—Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions
- MOD-027-1—Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions
- PRC-005-2—Protection System Maintenance
- PRC-005-3—Protection System and Automatic Reclosing Maintenance
- BAL-003-1—Frequency Response and Frequency Bias Setting

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities and take such further actions and make such further filings as are necessary and appropriate to effectuate the intent of the foregoing resolutions.

Physical Security Reliability Standard Development

Mr. Lauby introduced Mr. Noess who announced that the proposed Physical Security Reliability Standard had received final industry approval. He thanked the standard drafting team, the Standards Committee, and industry stakeholders for their collaborative efforts on this project. Mr. Noess indicated that NERC staff would begin to prepare the proposed Reliability Standard for approval by the NERC Board at a future meeting.

Mr. Brian Murphy, chair of the Standards Committee ("SC"), praised the collaborative nature of the development process and stated that the approach to development on this project could benefit all future standards development projects.

Amendments to SERC Bylaws

Mr. Berardesco presented a set of proposed amendments to the SERC Reliability Corporation Bylaws. He stated that the amendments reflect a decision made by SERC regarding its tax status and that these changes do not impact SERC's ability to operate as a Regional Entity. Mr. Berardesco indicated Board approval was required because the Bylaws are an exhibit to the delegation agreement and noted that FERC will also need to approve the amendments.

Upon motion duly made and seconded, the Board approved the following resolution:

WHEREAS, the SERC Board of Directors has proposed amendments to the Delegation Agreement between NERC and SERC ("Delegation Agreement") by amending Exhibit B – the SERC Bylaws.

WHEREAS, the proposed amendments do not affect SERC's Regional Entity functions.

WHEREAS, the proposed amendments continue to satisfy the governance criteria specified in the Delegation Agreement.

RESOLVED, that the Board hereby approves the proposed amendments to NERC's Delegation Agreement with SERC, consisting of amendments to Exhibit B – the SERC Bylaws, in the form as presented to the Board at this meeting.

FURTHER RESOLVED, that NERC management is hereby authorized to make the appropriate filings with ERO governmental authorities.

State of Reliability Report

Mr. Burgess provided an introduction to the State of Reliability Report ("SORR"). He explained that the SORR is developed by NERC's Reliability Assessment and Performance Analysis group, stakeholders, and regional assessment groups. Mr. Burgess stated the SORR utilizes a variety of data, event analyses, and historical performance information to identify trends and indicators related to Bulk-Power System performance and reliability. With that information, NERC and stakeholders are able to take proactive steps to focus on key areas of reliability performance.

Mr. Gugel provided an overview of the 2014 SORR. He stated the SORR represents NERC's independent view of ongoing Bulk-Power System trends through an objective analysis of the state of reliability. The SORR's key findings serve as guide to risk assessment, reliability standards development project prioritization, compliance and enforcement process improvement, event analysis, and critical infrastructure protection. Mr. Gugel presented a summary of the keys findings and recommendations, a copy of which was included with the advance meeting materials.

Summer Reliability Assessment

Mr. Burgess provided an overview of the Summer Reliability Assessment. He indicated that NERC provides seasonal assessments that describe anticipated conditions and key areas for focus and

attention during upcoming summer seasonal conditions. Mr. Moura presented a summary of the key findings and recommendations, a copy of which was included with the advance meeting materials.

ERO Strategic Plan Metrics

Mr. Cauley provided an overview of the Three-Year ERO Strategic Plan approval process. He noted that the Board approved the Strategic Plan without the plan metrics at its February 2014 meeting, so as to allow management to refine a few of the metrics to reflect industry comments. Mr. Cauley presented a summary of the revisions and indicated that the metrics are intended to provide guidance for achieving the goals outlined in the Strategic Plan. He stated that both the Strategic Plan and metrics will be updated as necessary.

Upon motion duly made and seconded, the Board approved the following resolution:

RESOLVED, that the Board hereby approves the metrics for use with the ERO Strategic Plan, as presented to the Board at this meeting.

Canadian Affairs

Mr. James Burpee, President and CEO of the Canadian Electricity Association, presented an update on current Canadian reliability-related initiatives.

Standing Committee Reports

Representatives of the Standing Committees provided reports to the Board highlighting items from their written reports as contained within the agenda package.

Operating Committee

Mr. James D. Castle, chair, highlighted some of the Operating Committee's ("OC") activities since the last Board meeting. He thanked Trustees Jaeger and Barber for their attendance at the OC's March meeting and stated the OC is looking forward to welcoming Ms. Case and Mr. Gorbet at future meetings. Mr. Castle praised the Board for their commitment to engaging with the OC. He also provided updates on the OC's work on (i) the Essential Reliability Services Taskforce, (ii) the cold weather preparedness reliability guideline, (iii) the independent experts' report, and (iv) improvements to the organization and structure of the OC.

Planning Committee

Mr. Benjamin Crisp, chair, reviewed progress on some of the Planning Committee's ("PC") key initiatives. He outlined the PC's work in helping to develop the Summer Reliability Assessment and State of Reliability Report. Mr. Crisp also summarized the PC's work with the GMD taskforce and efforts to provide technical basis and justification to that project's standard drafting team. He provided an overview of the PC's process changes which are intended to allow for more feedback from the regions and an increased ability to reprioritize projects within the PC as necessary. Mr. Crisp thanked the Trustees for their active participation with the PC.

Critical Infrastructure Protection Committee

Mr. Charles F. Abell, chair, briefly summarized the ongoing work of the CIPC. He highlighted the issuance of two reports related to NERC's GridEx II, one for the distributed play exercise and one for the executive table top exercise. Mr. Abell stated that the CIPC was actively engaged in implementing the recommendations and addressing the concerns identified in the reports. He also highlighted the strong attendance at and feedback from the CIPC technical workshops and stated that planning was underway for another workshop in June focusing on physical security issues.

Member Representatives Committee

Mr. John A. Anderson, chair, thanked Mr. Gorbet and the Board for the continued use of the Member Representatives Committee's ("MRC") policy input, and summarized the issues that had been discussed at the MRC meeting the previous day. He stated he was appreciative of new meeting structure and recognized MRC members for attending Board Committee meetings.

Personnel Certification Governance Committee

Mr. Brett Hallborg, chair, was not in attendance. Mr. Gorbet referred the meeting participants to the written report of the Personnel Certification and Governance Committee, located in the agenda package.

Standards Committee

Mr. Murphy expressed his gratitude for the good working relationship between the SC and the Board, NERC staff, industry, and the staff of FERC. He outlined work that was ongoing on a number of projects and initiatives including (i) coordination between the SC and the Reliability Issues Steering Committee ("RISC"), (ii) the Reliability Standards Development Plan and its relation to the newly approved ERO Strategic Plan metrics, and (iii) the development of an evaluation framework to be used in conjunction with the metrics.

Reliability Issues Steering Committee

Mr. Robert A. Schaffeld, chair, outlined some of the recent activities of the Reliability Issues Steering Committee ("RISC") including (i) several process improvements intended to assist with the delivery of clear recommendations to Board, (ii) revisions to the RISC charter that are intended to provide clarity on the role of the RISC, and (iii) the completion of an effort to extend and expand committee membership. Mr. Schaffeld also made mention of the RISC's upcoming Reliability Leadership Summit, scheduled to take place in September 2014. He thanked the Board for their continued involvement with RISC activities.

Upon motions duly made and seconded, the Board approved the following resolutions:

RISC Charter Amendments

RESOLVED, that the Board hereby approves the amended Reliability Issues Steering Committee (RISC) Charter, substantially in the form presented to the Board at this meeting, to replace the RISC Charter approved by the Board on August 16, 2012.

RISC Committee Membership Appointments

RESOLVED, that the Board hereby approves extensions to the current Reliability Issues Steering Committee (RISC) members' terms, as follows:

- MRC representative Scott Helyer, through May 2015
- MRC representative Jason Marshall, through May 2015
- At-large member and RISC chair Bob Schaffeld, through May 2016
- MRC representative John Twitty, through May 2015

FURTHER RESOLVED, that the Board hereby approves the following new members to the RISC:

Name	Title	Type of Membership	Term
Daniel Froetscher	Senior Vice President, Transmission, Distribution, and Customers, Arizona Public Service Company	At-Large Member	Two-year term ending May 2016
Ray Gorman	Chairman, New Brunswick Energy and Utilities Board	At-Large Member	Two-year term ending May 2016
Scot Hathaway	Vice President – Transmission, Dominion Virginia Power	At-Large Member	Two-year term ending May 2016
Duane Highley	President and CEO, Arkansas Electric Cooperative	At-Large Member	Two-year term ending May 2016
Nabil Hitti	Vice President, Transmission Network Operations, National Grid	Member Representatives Committee member to the RISC	Two-year term ending May 2016
Steve Whitley	President and CEO, New York ISO	At-Large Member	Two-year term ending May 2016
Terry Bilke	Consulting Advisor, Compliance Services, Midcontinent ISO	Compliance and Certification Committee member to the RISC	Two-year term ending May 2016

Compliance and Certification Committee

Mr. Terry Bilke, chair, reported on the activities of the three Compliance and Certification Committee ("CCC") subcommittees which included (i) involvement in the upcoming independent audit process, (ii) participation in the development of the Reliability Assurance Initiative ("RAI"), and (iii) monitoring of the ongoing risk-based registration project. He also thanked FERC staff for their involvement with the enforcement report. Mr. Bilke presented the 2014-2016 CCC Work Plan for Board approval, as well as the 2013 Stakeholder Perception Survey Report for Board acceptance.

Mr. Gorbet recognized that this is Mr. Bilke's last report to the Board as chair of the CCC and thanked him for his work. Mr. Gorbet welcomed the incoming CCC chair, Ms. Patti Metro.

Upon motions duly made and seconded, the Board approved the following resolutions:

CCC 2014-2016 Work Plan

RESOLVED, that the Board hereby approves the 2014-2016 Compliance and Certification Committee Work Plan, substantially in the form as presented to the Board at this meeting.

CCC 2013 Stakeholder Perception Survey Results and Report Recommendations

RESOLVED, that the Board hereby accepts the 2013 ERO Effectiveness and Stakeholder Perceptions Survey report, substantially in the form as presented to the Board at this meeting.

Electricity Sub-Sector Coordination Council

Mr. Cauley, executive committee member, reported on the recent activities of the Electricity Sub-Sector Coordination Council ("ESCC"), and some of its key focus areas. He described the committee's membership and structure, and stated that the committee is functioning as envisioned. Mr. Cauley also noted the involvement of Mr. Barber with the ESCC.

Forum and Group Reports

North American Energy Standards Board
Mr. Michael Desselle, chair, updated the Board on three matters: (i) the progress of the coordinated effort to retire Reliability Standards that contain commercial aspects, (ii) the development of the Parallel Flow Visualization Project, and (iii) the collaborative effort of North American Energy Standards Board ("NAESB") and NERC staff to support the implementation of the NAESB Electric Industry Registry.

Regional Entity Management Group
Mr. Scott Henry, chair, summarized the current key focus areas for the Regional Entity Management Group: (i) the Five-Year ERO assessment, (ii) the implementation of reforms to RAI and the associated training, (iii) work to fully implement the compliance auditor manual, and (iv) implementation of the new Bulk Electric System ("BES") definition and BES exception processes. Mr. Henry also stated that he appreciates the collaborative process that resulted in the successful development of common metrics but that more work must be done to track and trend their effectiveness. He noted that the joint meeting of the leadership of the regional Boards, the regional CEOs, and the NERC trustees was a success, and thanked Mr. Gorbet for hosting the joint meeting.

North American Transmission Forum
Mr. Galloway, president and CEO, summarized key collaborative efforts between NERC and the North American Transmission Forum, including an update on the 345kV breaker inspection, maintenance, and tracking process and preliminary work on the development of best practices regarding protection system misoperations. He also noted progress on ongoing work with the Electric Power Research

Institute on resiliency and with an effort to promote improved reliability of off-site power sources for nuclear power plants.

North American Generator Forum
Mr. Allen D. Schriver, chair, stated that in addition to the North American Generator Forum's ("NAGF") written report, the increased interactions between NAGF, NERC Staff, and the regions had led to the strengthening of processes and an increase in the quality of feedback received.

Board Committee Reports

Corporate Governance and Human Resources Committee
Ms. Schori, chair, summarized the recent meetings of the Corporate Governance and Human Resources Committee ("CGHRC"). She stated that the CGHRC met in closed session on April 23, 2014 to review management compensation and benefits, and to consider a deferred compensation plan for certain executives and other key employees. Ms. Schori noted that no action had been taken at the meeting and that the committee would continue to consider such a plan.

She reported also that the CGHRC met in open session on May 1, 2014. At that meeting, the committee reviewed a draft of the IRS Form 990, and received updates on both the 2014 corporate goals and NERC staffing. In addition, the committee recommended Board approval of proposed revisions to the Board of Trustees Compliance Committee mandate.

Upon motion duly made and seconded, the Board approved the following resolution:

Compliance Committee Mandate Amendments

RESOLVED, that the Board, upon recommendation of the Corporate Governance and Human Resources Committee, hereby approves the Compliance Committee Mandate, as presented to the Board at this meeting, to replace the Compliance Committee Mandate approved by the Board on May 9, 2012.

Board of Trustees Compliance Committee
Mr. Scherr reported that the Compliance Committee met in executive session on May 5, 2014, and in subsequent open session on May 6, 2014. He reported on some of the issues covered during those meetings, including (i) progress on RAI, (ii) the new processes for revising existing Reliability Standard Audit Worksheets ("RSAW") and management's work to finalize the document, and (iii) consideration of Compliance caseload statistics.

Finance and Audit Committee
Mr. Thilly, chair, reported that on May 6, 2014, the Finance and Audit Committee met in closed and open sessions. He reported that the committee reviewed and recommended Board acceptance of both the 2013 Audit Financial Statements and the First Quarter 2014 Unaudited Statement of Activities for NERC and the Regions. Mr. Thilly also provided an update on the development of the 2015

Business Plans and Budgets for NERC and the Regions and stated that the process has been refined to allow more time for stakeholder review and comment.

Upon motions duly made and seconded, the Board approved the following resolutions:

2013 Audit Financial Statements

RESOLVED, that the Board, upon recommendation of the Finance and Audit Committee, hereby accepts the 2013 Audit Financial Statements, as presented to the Board at this meeting.

First Quarter Unaudited Statement of Activities

RESOLVED, that the Board, upon recommendation of the Finance and Audit Committee, hereby accepts the NERC First Quarter 2014 Unaudited Statement of Activities, as presented to the Board at this meeting.

Enterprise-wide Risk Committee
Mr. Goulding, chair, reported that the first meeting of the Enterprise-wide Risk Committee took place in closed session on May 5, 2014. He indicated that the committee reviewed the 2014 Audit Plan, received an update on risk management activities, and reviewed the CCC's 2014-2016 Work Plan.

Standards Oversight and Technology Committee
Mr. Peterson, chair, stated that the Standards Oversight and Technology Committee met in open session on May 6, 2014. He reported that the committee received an update on the CIP Version 5 transition and that committee members engaged in an active discussion of issues and concerns raised with regard to ERO Enterprise IT Applications. Mr. Peterson indicated that committee members had taken a more active oversight role on those projects. He noted also that he believes there has been a significant improvement in the quality of NERC's work with regard to standards development over the last several years.

Closing Remarks of Chair Gorbet

Mr. Gorbet expressed his appreciation on behalf of the Board to all of those individuals who had made the Board meeting successful. He again thanked Commissioner Norris for attending and offering supportive and encouraging comments. Mr. Gorbet stated that NERC has grappled with many difficult issues at once, has been able to come to a successful resolution to many, and is well positioned for success when confronted with the challenges that are ahead. He commended the work of the NERC standing committees and expressed his satisfaction that Board members have and are continuing to become more involved with the work of the standing committees. Mr. Gorbet reiterated the importance of the MRC policy input process and indicated that the process would continue to be used and refined.

Adjournment

There being no further business, and upon motion duly made and seconded, the meeting was adjourned at 11:42 a.m. Eastern.

Submitted by,

Charles A. Berardesco
Corporate Secretary

Exhibit A

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Board of Trustees

May 7, 2014 | 8:30 a.m. - Noon Eastern

Hyatt Regency Philadelphia at Penn's Landing
201 S. Columbus Blvd.
Philadelphia, PA 19106
215-928-1234

Call to Order

NERC Antitrust Compliance Guidelines and Public Announcement

Consent Agenda — Approve

1. **Minutes***
   a. February 6, 2014 Meeting
2. **Committee Membership and Charter Changes***
   a. Compliance and Certification Committee Membership
   b. Compliance Processes and Procedures Subcommittee Formation
   c. Critical Infrastructure Protection Committee Membership
   d. Personnel Certification Governance Committee Membership

Regular Agenda

3. **Opening Remarks by Board Chair**
4. **Remarks by FERC Commissioner Cheryl LaFleur**
5. **Remarks by FERC Commissioner Tony Clark**
6. **Remarks by Mr. Denis O'Brien, CEO, Exelon Utilities**
7. **President's Report**

8. **Standards***
    a. Demand Data (MOD C) – MOD 031-1 — **Adopt**
    b. Voltage and Reactive Control – VAR-002-3 – **Adopt**
    c. Operating Personnel Communictions Protocols – COM-002-4 – **Adopt**
    d. Violation Risk Factor/Violation Severity Level Revisions – **Adopt**
        - TPL-001-4
        - CIP Version 5 (CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-008-5, CIP-009-5)
        - MOD-026-1 and MOD-027-1
        - PRC-005-2 and PRC-005-3
        - BAL-003-1
    e. Physical Security Standard — **Information**
9. **Amendments to SERC Bylaws* – Approve**
10. **State of Reliability Report*— Information**
11. **Summer Assessment*— Information**
12. **ERO Strategic Plan Metrics – Approve**
13. **Canadian Affairs – Jim Burpee — Information**
14. **Committee Reports***
    a. Operating Committee
    b. Planning Committee
    c. Critical Infrastructure Protection Committee
    d. Member Representatives Committee
    e. Personnel Certification Governance Committee
    f. Standards Committee
    g. Reliability Issues Steering Committee
        i. Charter Amendments – **Approve**
        ii. Committee Membership Appointments – **Approve**
    h. Compliance and Certification Committee
        i. 2014-2016 Work Plan – **Approve**
        ii. 2013 Stakeholder Perception Survey Results and Report Recommendations – **Accept**
    i. Electricity Sub-Sector Coordinating Council

15. **Forum and Group Reports***
    a. North American Energy Standards Board
    b. Regional Entity Management Group
    c. North American Transmission Forum
    d. North American Generator Forum
16. **Board Committee Reports**
    a. Corporate Governance and Human Resources
        i. Compliance Committee Mandate Amendments – **Approve**
    b. Compliance
    c. Finance and Audit
        i. 2013 Audit Financial Statements – **Accept**
        ii. First Quarter Statement of Activities – **Accept**
    d. Enterprise-wide Risk
    e. Standards Oversight and Technology

***Background materials included.**

Exhibit B

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Reliability Issues Steering Committee

May 7, 2014 | 12:30 p.m. – 2:30 p.m. EDT

ReadyTalk Conference
Audio Dial In: 866-740-1260 | Access Code 9473885 | Security Code 5741587
On the web at www.readytalk.com

Introductions and Chair's Remarks

NERC Antitrust Compliance Guidelines and Public Announcement

Agenda Items

1. **Board Meeting Update — (Discussion)**
2. **Reliability Leadership Summit — (Review, Discussion)**
3. **2015-2017 RSDP, Reliability Standards Development Plan — (Review, Discussion)**
4. **Risk Management Projects *— (Review, Discussion)**
5. **Committee Reports— (Discussion)**

   Status on matters as it pertains to the RISC

   a. Operating Committee
   b. Planning Committee
   c. Critical Infrastructure Committee
   d. Compliance and Certification Committee
   e. Standards Committee
6. **Review Future Meetings**
   a. June 17, 2014 8:00-5:00 CDT - In-Person Meeting Chicago, IL
   b. July 10, 2014 9:00-12:00 EDT - Conference Call
   c. August 14, 2014 12:30-2:30 PDT - Post-BOT Meeting, Vancouver, BC
   d. September 11, 2014 9:30-4:30 EDT - Reliability Leadership Summit, Washington, DC
   e. September 12, 2014 8:00-2:30 EDT - In-Person Meeting, Washington, DC
   f. October 07, 2014 9:00-12:00 EDT - Conference Call
   g. November 13, 2014 12:30-2:30 EST - Post-BOT Meeting, Atlanta, GA
   h. December 02, 2014 8:00-5:00 MST - In-Person Meeting, Phoenix, AZ
7. **Adjourn**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Reliability Issues Steering Committee

May 7, 2014 | 12:30 p.m. – 2:30 p.m. EDT

Hyatt Regency Philadelphia at Penn's Landing
201 South Columbus Blvd
Philadelphia, PA and ReadyTalk Conference Call

Introductions and Chair's Remarks

Chair Schaffeld and Secretary Burgess welcomed the new members and thanked the outgoing members for their contributions.

RISC Member Attendance:

Bob Schaffeld – Present
Jim Brenton – Present
Jim Case – Not Present
Sylvain Clermont – Present, outgoing member
Ben Crisp – Present
Daniel Froetscher – Not present, newly elected
Ray Gorman – Present
Scot Hathaway – Not Present, newly elected
Scott Helyer – Not Present
Duane Highley – Not Present, newly elected
Nabil Hitti – Present, newly elected
Jason Marshall – Present
Brian Murphy –Present
Clay Smith – Not present, outgoing member
John Twitty – Present
Andy Rodriquez – Present, outgoing member
Steve Whitley – Present, new member
Thomas Burgess – Present, new member

A number of observers attended the meeting including NERC Board of Trustees Chair, Fred Gorbet.

NERC Antitrust Compliance Guidelines and Public Announcement

Gugel reviewed the anti-trust guidance and the public meeting notification.

Agenda Items Were Reordered in the Meeting:

Item 1 - Board Meeting Update

A roundtable was conducted on Board meeting highlights.

Item 2 - Reliability Leadership Summit

- The FERC technical conference will be held in July. This conference compliments the Reliability Leadership Summit.
- For the Summit, the refined agenda was discussed and a number of recommendations were provided.

Actions:

- *Schaffeld and Burgess plan to invite the no-brainer panelists by the June RISC meeting.*
- *RISC members should provide contact information for panelists as well as the rationale for their selection to Schaffeld and Burgess.*

Item 3 - Review Future Meetings

- June 17, 2014 8:00-5:00 CDT - In-Person Meeting Atlanta, GA
    - This meeting was originally scheduled to be in Chicago, IL.
- July 10, 2014 9:00-12:00 EDT - Conference Call
- August 14, 2014 12:30-2:30 PDT - Post- Board of Trustees Meeting, Vancouver, BC
- September 11, 2014 9:30-4:30 EDT - Reliability Leadership Summit, Washington, DC
- September 12, 2014 8:00-2:30 EDT - In-Person Meeting, Washington, DC
- October 07, 2014 9:00-12:00 EDT - Conference Call
- November 13, 2014 12:30-2:30 EST - Post- Board of Trustees Meeting, Atlanta, GA
- December 02, 2014 8:00-5:00 MST - In-Person Meeting, Phoenix, AZ

Item 4 - 2015:2017 RSDP, Reliability Standards Development Plan

Murphy will provide an overview of this plan at the RISC meeting in June.

Actions:

- *Overview to include:*
    - *Any plans for outreach to the technical committees or other entities*
    - *Information on how the RISC should move forward on integrating triaged reliability assessments into the plan*

Item 5 - Risk Management Projects

A dialogue on how best to represent a "dashboard" of risk projects was facilitated by Burgess and Gugel.

Actions:

- *Dialogue to continue at the RISC meeting in June.*
- *ERO Top Priority Reliability Risks 2014-2017 to be part of the new member orientation in June.*

Item 6 - Committee Reports

a. Operating Committee– no update (member not present)

b. Planning Committee – Conducting scenario analysis for Adaptation and Planning for Change

c. Critical Infrastructure Protection Committee – Continuing with on-going activity

d. Compliance and Certification Committee – Focus is on risk based registration

e. Standards Committee – Refer to RSDP update.

Item 7 - Adjourn

There being no additional business to conduct, the meeting was adjourned.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Summary Agenda
2014 Reliability Leadership Summit

September 11, 2014 9:30a.m. – 4:30p.m.

Washington Marriott at Metro Center
775 12th St NW, Washington, DC

In Person Only

Welcome Remarks 9:30am – 9:45am

Bob Schaffeld, Vice President, Transmission, Southern Company; Chair of the RISC
Gerry Cauley, President and CEO, NERC

Morning Keynote Speaker 9:45am – 10:15am

Cheryl LaFleur?

Panel 1 – Changing Resource Mix, New Technologies, and the Impacts on Operations
10:15am – 11:15am

Our industry is undergoing fundamental change. Fuel prices, environmental regulations, and legislative support for renewable energy initiatives change not only how the bulk power system is planned, but how equipment and resources are being operated, controlled, and dispatched. New technologies (wind, solar, microgrids, plug-in hybrids, storage, PMUs, etc.) are also having an impact.

The convergence of large quantities of variable generation resources, the increase in gas-fired generation, and the retirement of conventional coal and nuclear generation resources, requires a complete rethinking on the way the industry assesses resource adequacy and essential reliability services. A change in resources means a change in operating characteristics. Newer generation technologies behave inherently different than traditional means of producing electricity.

How are these changes or the pace of change impacting our ability to plan for reliability? What new technologies present the most challenges for the industry to overcome? Are different approaches to operations or planning needed to address the changes facing us? What are the main policy drivers that should be considered so there is no impact to reliability?

Panelists:
General Panel Structure: 5 panelists, 5 minute opening remarks, 30 minutes of Q&A

Who are the panelists?

- RTOs?
- ERCOT
- CAISO
- MISO
- NE (gas dependency?)
- RCs?

Morning Break 11:15am – 11:30am

Panel 2 – Resource Adequacy and Complex Interdependencies 11:30am - 12:30pm

Ensuring North America has enough resources to meet changing demand is a critical component to reliability. The bulk power system was designed to use a portfolio of large-scale, synchronous generators to produce electricity and supply it to consumers through an interconnected high-voltage transmission backbone and a medium- and low-voltage distribution system. In North America, the power system is anchored by over a million megawatts of central station generation.

However, as the composition of the resource portfolio changes, complex risks to the industry are being identified. For example, the effect of increased reliance on natural gas for electric power and resource adequacy, the role of natural gas and electric storage, and the continued growth of demand and distributed resources are all vital components for ensuring future electric reliability.

Addressing these interdependent risks requires innovative problem solving. Industry leaders and policy-makers need to address these challenges and give them due consideration to ensure future BPS reliability is maintained.

How should the characteristics of essential reliability services be addressed given that the industry is a crossroads? Does the industry need to consider other metrics for assessing resource adequacy, beyond reserve margins? How should interdependences on gas and coal fuel resources be addressed? Wind and other variable resources? Given extreme conditions that plague many areas, such as hurricanes and drought, how should these considerations impact resource adequacy targets? Are requirements necessary?

Panelists:
General Panel Structure: 5 panelists, 5 minute opening remarks, 30 minutes of Q&A

Who are the panelists? Tom Burgess/John Moura (LTRA tie-in)? Others?

- MISO #2
- NPCC
- ERCOT – Ken McIntyre
- California
- PJM for changing reserve margins

Lunch 12:30pm – 1:30pm

Afternoon Keynote Speaker 1:30pm – 2:00pm

Focus on 9/11 or other major event. Black swan. Response, resiliency, recovery. Who should this be?

Panel 3 – Preparing for the Worst: Resiliency and Recovery 2:00pm – 3:00pm

Risks managers understand that beyond efforts to prevent a risk from manifesting, there are other ways to manage risk. Mitigation is taking appropriate action to reduce the impact of a risk when it does manifest. Because the bulk-power system has been designed to be reliable, incremental changes to reduce the likelihood of an event become cost prohibitive fairly quickly. However, focused efforts to reduce the size or duration of any event also serve to manage reliability risk.

What is resiliency? Are we doing all we can to ensure it? How best can the industry work together to support resiliency and recovery? What should the industry do to be prepared and ready for extreme weather events?

Panelists:

TBD; General Panel Structure: 5 panelists, 5 minute opening remarks, 30 minutes of Q&A

Who are the panelists?

- PGE
- Dominion
- DOE?
- FERC?
- Others?

Afternoon Break 3:00pm – 3:15pm

Panel 4– Leadership Round Table: Next Steps for Reliability 3:15pm – 4:15pm

Based on insights and themes presented, as well as others, this open-format discussion is intended to encourage leaders from industry to share thoughts and ideas relative to priority and significance of these reliability risks and relative priority steps to address.

Panelists:
Moderator – Bob Schaffeld
TBD; Round Table Structure: 10 panelists, 3 minute opening remarks, 25 minutes of discussion
Who are the panelists?

- Steve Whitely and/or Duane Highley?
- Billy Ball, Southern CTO?
- PA Consulting's "Reliability One" award winner(s)? PSEG, CONED, WE Energies, KCPL, or SDGE?
- Mike Bardee?
- Terry Boston?
- Jim Jura
- Caren Anders
- Others?

Closing Remarks 4:15pm – 4:30pm
Gerry Cauley, President and CEO of NERC

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

FAC-003-3 – Transmission Vegetation Management

This section must be completed by the Compliance Enforcement Authority.

Compliance Enforcement Authority:	
Registered Entity Name:	
NCR Number:	
Applicable Function(s): Applicable only for TO and GO	
Compliance Assessment Date:	
Compliance Monitoring Method:	
RSAW Version:	RSAW_FAC-003-3_2014_v2
Revision Date:	April 23, 2014
Names of Auditors:	

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

Subject Matter Experts

Identify Subject Matter Expert(s) responsible for this Reliability Standard. (Insert additional rows if necessary)

Registered Entity Response (Required):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

Requirement

R1. Each applicable Transmission Owner and applicable Generator Owner shall manage vegetation to prevent encroachments into the Minimum Vegetation Clearance Distance (MVCD) of its applicable line(s) which are either an element of an IROL, or an element of a Major WECC Transfer Path; operating within their Rating and all Rated Electrical Operating Conditions of the types shown below[2]:

1. An encroachment into the MVCD as shown in FAC-003-Table 2, observed in Real-time, absent a Sustained Outage,[3]
2. An encroachment due to a fall-in from inside the ROW that caused a vegetation-related Sustained Outage,[4]
3. An encroachment due to the blowing together of applicable lines and vegetation located inside the ROW that caused a vegetation-related Sustained Outage,[4]
4. An encroachment due to vegetation growth into the MVCD that caused a vegetation-related Sustained Outage.[4]

Measure

M1. Each applicable Transmission Owner and applicable Generator Owner has evidence that it managed vegetation to prevent encroachment into the MVCD as described in R1. Examples of acceptable forms of evidence may include dated attestations, dated reports containing no Sustained Outages associated with encroachment types 2 through 4 above, or records confirming no Real-time observations of any MVCD encroachments.

Questions for Registered Entity

Question: Does the applicable Generator Owner own overhead transmission lines that (1) extend greater than one mile or 1.609 kilometers beyond the fenced area of the generating station switchyard to the point of interconnection with a Transmission Owner's Facility or (2) do not have a clear line of sight4 from the generating station switchyard fence to the point of interconnection with a Transmission Owner's Facility? ☐ Yes ☐ No

If Yes, provide a list of the applicable transmission lines and respond to the following Questions.

Registered Entity Response to Question **(Required)**:

[2] This requirement does not apply to circumstances that are beyond the control of a applicable Transmission Owner or applicable Generator Owner subject to this reliability standard, including natural disasters such as earthquakes, fires, tornados, hurricanes, landslides, wind shear, fresh gale, major storms as defined either by the applicable Transmission Owner or applicable Generator Owner or an applicable regulatory body, ice storms, and floods; human or animal activity such as logging, animal severing tree, vehicle contact with tree, or installation, removal, or digging of vegetation. Nothing in this footnote should be construed to limit the Transmission Owner's or applicable Generator Owner's right to exercise its full legal rights on the ROW.

[3] If a later confirmation of a Fault by the applicable Transmission Owner or applicable Generator Owner shows that a vegetation encroachment within the MVCD has occurred from vegetation within the ROW, this shall be considered the equivalent of a Real-time observation.

[4] Multiple Sustained Outages on an individual line, if caused by the same vegetation, will be reported as one outage regardless of the actual number of outages within a 24-hour period.

Question: Does the applicable Transmission Owner or Generator Owner own overhead transmission lines that are either an element of an IROL or an element of a Major WECC Transfer Path? ☐ Yes ☐ No

If Yes, provide a list of the applicable transmission lines and respond to the next Question.

Registered Entity Response to Question **(Required)**:

Question: Did the applicable Transmission Owner or Generator Owner have any encroachment (Types 1-4) into the MVCD of its applicable line(s) in the audit period? ☐ Yes ☐ No

If Yes, describe the encroachment(s).

Registered Entity Response to Question **(Required)**:

Registered Entity Response (Required):

Describe, in narrative form, how you meet compliance with this Requirement.

Registered Entity Evidence Listing (Required):

Provide the following for all evidence submitted (Insert additional rows if necessary):
File Name, File Extension, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description

1.
2.
3.

Audit Team Evidence Reviewed

This section must be completed by the Compliance Enforcement Authority

1.
2.
3.

Compliance Assessment Approach Specific to FAC-003-3, R1

This section must be completed by the Compliance Enforcement Authority

Review the evidence to verify the Registered Entity has performed the following:

	Responded to the Questions and provided evidence of compliance if it owns applicable line(s).
	Managed vegetation to prevent encroachments into the Minimum Vegetation Clearance Distance (MVCD) as follows:
	• No Real-time observations of any MVCD encroachments absent a Sustained Outage (type 1) or;
	• No Sustained Outages associated with encroachment types 2 through 4 or;
	If applicable, provided documentation of circumstances resulting in an encroachment that are beyond the control of an applicable Transmission Owner or applicable Generator Owner subject to compliance with this reliability standard including natural disasters, or human or animal activity, as detailed in footnote 5.
Note to Auditor: Information on the purpose, applicability, and effective dates of this standard is included in the Additional Information section of this RSAW. Auditor should consider verifying the entity's list of overhead lines that were identified as an element of an IROL or an element of a Major WECC Transfer Path are the same as the applicable Planning Coordinator's list. Review the guidance provided in footnotes 2-4 as well as example evidence in the requirement measure**.** Auditor should review the Quarterly Vegetation-Related Transmission Outage Reports to verify entity response for the applicable audit period. Consider Requirement 1 on page 18 of the Guidelines and Technical Basis in the attached FAC-003-3 Standard for more information.	

Auditor Notes:

R2 Supporting Evidence and Documentation

Requirement

R2. Each applicable Transmission Owner and applicable Generator Owner shall manage vegetation to prevent encroachments into the MVCD of its applicable line(s) which are not either an element of an IROL, or an element of a Major WECC Transfer Path; operating within its Rating and all Rated Electrical Operating Conditions of the types shown below[5]:

1. An encroachment into the MVCD, observed in Real-time, absent a Sustained Outage,6
2. An encroachment due to a fall-in from inside the ROW that caused a vegetation-related Sustained Outage,7
3. An encroachment due to blowing together of applicable lines and vegetation located inside the ROW that caused a vegetation-related Sustained Outage,7
4. An encroachment due to vegetation growth into the line MVCD that caused a vegetation-related Sustained Outage7

Measure

M2. Each applicable Transmission Owner and applicable Generator Owner has evidence that it managed vegetation to prevent encroachment into the MVCD as described in R2. Examples of acceptable forms of evidence may include dated attestations, dated reports containing no Sustained Outages associated with encroachment types 2 through 4 above, or records confirming no Real-time observations of any MVCD encroachments.

Questions for Registered Entity

Question: Does the applicable Generator Owner own overhead transmission lines that (1) extend greater than one mile or 1.609 kilometers beyond the fenced area of the generating station switchyard to the point of interconnection with a Transmission Owner's Facility or (2) do not have a clear line of sight4 from the generating station switchyard fence to the point of interconnection with a Transmission Owner's Facility? ☐ Yes ☐ No

If Yes, provide a list of the applicable transmission lines and respond to the following Questions.

Registered Entity Response to Question **(Required)**:

Question: Does the applicable Transmission Owner or Generator Owner own overhead transmission lines operated at 200kV or above that are not either an element of an IROL or an element of a Major WECC Transfer Path that are operating within its Rating? ☐ Yes ☐ No

If Yes, provide a list of the applicable transmission lines.

Registered Entity Response to Question **(Required)**:

Question: Did the applicable Transmission Owner or Generator Owner have any encroachment (Types 1-4) into the MVCD of its applicable line(s) in the audit period? ☐ Yes ☐ No. **If Yes,** describe the encroachment(s). **Registered Entity Response** to Question **(Required)**:

Registered Entity Response (Required):

Describe, in narrative form, how you meet compliance with this Requirement.

Registered Entity Evidence Listing (Required):

Provide the following for all evidence submitted (Insert additional rows if necessary): File Name, File Extension, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description

1.
2.
3.

Audit Team Evidence Reviewed

This section must be completed by the Compliance Enforcement Authority

1.
2.
3.

Compliance Assessment Approach Specific to FAC-003-3, R2

This section must be completed by the Compliance Enforcement Authority

Review the evidence to verify the Registered Entity has performed the following:

	Responded to the Questions and provided evidence of compliance if it owns applicable line(s).
	Managed vegetation to prevent encroachments into the Minimum Vegetation Clearance Distance (MVCD) as follows:
	• No Real-time observations of any MVCD encroachments absent a Sustained Outage (type 1) or;
	• No Sustained Outages associated with encroachment types 2 through 4 or;
	If applicable, provided documentation of circumstances resulting in an encroachment that are beyond the control of an applicable Transmission Owner or applicable Generator Owner subject to compliance with this reliability standard including natural disasters, or human or animal activity, as detailed in footnote 5.

Note to Auditor: Auditor should consider verifying the entity's list of overhead lines that were not identified as an element of an IROL or an element of a Major WECC Transfer Path are the same as the applicable Planning Coordinator's list. Review the guidance provided in footnotes 2-4 as well as example evidence in the requirement measure. Auditor should review the Quarterly Vegetation-Related Transmission Outage Reports to verify entity response for the applicable audit period.

Consider Requirement 2 on page 18 of the Guidelines and Technical Basis in the attached FAC-003-3 Standard for more information.

Auditor Notes:

R3 Supporting Evidence and Documentation

Requirement

R3. Each applicable Transmission Owner and applicable Generator Owner shall have documented maintenance strategies or procedures or processes or specifications it uses to prevent the encroachment of vegetation into the MVCD of its applicable lines that accounts for the following:
3.1 Movement of applicable line conductors under their Rating and all Rated Electrical Operating Conditions;
3.2 Inter-relationships between vegetation growth rates, vegetation control methods, and inspection frequency.

Measure

M3. The maintenance strategies or procedures or processes or specifications provided demonstrate that the applicable Transmission Owner and applicable Generator Owner can prevent encroachment into the MVCD considering the factors identified in the requirement.

Registered Entity Response (Required):

Describe, in narrative form, how you meet compliance with this Requirement.

Registered Entity Evidence Listing (Required):

Provide the following for all evidence submitted (Insert additional rows if necessary):
File Name, File Extension, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description

1.
2.
3.

Audit Team Evidence Reviewed

This section must be completed by the Compliance Enforcement Authority

1.
2.
3.

Compliance Assessment Approach Specific to FAC-003-3, R3

This section must be completed by the Compliance Enforcement Authority

Review the evidence to verify the Registered Entity has provided the following:

	Documented maintenance strategies or procedures or processes or specifications it uses to prevent the encroachment of vegetation into the MVCD of its applicable lines that accounts for the following:
	• Consideration of movement of applicable line conductors under their Rating and all Rated

	Electrical Operating Conditions;
	• Consideration of Inter-relationships between the following:
	○ Vegetation growth rates
	○ Vegetation control methods
	○ Inspection frequency
Note to Auditor: Consider Requirement 3 on pages 19-20 of the Guidelines and Technical Basis in the attached FAC-003-3 Standard for more information.	

Auditor Notes:

R4 Supporting Evidence and Documentation

Requirement

R4. Each applicable Transmission Owner and applicable Generator Owner, without any intentional time delay, shall notify the control center holding switching authority for the associated applicable line when the applicable Transmission Owner and applicable Generator Owner has confirmed the existence of a vegetation condition that is likely to cause a Fault at any moment.

Measure

M4. Each applicable Transmission Owner and applicable Generator Owner that has a confirmed vegetation condition likely to cause a Fault at any moment will have evidence that it notified the control center holding switching authority for the associated transmission line without any intentional time delay. Examples of evidence may include control center logs, voice recordings, switching orders, clearance orders and subsequent work orders.

Questions for Registered Entity

Question: Did the applicable Transmission Owner or applicable Generator Owner have confirmed existence of any vegetation conditions likely to cause a Fault at any moment in the audit period? ☐ Yes ☐ No

If Yes, explain the event and provide evidence of notification of the control center without any intentional time delay.

Registered Entity Response to Question **(Required)**:

Registered Entity Response (Required):

Describe, in narrative form, how you meet compliance with this Requirement.

Registered Entity Evidence Listing (Required):

Provide the following for all evidence submitted (Insert additional rows if necessary):
File Name, File Extension, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description

1.
2.
3.

Audit Team Evidence Reviewed

This section must be completed by the Compliance Enforcement Authority

1.
2.
3.

Compliance Assessment Approach Specific to FAC-003-3, R4

This section must be completed by the Compliance Enforcement Authority

Review the evidence to verify the Registered Entity has performed the following:

	Responded to the Question and provided evidence of compliance.
	Notified the control center holding switching authority for the associated transmission line without any intentional time delay when:
	• The applicable Transmission Owner or applicable Generator Owner has confirmed the existence of a vegetation condition that is likely to cause a Fault at any moment and;
	• That this notification was made without any intentional time delay
Note to Auditor: Consider Requirement 4 on pages 20-21 of the Guidelines and Technical Basis in the attached FAC-003-3 Standard for more information.	

Auditor Notes:

R5 Supporting Evidence and Documentation

Requirement

R5. When an applicable Transmission Owner and applicable Generator Owner is constrained from performing vegetation work on an applicable line operating within its Rating and all Rated Electrical Operating Conditions, and the constraint may lead to a vegetation encroachment into the MVCD prior to the implementation of the next annual work plan, then the applicable Transmission Owner or applicable Generator Owner shall take corrective action to ensure continued vegetation management to prevent encroachments.

Measure

M5. Each applicable Transmission Owner and applicable Generator Owner has evidence of the corrective action taken for each constraint where an applicable transmission line was put at potential risk. Examples of acceptable forms of evidence may include initially-planned work orders, documentation of constraints from landowners, court orders, inspection records of increased monitoring, documentation of the de-rating of lines, revised work orders, invoices, or evidence that the line was de-energized.

Questions for Registered Entity

Question: Was the applicable Transmission Owner or applicable Generator Owner constrained during the audit period from performing vegetation work on applicable line(s) operating within its Rating and all Rated Electrical Operating Conditions? ☐ Yes ☐ No

If Yes, could the constraint have led to a vegetation encroachment into the MVCD prior to the implementation of the next annual work plan? ☐ Yes ☐ No

If Yes, did the applicable Transmission Owner or applicable Generator Owner take corrective action to ensure continued vegetation management to prevent encroachments? ☐ Yes ☐ No

If Yes, to any of the questions, provide a description of the constraint(s) and the corrective action taken to prevent encroachments.

Registered Entity Response to Question **(Required)**:

Registered Entity Response (Required):

Describe, in narrative form, how you meet compliance with this Requirement.

Registered Entity Evidence Listing (Required):

Provide the following for all evidence submitted (Insert additional rows if necessary):
File Name, File Extension, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description

1.
2.
3.

Audit Team Evidence Reviewed

This section must be completed by the Compliance Enforcement Authority

1.
2.
3.

Compliance Assessment Approach Specific to FAC-003-3, R5

This section must be completed by the Compliance Enforcement Authority

Review the evidence to verify the Registered Entity has performed the following:

	Responded to the Question and provided evidence of compliance.
	Provided evidence of being constrained from performing vegetation work on applicable line(s) operating within its Rating and all Rated Electrical Operating Conditions, and;
	• The constraint may lead to a vegetation encroachment into the MVCD prior to the implementation of the next annual work plan and;
	• The applicable Transmission Owner or applicable Generator Owner took corrective action to ensure continued vegetation management to prevent encroachments
Note to Auditor: In situations where transmission line reliability is potentially at risk due to a constraint, the applicable Transmission Owner is required to take an interim corrective action to mitigate the potential risk to the transmission line. Consider Requirement 5 on pages 21-22 of the Guidelines and Technical Basis in the attached FAC-003-3 Standard for more information.	

Auditor Notes:

R6 Supporting Evidence and Documentation

Requirement

R6. Each applicable Transmission Owner and applicable Generator Owner shall perform a Vegetation Inspection of 100% of its applicable transmission lines (measured in units of choice - circuit, pole line, line miles or kilometers, etc.) at least once per calendar year and with no more than 18 calendar months between inspections on the same ROW[5]

Measure

M6. Each applicable Transmission Owner and applicable Generator Owner has evidence that it conducted Vegetation Inspections of the transmission line ROW for all applicable lines at least once per calendar year but with no more than 18 calendar months between inspections on the same ROW. Examples of acceptable forms of evidence may include completed and dated work orders, dated invoices, or dated inspection records.

Registered Entity Response (Required):

Describe, in narrative form, how you meet compliance with this Requirement.

Registered Entity Evidence Listing (Required):

Provide the following for all evidence submitted (Insert additional rows if necessary):
File Name, File Extension, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description

1.
2.
3.

Audit Team Evidence Reviewed

This section must be completed by the Compliance Enforcement Authority

1.
2.
3.

Compliance Assessment Approach Specific to FAC-003-3, R6

This section must be completed by the Compliance Enforcement Authority

Review the evidence to verify the Registered Entity has performed the following:

	A Vegetation Inspection of 100% of its applicable transmission lines at least once per calendar year and

[5] When the applicable Transmission Owner or applicable Generator Owner is prevented from performing a Vegetation Inspection within the timeframe in R6 due to a natural disaster, the TO or GO is granted a time extension that is equivalent to the duration of the time the TO or GO was prevented from performing the Vegetation Inspection.

	with no more than 18 calendar months between inspections on the same ROW or;
	Provided evidence of any necessary Vegetation Inspection timeframe extensions due to a natural disaster per footnote 8.

Note to Auditor: Verify that 100% of the applicable transmission lines were inspected within the intervals established in the applicable entity's "documented maintenance strategies" established in Requirement 3. Initially, entities are required to inspect 100% of their applicable transmission lines in the calendar year 2014, regardless of their previous inspection cycle. An entity performing inspections between 1/1/14 and 6/30/14 would satisfy this requirement. For calendar year 2015, such an entity would be required to perform subsequent inspections within 18 months of the prior inspection date. For entities performing their calendar year 2014 inspections after 7/1/14, they would have until 12/31/15 to perform the calendar year 2015 inspections. Consider Requirement 6 page 22 of the Guidelines and Technical Basis in the attached FAC-003-3 Standard for more information.

Auditor Notes:

R7 Supporting Evidence and Documentation

Requirement

R7. Each applicable Transmission Owner or applicable Generator Owner shall complete 100% of its annual vegetation work plan of applicable lines to ensure no vegetation encroachments occur within the MVCD. Modifications to the work plan in response to changing conditions or to findings from vegetation inspections may be made (provided they do not allow encroachment of vegetation into the MVCD) and must be documented. The percent completed calculation is based on the number of units actually completed divided by the number of units in the final amended plan (measured in units of choice - circuit, pole line, line miles or kilometers, etc.) Examples of reasons for modification to annual plan may include:

- Change in expected growth rate/ environmental factors
- Circumstances that are beyond the control of a applicable Transmission Owner or applicable Generator Owner[6]
- Rescheduling work between growing seasons
- Crew or contractor availability/ Mutual assistance agreements
- Identified unanticipated high priority work
- Weather conditions/Accessibility
- Permitting delays
- Land ownership changes/Change in land use by the landowner
- Emerging technologies

Measure

M7. Each applicable Transmission Owner or applicable Generator Owner has evidence that it completed its annual vegetation work plan for its applicable lines. Examples of acceptable forms of evidence may include a copy of the completed annual work plan (as finally modified), dated work orders, dated invoices, or dated inspection records.

Registered Entity Response (Required):

Describe, in narrative form, how you meet compliance with this Requirement.

Registered Entity Evidence Listing (Required):

Provide the following for all evidence submitted (Insert additional rows if necessary):
File Name, File Extension, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description

[6] Circumstances that are beyond the control of an applicable Transmission Owner or applicable Generator Owner include but are not limited to natural disasters such as earthquakes, fires, tornados, hurricanes, landslides, ice storms, floods, or major storms as defined either by the TO or GO or an applicable regulatory body.

1.
2.
3.

Audit Team Evidence Reviewed

This section must be completed by the Compliance Enforcement Authority

1.
2.
3.

Compliance Assessment Approach Specific to FAC-003-3, R7

This section must be completed by the Compliance Enforcement Authority

Review the evidence to verify the Registered Entity has performed the following:

	Completed 100% of its annual vegetation work plan of applicable lines or;
	Provided documentation of reasons for modification of its annual plan
	Provided documentation that the percent completed calculation is based on the number of units actually completed divided by the number of units in the final amended plan
Note to Auditor: This requirement sets the expectation that the work identified in the annual work plan will be completed as planned. Deferrals or relevant changes to the annual plan shall be documented. Auditor should rely on professional judgment to accurately identify and select a sample of transmission lines ROWs that traverse the major biomes within the applicable entities footprint. Auditors should consider biome conditions such as climate, geography, elevation, botany, population density, and land uses when selecting the sample transmission lines for R7. Consider Requirement 7 on pages 23-24 of the Guidelines and Technical Basis in the attached FAC-003-3 Standard for more information	

Auditor Notes:

Compliance Finding Summary

This section must be completed by the Compliance Enforcement Authority

Req.	NF	PV	OEA	NA	Statement
1					
2					
3					
4					
5					
6					
7					

Additional Information

The following information comes directly from the standard FAC-003-03

1. **Title:** Transmission Vegetation Management

2. **Number:** FAC-003-3

3. **Purpose:** To maintain a reliable electric transmission system by using a defense-in-depth strategy to manage vegetation located on transmission rights of way (ROW) and minimize encroachments from vegetation located adjacent to the ROW, thus preventing the risk of those vegetation-related outages that could lead to Cascading.
4. **Applicability**

4.1. Functional Entities:

4.1.1. Applicable Transmission Owners

4.1.1.1 Transmission Owners that own Transmission Facilities defined in 4.2.

4.1.2 Applicable Generator Owners

4.1.2.1 Generator Owners that own generation Facilities defined in 4.3

4.2. Transmission Facilities: Defined below (referred to as "applicable lines"), including but not limited to those that cross lands owned by federal[7], state, provincial, public, private, or tribal entities:

4.2. 1 Each overhead transmission line operated at 200kV or higher.

4.2.2 Each overhead transmission line operated below 200kV identified as an element of an IROL under NERC Standard FAC-014 by the Planning Coordinator.

4.2.3 Each overhead transmission line operated below 200 kV identified as an element of a Major WECC Transfer Path in the Bulk Electric System by WECC.

4.2.4 Each overhead transmission line identified above (4.2.1 through 4.2.3) located outside the fenced area of the switchyard, station or substation and any portion of the span of the transmission line that is crossing the substation fence.

4.3. Generation Facilities: Defined below (referred to as "applicable lines"), including but not limited to those that cross lands owned by federal[8], state, provincial, public, private, or tribal entities:

4.3.1 Overhead transmission lines that (1) extend greater than one mile or 1.609 kilometers beyond the fenced area of the generating station switchyard to the point of interconnection with a

[7] EPAct 2005 section 1211c: "Access approvals by Federal agencies."
[8] Id.

Transmission Owner's Facility or (2) do not have a clear line of sight[9] from the generating station switchyard fence to the point of interconnection with a Transmission Owner's Facility and are:

4.3.1.1 Operated at 200kV or higher; or

4.3.1.2 Operated below 200kV identified as an element of an IROL under NERC Standard FAC-014 by the Planning Coordinator; or

4.3.1.3 Operated below 200 kV identified as an element of a Major WECC Transfer Path in the Bulk Electric System by WECC.

Effective Dates

There are two effective dates associated with this standard.

The first effective date allows Generator Owners time to develop documented maintenance strategies or procedures or processes or specifications as outlined in Requirement R3.

In those jurisdictions where regulatory approval is required, Requirement R3 applied to the Generator Owner becomes effective on the first calendar day of the first calendar quarter one year after the date of the order approving the standard from applicable regulatory authorities where such explicit approval for all requirements is required. In those jurisdictions where no regulatory approval is required, Requirement R3 becomes effective on the first day of the first calendar quarter one year following Board of Trustees' adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

The second effective date allows entities time to comply with Requirements R1, R2, R4, R5, R6, and R7.

In those jurisdictions where regulatory approval is required, Requirements R1, R2, R4, R5, R6, and R7 applied to the Generator Owner become effective on the first calendar day of the first calendar quarter two years after the date of the order approving the standard from applicable regulatory authorities where such explicit approval for all requirements is required. In those jurisdictions where no regulatory approval is required, Requirements R1, R2, R4, R5, R6, and R7 become effective on the first day of the first calendar quarter two years following Board of Trustees' adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Effective dates for individual lines when they undergo specific transition cases:

1. A line operated below 200kV, designated by the Planning Coordinator as an element of an Interconnection Reliability Operating Limit (IROL) or designated by the Western Electricity Coordinating Council (WECC) as an element of a Major WECC Transfer Path, becomes subject to this standard the latter of: 1) 12 months after the date the Planning Coordinator or WECC initially designates the line as being an element of an IROL or an element of a Major WECC Transfer Path, or 2) January 1 of the

[9] "Clear line of sight" means the distance that can be seen by the average person without special instrumentation (e.g., binoculars, telescope, spyglasses, etc.) on a clear day.

planning year when the line is forecast to become an element of an IROL or an element of a Major WECC Transfer Path.

2. A line operated below 200 kV currently subject to this standard as a designated element of an IROL or a Major WECC Transfer Path which has a specified date for the removal of such designation will no longer be subject to this standard effective on that specified date.

3. A line operated at 200 kV or above, currently subject to this standard which is a designated element of an IROL or a Major WECC Transfer Path and which has a specified date for the removal of such designation will be subject to Requirement R2 and no longer be subject to Requirement R1 effective on that specified date.

4. An existing transmission line operated at 200kV or higher which is newly acquired by an asset owner and which was not previously subject to this standard becomes subject to this standard 12 months after the acquisition date.

5. An existing transmission line operated below 200kV which is newly acquired by an asset owner and which was not previously subject to this standard becomes subject to this standard 12 months after the acquisition date of the line if at the time of acquisition the line is designated by the Planning Coordinator as an element of an IROL or by WECC as an element of a Major WECC Transfer Path.

.

FAC-003-3.pdf

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria, or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

There are two approaches to sampling: statistical and non-statistical, and choosing which to use depends on the objectives for sampling. (When the population sample to be reviewed is documentation, a statistical approach using RAT-STATS is expected.) Both are represented in the sample guideline in line with standard practices for their use. The Audit Team Lead may determine if the scope of the audit samples should be reduced to levels below those established in the sample guideline. In doing so, the audit team will document the rationale for reducing the scope of the of sample population in the RSAW or audit report.

Additionally, separate from the audit, the registered entity may use this methodology to determine the sample population to test in order to provide themselves reasonable assurance that management's expectations are being met by the organization.

Auditor should rely on professional judgment to accurately identify and select a sample of transmission lines ROWs that traverse the major biomes within the applicable entities footprint. Auditors should consider biome conditions such as climate, geography, elevation, botany, population density and land uses when selecting the sample transmission lines for R7.

Regulatory Language

Order No. 785 (September 19, 2013)

P1. Pursuant to section 215 of the Federal Power Act, the Federal Energy Regulatory Commission (Commission) approves modifications to four existing Reliability Standards submitted by the North American Electric Reliability Corporation (NERC), the Commission certified Electric Reliability Organization. Specifically, the Commission approves Reliability Standards FAC-001-1 (Facility Connection Requirements), FAC-003-3 (Transmission Vegetation Management), PRC-004-2.1a (Analysis and Mitigation of Transmission and Generation Protection System Misoperations), and PRC-005-1.1b (Transmission and Generation Protection System Maintenance and Testing). The modifications improve reliability either by extending applicability of the Reliability Standard to certain generator interconnection facilities, or by clarifying that the existing Reliability Standard is and remains applicable to generator interconnection facilities. The Commission also approves the related Violation Risk Factors and Violation Severity Levels, as well as the implementation plan and effective dates proposed by NERC.

P 9. With respect to implementation, NERC requested an effective date [for Generator Owners] of one year following the first quarter after regulatory approvals for FAC-001-1, and for FAC-003-3 Requirement R3. For the remaining requirements of FAC-003-3, NERC requested an effective date of two years following the first calendar quarter after regulatory approvals…. [NERC's July 30, 2012 petition states: If FAC-003-2 is filed with applicable regulatory authorities and approved before FAC-003-3 is filed with applicable regulatory authorities, then when and if FAC-003-3 is approved by applicable regulatory authorities, the implementation plan and effective dates for Transmission Owners in FAC-003-2 will be transferred into this implementation plan."]

P 26. We approve Reliability Standard FAC-003-3. Consistent with the NOPR, we find that the modifications to FAC-003 address a potential reliability gap in the current set of Reliability Standards, since they do not include a requirement for generator owners to perform vegetation management on their tie-lines or to maintain minimum levels of clearance between vegetation and significant overhead generator interconnection facilities. Further, we conclude that the proposed limits on applicability reflected in FAC-003-3 are reasonable, as it is common for generator interconnection facilities of relatively short span (i.e., less than one mile) to cross only areas with limited or no vegetation.

P 27. Further, we adopt our proposed guidance that the exemption for overhead lines with a clear line of sight from the generator to the point of interconnection should be "interpreted narrowly," meaning there should be "no obstructions . . . that prevent personnel from identifying potential reliability hazards over the full length of the line." Footnote: *See* NOPR, 143 FERC ¶ 61,049 at P 20.

P 60. This Final Rule approves Reliability Standards FAC-001-1, FAC-003-3, PRC-004-2.1a, and PRC-005-1.1b, which would replace currently effective Reliability Standards FAC-001-0, FAC-003-1, PRC-004-2a, and PRC-005-1b…. Footnote: As of the date of issuance of this Final Rule, the currently effective standard is FAC-003-1. While a revised version of that standard, FAC-003-2, was approved in Docket No. RM12-4-000, it has yet to go into effect. The information collection requirements of Reliability Standard FAC-003-2 were approved by the OMB on May 29, 2013, under FERC-725A (OMB Control No. 1902-0244).

P 62. The modifications reflected in FAC-003-3 extend NERC's vegetation management requirements to certain generator interconnection facilities, including requirements to create and maintain records related to the generator owner's vegetation management work plan and performance of inspections. Generator owners typically already maintain the vegetation surrounding the right-of-way for the generator interconnection facility that connects the generating station switchyard to the point of interconnection with a transmission owner's facility. However, the proposed requirements outlined in FAC-003-3 may exceed a generator owner's current vegetation management program, particularly with respect to recordkeeping and reporting.

Order No. 777 (March 21, 2013)

P 27. We adopt our NOPR proposal and approve Reliability Standard FAC-003-2, including the associated definitions and implementation plan, as just, reasonable, not unduly discriminatory or preferential, and in the public interest. We find that FAC-003-2 is an improvement over the currently-effective Version 1 standard, will support vegetation management practices that can effectively protect against vegetation-related transmission outages, and satisfies a number of the outstanding directives from Order No. 693…. Footnote: Likewise, we approve as requested by NERC, the retirement of FAC-003-1 and the current definitions of "right-of-way" and "vegetation inspection" effective "midnight immediately prior to the first day of the first calendar quarter that is a year following the effective date" of the final rule. NERC December 21, 2011 Petition at 2.

Revision History

Version	Date	Reviewers	Revision Description
1	2/25/2014	RSAW Task Force	New Document
2	4/23/2014	RSAW Task Force	Clarify R6 auditor notes regarding timing of periodic inspections.

Compliance Questionnaire and
Reliability Standard Audit Worksheet

NUC-001-2.1 — Nuclear Plant Interface Coordination

Registered Entity: *(Must be completed by the Compliance Enforcement Authority)*

NCR Number: *(Must be completed by the Compliance Enforcement Authority)*

Applicable Function(s): **TOP, TO, TP, TSP, BA, RC, PA, DP, LSE, GO, GOP**

Auditors:

Disclaimer

NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

Subject Matter Experts

Identify your company's subject matter expert(s) responsible for this Reliability Standard. Include the person's title, organization and the requirement(s) for which they are responsible. Insert additional lines if necessary.

Response: ***(Registered Entity Response Required)***

SME Name	Title	Organization	Requirement

Reliability Standard Language

NUC-001-2.1 — Nuclear Plant Interface Coordination

Purpose:
This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown.

Applicability:
NPGO, TOP, TO, TP, TSP, BA, RC, PA, DP, LSE, GO, GOP

NERC BOT Approval Date: 5/1/2007

FERC Approval Date: 10/16/2008

Reliability Standard Enforcement Date in the United States: 4/1/2013

Requirements:

R1. The Nuclear Plant Generator Operator shall provide the proposed NPIRs in writing to the applicable Transmission Entities and shall verify receipt [*Risk Factor: Lower*]

Describe, in narrative form, how you meet compliance with this requirement: *(Registered Entity Response Required)*

R1 Supporting Evidence and Documentation

Response: *(Registered Entity Response Required)*

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version

Audit Team: Additional Evidence Reviewed:

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to NUC-001-2.1 R1.

___ Review evidence the Nuclear Plant Generator operator provided the proposed Nuclear Plant Interface Requirements in writing to the applicable Transmission Entities.

___ Review the Nuclear Plant Generator Operator received confirmation of the delivery of the NPIR.

Detailed notes:

R2. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements[1] that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs. [Risk Factor: Medium]

1. Agreements may include mutually agreed upon procedures or protocols in effect between entities or between departments of a vertically integrated system.

Describe, in narrative form, how you meet compliance with this requirement: *(Registered Entity Response Required)*

R2 Supporting Evidence and Documentation

Response: *(Registered Entity Response Required)*

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version
Audit Team: Additional Evidence Reviewed:		

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to NUC-001-2 R2.1.

___ Review evidence the Nuclear Plant Generator Operator and Transmission Entities have in effect one or more agreements.

___ Verify agreements include mutually agreed to NPIRS

___ Verify agreements identify how the Nuclear Plant Generator Operator and Transmission Entities address implementing the NPIRs.

Detailed notes:

R3. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator. [*Risk Factor: Medium*]

Describe, in narrative form, how you meet compliance with this requirement: *(Registered Entity Response Required)*

R3 Supporting Evidence and Documentation

Response: ***(Registered Entity Response Required)***

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version
Audit Team: Additional Evidence Reviewed:		

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to NUC-001-2.1 R3.

___ Review evidence the Transmission Entities incorporated the NPIRs into their planning process.

___ Verify the Transmission Entity communicated the results of the analyses to the Nuclear Plant Generator Operator.

Detailed notes:

R4. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall: [*Risk Factor: High*]

R4.1. Incorporate the NPIRs into their operating analyses of the electric system.

R4.2. Operate the electric system to meet the NPIRs.

R4.3. Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.

Describe, in narrative form, how you meet compliance with this requirement: ***(Registered Entity Response Required)***

R4 Supporting Evidence and Documentation

Response: ***(Registered Entity Response Required)***

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version
Audit Team: Additional Evidence Reviewed:		

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to NUC-001-2.1 R4.

___ (R4.1) Review evidence the Transmission Entities incorporated the NPIRs into their operating analyses of the electric system.

___ (R4.2) Verify the Transmission Entity operated the electric system to meet the NPIRs.

___ (R4.3) As the Transmission Entity, have you lost the ability to assess the operation of the electric system affecting the NPIR?

___ If yes, Verify the Transmission Entity has informed the Nuclear Generator Operator.

Detailed notes:

R5. The Nuclear Plant Generator Operator shall operate per the Agreements developed in accordance with this standard. [*Risk Factor: High*]

Describe, in narrative form, how you meet compliance with this requirement: *(Registered Entity Response Required)*

R5 Supporting Evidence and Documentation

Response: *(Registered Entity Response Required)*

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version
Audit Team: Additional Evidence Reviewed:		

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to NUC-001-2.1 R5.

___ Review evidence the Nuclear Plant Generator Operator operates per the agreements developed in accordance with this standard.

Detailed notes:

R6. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs. [*Risk Factor: Medium*]

Describe, in narrative form, how you meet compliance with this requirement: ***(Registered Entity Response Required)***

R6 Supporting Evidence and Documentation

Response: ***(Registered Entity Response Required)***

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version
Audit Team: Additional Evidence Reviewed:		

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to NUC-001-2.1 R6.

___ Review evidence the applicable Transmission Entities and Nuclear Plant Generator Operator coordinate outages and maintenance activities per the agreements.

Detailed notes:

R7. Per the Agreements developed in accordance with this standard, the Nuclear Plant Generator Operator shall inform the applicable Transmission Entities of actual or proposed changes to nuclear plant design, configuration, operations, limits, Protection Systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]

Describe, in narrative form, how you meet compliance with this requirement: ***(Registered Entity***

Response Required)

R7 Supporting Evidence and Documentation

Response: ***(Registered Entity Response Required)***

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version
Audit Team: Additional Evidence Reviewed:		

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to NUC-001-2.1 R7.

___ Review evidence Nuclear Plant Generator Operator informed the applicable Transmission Entities of actual or proposed changes to nuclear plant design, configuration, operations, limits, Protection Systems, or capabilities that may impact the ability of the electric system to meet the NPIRs

Detailed notes:

R8. Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs. [*Risk Factor: High*]

Describe, in narrative form, how you meet compliance with this requirement: ***(Registered Entity***

Response Required)

R8 Supporting Evidence and Documentation

Response: ***(Registered Entity Response Required)***

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version
Audit Team: Additional Evidence Reviewed:		

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to NUC-001-2.1 R8.

___ Review evidence applicable Transmission Entities informed the Nuclear Plant Generator Operator of actual or proposed changes to nuclear plant design, configuration, operations, limits, protection systems, or capabilities that may impact the ability of the electric system to meet the NPIRs.

Detailed notes:

R9. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2: [*Risk Factor: Medium*]

R9.1. Administrative elements:

R9.1.1. Definitions of key terms used in the agreement. (Retirement of R9.1.1 approved by FERC effective January 21, 2014.)

R9.1.2. Names of the responsible entities, organizational relationships, and responsibilities related to the NPIRs. (Retirement of R9.1.2 approved by FERC effective January 21, 2014.)

R9.1.3. A requirement to review the agreement(s) at least every three years. (Retirement of R9.1.3 approved by FERC effective January 21, 2014.)

R9.1.4. A dispute resolution mechanism. (Retirement of R9.1.4 approved by FERC effective January 21, 2014.)

R9.2. Technical requirements and analysis:

R9.2.1. Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.

R9.2.2. Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.

R9.2.3. Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.

Describe, in narrative form, how you meet compliance with this requirement: ***(Registered Entity Response Required)***

R9.3. Operations and maintenance coordination:

R9.3.1. Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.

R9.3.2. Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.

R9.3.3. Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.

R9.3.4. Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.

R9.3.5. Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power.

R9.3.6. Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.

R9.3.7. Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.

Describe, in narrative form, how you meet compliance with this requirement: ***(Registered Entity Response Required)***

R9.4. Communications and training:

R9.4.1. Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.

R9.4.2. Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.

R9.4.3. Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.

R9.4.4. Provisions for supplying information necessary to report to government agencies, as related to NPIRs.

R9.4.5. Provisions for personnel training, as related to NPIRs.

Describe, in narrative form, how you meet compliance with this requirement: ***(Registered Entity Response Required)***

R9 Supporting Evidence and Documentation

Response: ***(Registered Entity Response Required)***

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version
Audit Team: Additional Evidence Reviewed:		

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to NUC-001-2.1 R9.

___ Verify the Nuclear Plant Generator Operator and the applicable Transmission Entities shall include, as a minimum, the following elements within the agreement(s) identified in R2:

Technical requirements and analysis:

___ (R9.2.1) Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the agreement.

___ (R9.2.2) Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.

___ (R9.2.3) Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.

Operations and maintenance coordination:

___ (R9.3.1) Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.

___ (R9.3.2) Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.

___ (R9.3.3) Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.

___ (R9.3.4) Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.

___ (R9.3.5) Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power.

___ (R9.3.6) Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.

___ (R9.3.7) Coordination of the NPIRs with transmission system Special Protection Systems and underfrequency and undervoltage load shedding programs.

Communications and training:

___ (R9.4.1) Provisions for communications between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of terms.

___ (R9.4.2) Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.

___ (R9.4.3) Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.

___ (R9.4.4) Provisions for supplying information necessary to report to government agencies, as related to NPIRs.

___ (R9.4.5) Provisions for personnel training, as related to NPIRs.

Detailed notes:

Supplemental Information

Other - The list of questions above is not all inclusive of evidence required to show compliance with the Reliability Standard. Provide additional information here, **as necessary** that demonstrates compliance with this Reliability Standard.

Entity Response: ***(Registered Entity Response)***

Compliance Findings Summary (to be filled out by auditor)

Req.	NF	PV	OEA	NA	Statement
1					
2					
3					
4					
5					
6					
7					
8					
9					

Excerpts From FERC Orders -- For Reference Purposes Only
Updated Through ----------
NUC-001-1

Order 716

http://www.nerc.com/files/Order_716-NUC_Standard.pdf

P1 "Pursuant to section 215 of the Federal Power Act (FPA), the Commission approves the Nuclear Plant Interface Coordination Reliability Standard (NUC-001-1) developed by the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO)...."

P2 "On November 19, 2007, NERC filed its petition for Commission approval of the Nuclear Plant Interface Coordination Reliability Standard, designated NUC-001-1 (November 19, 2007 Petition). NERC supplemented the filing on December 11, 2007 (December 11, 2007 Supplement) to propose four related NERC Glossary terms: "Nuclear Plant Generator Operator," "Nuclear Plant Off-site Power Supply (Off-site Power)," "Nuclear Plant Licensing Requirements (NPLRs)," and "Nuclear Plant Interface Requirements (NPIRs)." In the November 19, 2007 Petition, NERC stated that the proposed Reliability Standard addresses the coordination of interface requirements for two domains: (i) Bulk-Power System planning and operations and (ii) nuclear power plant licensing requirements for off-site power necessary to enable safe nuclear plant operation and shutdown."

P4 "...The Reliability Standard requires nuclear plant generator operators and transmission entities to develop expectations and procedures for coordinating operations to meet the nuclear plant licensing requirements, as well as SOLs and IROLs, and to develop agreements or arrangements, which may include mutually agreed upon procedures or protocols, reflecting those expectations and procedures. These agreements or arrangements are known as interface agreements. The resulting operations and planning requirements developed in the agreements to address the nuclear plant licensing requirements, SOLs and IROLs are called nuclear plant interface requirements or NPIRs.10 NERC stated that Requirements R3 through R8, which state that the interface agreement parties will address the NPIRs in planning, operations, and facility upgrade and outage coordination, provide additional specificity on these expectations."

P17 "...The Commission finds that coordination of nuclear licensing requirements and grid operating limits through auditable interface agreements will ensure that an important resource is operated safely and reliably, while minimizing grid disturbances from separation of nuclear power plants from the grid, due to the loss or degradation of auxiliary power supply. Further, the Commission disagrees with CenterPoint Energy that the Reliability Standard is flawed and unnecessary. Nuclear power plants represent an important power resource and provide reliability support throughout the Bulk-Power System. Unlike other large units, nuclear power plants are subject to separate regulatory oversight that mandates stringent operating and auxiliary power requirements, which, if not met, require the plant to separate from the grid. We find that NUC-001-1 is an appropriate means to ensure that the particular requirements faced by nuclear power plants are met, maximizing the reliability support to be provided while minimizing the potential for grid disruption caused by separation."

P18 "...NUC-001-1 supplements NRC oversight of nuclear plant facilities by providing oversight of the transmission entities that operate facilities on the Bulk-Power System providing off-site power supply and delivery service to meet nuclear plant licensing requirements."

P21 "The Commission approves the applicability provisions of NUC-001-1 as appropriately identifying the applicable entities, while providing the flexibility to accommodate differing design criteria, grid configurations and services procured by the various nuclear power plants addressed. The Commission finds appropriate the ERO's use of the term transmission entities in NUC-001-1 to refer to the subset of registered entities that provide services to nuclear plant generator operators. Similarly, the term nuclear plant generator operators refers to the subset of generator owners and generator operators that are NRC licensees. While the Commission prefers that Reliability Standards apply to all entities within a functional category defined in the Registry Criteria, it has approved appropriate limitations incorporated into an applicability provision. We address the specific questions raised by the Commission in the NOPR, as well as responses and comments, on an issue-by-issue basis below."

P28 "The Commission accepts NERC's proposal to require nuclear plant generator operators to identify entities that provide services related to off-site power supply or delivery. With NERC's and other industry representatives' assurances, the Commission is satisfied that the appropriate transmission entities can be identified based on the nuclear plant generator operators' historical compliance with NRC licensing requirements to obtain off-site power and develop solutions with grid operators to avoid service interruptions from foreseeable grid disturbances."

P29 "...A nuclear plant generator operator may be found in noncompliance for failing to provide notice to an entity responsible for providing services relating to its off-site power-related licensing requirements."

P34 "In the NOPR, the Commission proposed to accept the identification and registration process described by NERC in the November 19, 2007 Petition with the understanding that NERC will use its authority under the compliance registry process to register all users, owners, and operators of the Bulk-Power System that provide transmission or generating services relating to off-site power supply or delivery. Further, the Commission requested clarification from the ERO, as well as public comment, on three issues: (i) how NERC's plan to identify transmission entities on a "plant-by-plant basis" in the compliance registration process relates to the definition of bulk electric system; (ii) whether NUC-001-1 is enforceable against a transmission entity upon execution of an interface agreement or some earlier time; and (iii) how the Reliability Standard will be implemented for an entity that both operates a nuclear power plant and is responsible to provide services related to NPIRs."

P42 "The Commission accepts NERC's approach to determining applicable entities. The Commission agrees with the ERO that the identification of transmission entities, which may fit any one of 11 functional categories described in the NERC Functional Model, provides the ERO with needed breadth and flexibility in identifying and registering all users, owners and operators of the Bulk-Power System that provide services related to NPIRs."

P46 "...We also reject the concerns raised by Wisconsin Electric and TVA that the terms transmission entity and nuclear plant generator operator do not appear in the NERC Functional Model. While the NERC Functional Model is a useful guidance document, "the Applicability section of a particular Reliability Standard should be the ultimate determinant of applicability of each Reliability Standard." Moreover, the ERO's definition of transmission entity is linked to the functional categories set forth in the NERC Functional Model.27 Likewise, the nuclear plant generator operator can simply be viewed as a sub-category of the generator operator function."

P51 "The Commission accepts NERC's clarification that registration of lower voltage facilities and the applicability of NUC-001-1 will be limited to those facilities identified by the nuclear plant generator operator in its NPIRs. (Footnote 30: This approach for lower voltage facilities is consistent with our determination in prior proceedings that the ERO may register an entity that falls below the minimum registry criteria on a facility-by-facility basis. See Order No. 693-A at P 38.) We would expect that any NPIRs agreed to between a nuclear plant generator operator and transmission entity would include all facilities needed to transmit offsite power and auxiliary power to the nuclear facility. The Commission remains sensitive to the need for NERC to register operators of lower-voltage facilities used to deliver off-site power. The NOPR stated the Commission's understanding that NERC would register entities operating facilities not currently identified in the Regional Entities' definition of bulk electric system that are needed for Bulk-Power System reliability, through NERC's authority to register an owner or operator of an otherwise exempt facility that is needed for Bulk-Power System reliability, on a facility-by-facility basis. We note that it is in the best interest of the nuclear plant generator operator to have any such facility identified in the NPIRs."

P68 "...NERC and others have made clear that NUC-001-1 was intended to apply to transmission entities following receipt of notification from the nuclear plant generator operator, rather than after execution of the interface agreement. The applicability of NUC-001-1 is determined by the function performed by the entity—that is, an entity that provides services relating to a nuclear plant generator operator's nuclear plant licensing requirements is subject to NUC-001-1 on the latter of the effective date of the Reliability Standard or when a proposed NPIR is provided by the nuclear plant generator operator. This is consistent with other Reliability Standards where an entity is subject to a Reliability Standard based on the factual determination of whether it operates certain facilities or provides a certain service, not based on the consent of the entity."

P69 "We believe that this interpretation resolves the concerns of commenters who predict that entities supplying services to enable nuclear plant generator operators to meet nuclear plant licensing requirements would balk at executing an interface agreement if they become subject to NUC-001-1. This should not occur since transmission entities will be identified as providing services relating to NPIRs by a nuclear plant generator operator and will become subject to NUC-001-1 when they receive notice, not when they finalize an agreement."

P73 "The Commission accepts NERC's clarification that NUC-001-1 applies to nuclear plant generator operators and transmission entities where both parties are in a single integrated system. NERC clarified that a formal agreement is not necessary to have an agreement, procedures, or protocols in place that will comply with Requirement R2. Based on this clarification and industry comments, we accept NERC's conclusion that the Requirements of NUC-001-1 can be met by a single entity that is both the nuclear plant generator operator and the transmission entity. The Commission directs the ERO, in enforcing NUC-001-1, to require that an integrated entity provides documentation of its arrangements, including appropriate procedures and protocols, ensuring that its business units perform the functions under NUC-001-1 that would otherwise be met by separate entities. This will ensure that an integrated entity's compliance with NUC-001-1 is auditable in a manner comparable to other entities that are subject to the Reliability Standard."

P80 "The Commission accepts the ERO's explanation of its registration and compliance options when parties fail to come to an agreement. Should parties fail to come to an agreement and thus find themselves in violation of the requirement that they have such an agreement in place, NERC states that it may require mediation or arbitration as a remedial action. We agree that ordering such dispute resolution processes may be an appropriate response in some instances in which there is no immediate risk to grid reliability and support NERC requiring the use of arbitration or mediation on a voluntary basis where appropriate." (Footnote 43: Where there is an immediate reliability risk, we direct the ERO to take appropriate action to address the risk.)

P87 "Based on NERC's statement that parties may rely on less formal procedures and protocols, the Commission finds that NUC-001-1 does not dictate any particular format for the interface agreement. Nuclear plant generator operators and transmission entities may rely on pre-existing arrangements so long as the parties can document the fact that they have agreed that the pre-existing arrangements address all of the NPIRs, cover all required facilities and otherwise fulfill the requirements of NUC-001-1. (Footnote 47: Nuclear plant generator operators and transmission entities that choose to rely on generally-applicable tariffs should make provision to ensure that the tariff terms and conditions continue to meet the parties' needs should the tariff or nuclear licensing requirements change, and document such an arrangement.) This includes multi-party agreements."

P100 "...While not all system changes can be anticipated, the Commission expects that significant changes to the parties' operating relationship would be formalized and documented in an auditable format as interim changes in an addendum or revisions to the agreement, as appropriate."

P109 "The Commission clarifies that employees of nuclear plant generator operators and transmission entities should receive the training necessary to execute the terms of the interface agreement, and such training should be specified in the interface agreement between the parties. In addition, employees operating facilities used to provide services to meet NPIRs should be properly trained to Reliability Standard training requirements that apply to those facilities or the function served by the employees."

P124 "The Commission confirms its understanding that coordination under the Reliability Standard includes coordination among transmission entities. No party objected to the Commission's interpretation that the coordination required under Requirement R9.3.1 includes designating an entity to coordinate among various transmission entities providing unbundled services, and that such a role had been previously filled by former control area operators. Therefore, we adopt that proposal."

February 3, 2012 Order Approving Revised Definition of Protection System, Docket No. RD11-13-000
http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_approving_modif_Definition_2.3.2012.pdf

P5. The current definition of Protection System includes protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry. The revised definition with the proposed modification states:

"Protection System –

- Protective relays which respond to electrical quantities,
- Communications systems necessary for correct operation of protective functions,
- Voltage and current sensing devices providing inputs to protective relays,
- Station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply), and
- Control circuitry associated with protective functions through the trip coil(s) of the circuit breaker or other interrupting devices."

P9. The Commission finds that the ERO's modification to the definition of Protection System is just, reasonable, not unduly discriminatory or preferential, and in the public interest. As explained by NERC, battery chargers are essential to assure that batteries used to operate protection systems are in a continuous state of readiness. Therefore, it is appropriate that battery chargers be included in the definition of Protection System. The modified definition removes any uncertainty as to whether battery chargers should be included in a responsible entity's maintenance and testing program and, therefore, closes a reliability gap identified by NERC.

Order No. 788
http://www.nerc.com/FilingsOrders/us/Pages/2013fercordersrules.aspx

FERC issued a final rule approving NERC's proposed retirement of 34 requirements within 19 Reliability Standards in response to the Commission's proposal in paragraph 81 of the March 15, 2012 order in Docket No. RC11-6-000. The final rule approved the retirement of the 34 requirements that either provided little protection for Bulk-Power System reliability or were redundant with other aspects of the Reliability Standards, including NUC-001-2, Requirements R9.1, R9.1.1, R9.1.2, R9.1.3, and R1.9.4.

Revision History

Version	Date	Reviewers	Revision Description
1	May 2010	RSAW Working Group	New Document.
1	December 2010	QRSAW WG	Revised Findings Table, modified Supporting Evidence tables, and added Revision History.
1	January 2011	Craig Struck	Reviewed for format consistency and content.
1.1	September 2011	Craig Struck	Format changes for 2012.
2.2	April 2014	RSAWTF	Revised to reflect removal of R9.1 and subrequirements per Paragraph 81 project and Implementation Plan for revised term for "Protection System" per Project 2007-17.

Compliance Questionnaire and
Reliability Standard Audit Worksheet

PRC-001-1.1 — System Protection Coordination

Registered Entity: *(Must be completed by the Compliance Enforcement Authority)*

NCR Number: *(Must be completed by the Compliance Enforcement Authority)*

Applicable Function(s): **BA, TOP, GOP**

Auditors:

Disclaimer

NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

Subject Matter Experts

Identify your company's subject matter expert(s) responsible for this Reliability Standard. Include the person's title, organization and the requirement(s) for which they are responsible. Insert additional lines if necessary.

Response: ***(Registered Entity Response Required)***

SME Name	Title	Organization	Requirement

Reliability Standard Language

PRC-001-1.1 — System Protection Coordination

Purpose:

To ensure system protection is coordinated among operating entities.

Applicability:

Balancing Authorities
Transmission Operators
Generator Operators

NERC BOT Approval Date: 11/1/2006

FERC Approval Date: 3/16/2007

Reliability Standard Enforcement Date in the United States: 4/1/2013

Requirements:

R1. Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of Protection System schemes applied in its area.

Describe, in narrative form, how you meet compliance with this requirement: *(Registered Entity Response Required)*

Question:

Who are the Transmission Operator, Generator Operator, and Balancing Authority personnel identified as being familiar with the purpose and limitations of Protection System schemes applied in their area? Please provide the job titles of identified personnel.

Registered Entity Response (Required):

R1 Supporting Evidence and Documentation

Response: ***(Registered Entity Response Required)***

Provide the following: Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version
Audit Team: Additional Evidence Reviewed:		

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to PRC-001-1.1 R1.

___ Verify the identified personnel are familiar with:
___ The purpose of relay protection schemes applied in its area.
___ The limitations of relay protection schemes applied in its area.

(Protection System schemes shall include, but are not limited to, Special Protection Systems within its area.)

Note to auditor: Auditors shall use their professional judgment to determine whether identified personnel are familiar with the purpose and limitations of Protection System schemes applied in its area. Identified Generator Operator personnel should be familiar with the purpose and limitations of its generator protection system and any associated generator interconnection Facilities. In general, the purpose of relay protection schemes relates to what type of fault the protection system will detect (ground fault, phase to phase fault, failure to clear fault, backup etc.) and how the detection is accomplished (measure impedance of fault, differential measurement, etc.). Examples of limitations could include, but are not limited to, a Zone 1 relay typically being set to detect faults up to about 80% of a line, or a transformer differential relay only detecting a fault between two current transformers on each side of the transformer bank. Evidence may include, but is not limited to, training records and personnel interviews, training

with an overview of the different types of protection used on the system for generators, transmission line(s), and transformers on the entity's system. Also, an overview of the zones of protection, fault locations and which relay would operate based on the location is desirable. If the entity has Special Protection Systems (SPSs), any training could include an overview of the SPS's operation, arming and disarming of the SPS and how to verify which mode is in service. Documentation of any training provided should be specific training on the purpose of protection systems and limitations associated with the entity's system. Auditors need reasonable assurance that the required familiarity exists at the functional level (TOP, BA, GOP) of the entity. An interview of all identified personnel, or a statistical sample thereof, may be performed, but is not required.

Auditor's Detailed Notes:

R2. Each Generator Operator and Transmission Operator shall notify reliability entities of relay or equipment failures as follows:

R2.1. If a protective relay or equipment failure reduces system reliability, the Generator Operator shall notify its Transmission Operator and Host Balancing Authority. The Generator Operator shall take corrective action as soon as possible.

R2.2. If a protective relay or equipment failure reduces system reliability, the Transmission Operator shall notify its Reliability Coordinator and affected Transmission Operators and Balancing Authorities. The Transmission Operator shall take corrective action as soon as possible.

Describe, in narrative form, how you meet compliance with this requirement: ***(Registered Entity Response Required)***

Question – Did you have an equipment or relay failure during the audit period which reduced system reliability? If yes, provide evidence you notified the proper entities.

Entity Response: ***(Registered Entity Response Required)***

R2 Supporting Evidence and Documentation

Response: ***(Registered Entity Response Required)***

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version
Audit Team: Additional Evidence Reviewed:		

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to PRC-001-1.1 R2.

___ Verify the entity took the following actions related to a relay or equipment failure that reduced system reliability:

- ___ (R2.1) Generator Operator notified its Transmission Operator and Host Balancing Authority and
- ___ Generator Operator took corrective action as soon as possible.
- ___
- ___ (R2.2) Transmission Operator notified its Reliability Coordinator and affected Transmission Operators and Balancing Authorities and
- ___ Transmission Operator took corrective action as soon as possible.

Auditor's Detailed notes:

R3. A Generator Operator or Transmission Operator shall coordinate new Protective Systems and changes as follows.

R3.1. Each Generator Operator shall coordinate all new Protective Systems and all Protective System changes with its Transmission Operator and Host Balancing Authority.

R3.2. Each Transmission Operator shall coordinate all new Protective Systems and all Protective System changes with neighboring Transmission Operators and Balancing Authorities.

Describe, in narrative form, how you meet compliance with this requirement: ***(Registered Entity Response Required)***

Question: Have you made changes to new or added new Protective Systems during the audit period? If yes, provide evidence you coordinated with the appropriate entities.

Entity Response: ***(Registered Entity Response Required)***

R3 Supporting Evidence and Documentation

Response: ***(Registered Entity Response Required)***

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version
Audit Team: Additional Evidence Reviewed:		

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to PRC-001-1.1 R3.

___ Verify the entity coordinated new Protective Systems and changes as follows:
- ___ Each Generator Operator coordinated with its Transmission Operator and Host Balancing Authority.
- ___ Each Transmission Operator coordinated with neighboring Transmission Operators and Balancing Authorities.

Auditor's Detailed notes:

R4. Each Transmission Operator shall coordinate Protection Systems on major transmission lines and interconnections with neighboring Generator Operators, Transmission Operators, and Balancing Authorities.

Describe, in narrative form, how you meet compliance with this requirement: ***(Registered Entity Response Required)***

R4 Supporting Evidence and Documentation

Response: ***(Registered Entity Response Required)***

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version
Audit Team: Additional Evidence Reviewed:		

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to PRC-001-1.1 R4.

___ Verify each Transmission Operator coordinated Protection Systems on major transmission lines and interconnections with neighboring Generator Operators, Transmission Operators, and Balancing Authorities.

Auditor's Detailed notes:

R5. A Generator Operator or Transmission Operator shall coordinate changes in generation, transmission, load or operating conditions that could require changes in the Protection Systems of others:

R5.1. Each Generator Operator shall notify its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's Protection Systems.

R5.2. Each Transmission Operator shall notify neighboring Transmission Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' Protection Systems.

Describe, in narrative form, how you meet compliance with this requirement: ***(Registered Entity Response Required)***

Question: Did you experience changes in operating conditions that could require changes of Protection Systems of other entities? If yes, provide evidence of coordination.

Entity Response: ***(Registered Entity Response Required)***

R5 Supporting Evidence and Documentation

Response: ***(Registered Entity Response Required)***

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version

Audit Team: Additional Evidence Reviewed:

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to PRC-001-1.1 R5.

___ Verify each Generator Operator or Transmission Operator coordinated changes in generation, transmission, load or operating conditions that could require changes in the Protection Systems of others.

___ Verify the Generator Operator notified its Transmission Operator in advance of changes in generation or operating conditions that could require changes in the Transmission Operator's Protection Systems.

___ Verify the Transmission Operator notified neighboring Transmission Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' Protection Systems.

Auditor's Detailed notes:

R6. Each Transmission Operator and Balancing Authority shall monitor the status of each Special Protection System in their area, and shall notify affected Transmission Operators and Balancing Authorities of each change in status.

Describe, in narrative form, how you meet compliance with this requirement: ***(Registered Entity Response Required)***

R6 Supporting Evidence and Documentation

Response: ***(Registered Entity Response Required)***

Provide the following:
Document Title and/or File Name, Page & Section, Date & Version

Title	Date	Version

Audit Team: Additional Evidence Reviewed:

This section must be completed by the Compliance Enforcement Authority

Compliance Assessment Approach Specific to PRC-001-1.1 R6.

___ Verify the entity monitors the status of each Special Protection System in its area.

___ Verify the entity notified affected Transmission Operators and Balancing Authorities of each change in status.

Auditor's Detailed notes:

Supplemental Information

Other - The list of questions above is not all inclusive of evidence required to show compliance with the Reliability Standard. Provide additional information here, **as necessary** that demonstrates compliance with this Reliability Standard.

Entity Response: ***(Registered Entity Response)***

Compliance Findings Summary (to be filled out by auditor)

Req.	NF	PV	OEA	NA	Statement
1					
2					
3					
4					

5					
6					

Excerpts from FERC Orders -- For Reference Purposes Only
Updated Through March 31, 2009
PRC-001-1

Order 693

P 1418. Protection and Control systems (PRC) on Bulk-Power System elements are an integral part of reliable grid operation. Protection systems are designed to detect and isolate faulty elements on a system, thereby limiting the severity and spread of system disturbances, and preventing possible damage to protected elements. The function, settings and limitations of a protection system are critical in establishing SOLs and IROLs. The PRC Reliability Standards apply to transmission operators, transmission owners, generator operators, generator owners, distribution providers and regional reliability organizations and cover a wide range of topics related to the protection and control of power systems.

P 1419. PRC-001-1 ensures that protection systems are coordinated among operating entities by requiring transmission and generator operators to notify appropriate entities of relay or equipment failures that could affect system reliability. In addition, transmission and generator operators must coordinate with appropriate entities when new protection systems are installed, or when existing protection systems are modified.

P 1433. The Commission approves PRC-001-1 as mandatory and enforceable….

P 1435. Protection systems on Bulk-Power System elements are an integral part of reliable operations. They are designed to detect and isolate faulty elements on a power system, thereby limiting the severity and spread of disturbances and preventing possible damage to protected elements. If a protection system can no longer perform as designed because of a failure of its relays, system reliability is reduced or threatened. In deriving SOLs and IROLs, moreover, the functions, settings, and limitations of protection systems are recognized and integrated. Systems are only reliable when protection systems perform as designed. This is what PRC-001-1 means in linking a reduction in system reliability with a protection relay failure or other equipment failure.

P 1436. … we note that while the PRC Reliability Standards do not specifically require protection systems consisting of redundant and independent protection groups for each critical element in the Bulk-Power System, such requirements are included as one potential solution in the TPL Reliability Standards.

P 1438. In the case, … of a system element protected by a single protection System with a failed relay that threatens system reliability, that scenario would require the use of appropriate operating solutions including removing a system element from service. Another possible solution is to operate a system at a lower SOL or IROL that recognizes the degraded protection performance.

P 1439. Corrective actions taken by transmission operators to return a system to a secure operating state when a protective relay or equipment failure reduces system reliability normally refer to “operator control actions”, consisting of operator actions such as removing the facility without protection from service, generation redispatch, transmission re-configuration, etc. Corrective action must be completed as soon as possible, but no longer than 30 minutes after a notice of protection system failure. Failure to complete corrective action within

30 minutes will be considered a violation of the relevant IROL or TOP Reliability Standards. In contrast, troubleshooting or replacing failed relays or equipment are performed by field maintenance personnel and normally take hours or even days to complete. These actions are not normally considered corrective actions in the context of real-time operation of the Bulk-Power System.

P 1440. We believe that "[t]he transmission operator shall take corrective action as soon as possible" refers to transmission operators taking operator control actions. It does not refer to troubleshooting, repairing or replacing failed relays or equipment, etc., since these time-consuming corrective actions would prolong the risk of cascading failures to the Bulk-Power System.

P 1442. We agree … that generator operators do not have the same ability as transmission operators to take corrective control actions on the Bulk-Power System…

P 1443. As explained above, the requirement for system operators to take corrective control action when protective relay or equipment failure reduces system reliability should be treated the same as the requirement for returning a system to a secure and reliable state after an IROL violation, i.e., as soon as possible, but no longer than 30 minutes after a violation. A longer time limit would place an entity in violation of relevant IROL or TOP Reliability Standards.

P 1448. … The time allowed for mitigating actual IROL violations is very clear: as soon as possible and within 30 minutes. We clarify that our concern is not about "field protection and control personnel not being alerted about failure of relays and protection systems on critical elements." Our focus, rather, is that upon detection of failure of relays and protection systems on critical elements, field personnel must report the failures promptly to the transmission operators so that corrective operator control actions can be taken as soon as possible and within 30 minutes… with respect to …[concerns] that our proposed directives would result in local-level personnel undermining or not following the instructions of reliability coordinator personnel at a time when the system is unstable, we do not understand how local level personnel, who have no operating control of a transmission operator's system or a reliability coordinator's system could do so.

P 1449. The Commission approves Reliability Standard PRC-001-1 as mandatory and enforceable. …

June 8, 2007 Order Approving Regional Reliability Standards for the Western Interconnection and Directing Modifications, Docket No. RR07-11-000

P 87. We note that upon failure of protective relays, NERC Reliability Standard PRC-001-1 requires transmission operators and generator operators to take corrective actions as soon as possible (within thirty minutes as directed by Order No. 693). Order No. 693 clarifies that "corrective actions" do not refer to the repair of protective relays, but instead to actions that ensure the reliability of the system, such as lowering IROLs and SOLs. The proposed regional Reliability Standard does not relieve compliance with this requirement but, rather, adds more stringency by defining a maximum timeframe for removal and repair of protective equipment.

February 3, 2012 Order Approving Revised Definition of Protection System, Docket No. RD11-13-000

P 5. The current definition of Protection System includes protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry. The revised definition with the proposed modification states:

"Protection System –

- Protective relays which respond to electrical quantities,
- Communications systems necessary for correct operation of protective functions,
- Voltage and current sensing devices providing inputs to protective relays,
- Station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply), and
- Control circuitry associated with protective functions through the trip coil(s) of the circuit breaker or other interrupting devices."

P 9. The Commission finds that the ERO's modification to the definition of Protection System is just, reasonable, not unduly discriminatory or preferential, and in the public interest. As explained by NERC, battery chargers are essential to assure that batteries used to operate protection systems are in a continuous state of readiness. Therefore, it is appropriate that battery chargers be included in the definition of Protection System. The modified definition removes any uncertainty as to whether battery chargers should be included in a responsible entity's maintenance and testing program and, therefore, closes a reliability gap identified by NERC.

Revision History

Version	Date	Reviewers	Revision Description
1	October 2009	RSAW Working Group	New Document.
1	December 2010	QRSAW WG	Revised Findings Table, modified Supporting Evidence tables, and added Revision History.
1	January 2011	Craig Struck	Reviewed for format consistency and content.
1.1	September 2011	Craig Struck	Format changes for 2012.
1.2	October 2013	ECEMG	Clarified auditor guidance for R1 and R3. Other minor changes to format and wording.
1.3	February 2014	ECEMG	Clarified auditor guidance for R1.
1.4	April 2014	RSAWTF	Errata associated with Project 2007-17 regarding revised definition of "Protection System."

Reliability Standard Audit Worksheet[1]

PRC-005-1.1b — Transmission and Generation Protection System Maintenance and Testing

This section must be completed by the Compliance Enforcement Authority.

Registered Entity:
NCR Number:
Compliance Assessment Date:
Compliance Monitoring Method:
Applicable Function(s): DP, GO, TO
Names of Auditors:

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

Subject Matter Experts

Identify Subject Matter Expert(s) responsible for this Reliability Standard. (Insert additional rows if necessary)

Registered Entity Response (Required):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation or generation interconnection Facility Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include:

R1.1. Maintenance and testing intervals and their basis.

R1.2. Summary of maintenance and testing procedures.

Registered Entity Response (Required):

Describe, in narrative form, how you meet compliance with this requirement.

Registered Entity Evidence (Required):

Provide the following for all evidence submitted (Insert additional rows if necessary): File Name, File Extension, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description

Compliance Assessment Approach Specific to PRC-005-1.1b R1

This section must be completed by the Compliance Enforcement Authority

Review the evidence to verify the Registered Entity has:

(R1) Review the evidence provided by the entity to determine if the entity has a transmission Protection System and/or a generation or generator interconnection Facility Protection System (*see* Requirement 2). If yes:	
	Review the evidence provided by the entity to verify the entity has a maintenance and testing program for the Protection System. The maintenance and testing program should include:

	Protective relays which respond to electrical quantities
	Communication systems necessary for correct operation of protective functions
	Voltage and current sensing devices providing inputs to protective relays
	Station DC supply associated with protective functions (including Station batteries, battery chargers, and non battery based DC supply)
	DC control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.
Review the program and determine if it has the following for each protective system device:	
	(R1.1) Maintenance and testing intervals
	(R1.1) Basis for those intervals
	(R1.2) Summary of Maintenance and Testing procedures

Note to Auditor:

All equipment specified by the new definition that was not covered by the old definition must be included in the maintenance and testing program (i.e., a periodicity, basis, and testing/maintenance procedure) by April 1, 2013. The actual test should be completed by the end of the first specified testing cycle. (For example, if quarterly and annual battery charger tests are added, all quarterly battery charger tests should be complete by July 1, 2013 and annual tests by April 1, 2014.) For more information, review Technical Justification Resource Document for Project 2010-07 Generator Requirements at the Transmission Interface.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation or generator interconnection Facility Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Entity on request (within 30 calendar days). The documentation of the program implementation shall include:

R2.1. Evidence Protection System devices were maintained and tested within the defined intervals.

R2.2. Date each Protection System device was last tested/maintained.

Registered Entity Response (Required):

Describe, in narrative form, how you meet compliance with this requirement.

Data Request: Provide a list of all substations 100kV and above, generating stations and generator interconnection Facilities connected to the BES for use in NERC Sampling Methodology.

TEST RECORDS NOTE: If test records are provided as evidence of compliance with R2 please provide an annotated sample test record for each type of test record provided. The sample test record(s) should include descriptive annotations for each relevant section, heading, cell, etc. The annotations should include an explanation of what each relevant section/heading/cell is and what the test results are indicating. The annotations should be written from the perspective that the person reviewing the test record is unfamiliar with your test record format. Examples of annotations could include cell comments in MS Excel spreadsheets, review comments in MS Word documents, and Sticky Note comments in PDF formatted documents, to name a few.

Registered Entity Evidence (Required):

Provide the following for all evidence submitted (Insert additional rows if necessary): File Name, File Extension, Document Title, Revision, Date, Page(s), Section(s), Section Title(s), Description

Compliance Assessment Approach Specific to PRC-005-1.1b R2

This section must be completed by the Compliance Enforcement Authority

Review the evidence to verify the Registered Entity has:

(R2) Review the evidence provided by the entity to determine if the entity is required to have a Protection System maintenance and testing program. If yes:	
Review the evidence provided by the entity to determine if the entity provided the above information to its Regional Entity within 30 calendar days of the request (Prior to compliance assessment, determine if a 30 day data request was made (the audit notice constitutes a 30 day request)) and that the documentation included:	
	(R2.1) Evidence Protection System devices were maintained and tested within the defined intervals.
	(R2.2) Date when each Protection System device was last tested/maintained.
Note to Auditor: CEAs are to obtain the last date a registered entity tested and maintained its Protection System devices in order to verify compliance with PRC-005-1 R2 starting from June 18, 2007. The last maintenance or test date is necessary for a CEA to determine whether a registered entity is conducting maintenance and testing	

within the intervals defined by its own Protection System maintenance and testing program, including circumstances when the interval began prior to June 18, 2007, the mandatory and enforceable date of the standard.
However, CEAs are not to require registered entities to produce records of testing and maintenance activities conducted prior to June 18, 2007, because keeping such records was not mandatory at that time. Therefore, CEAs are only to require production of actual maintenance and testing records from June 18, 2007 forward.
When obtaining the last date of maintenance and testing activity prior to June 18, 2007, CEAs are to allow several options of evidence, including: (1) the registered entity's actual maintenance and testing records, if available, (2) a simple representation by the registered entity regarding the last known maintenance and testing date, or (3) the registered entity's good faith approximation of the previous maintenance and testing date, based on best available information.

If an entity elects to provide a CEA with the evidence listed in points (2) or (3) above, the CEA is to obtain the entity's description of the basis for its representation of an actual or estimated date. The basis can refer to the registered entity's actual knowledge, approximate periodicity of established maintenance and testing practices, timing of commissioning of equipment, or any other reasonable basis.

Focus on Current Intervals
A CEA is to enforce PRC-005-1 R2 only with consideration of interval dates beginning June 18, 2007 or later if the entity can demonstrate it has conducted the required maintenance and testing at least once since June 18, 2007, unless there is additional cause that warrants requesting additional evidence.

For example, if a registered entity completed its required maintenance and testing activities in November 2007 and provided appropriate maintenance and testing records, the CEA is to accept that evidence and is not to request the registered entity's prior maintenance and testing date if it occurred before June 18, 2007. However, a CEA is to request evidence of the registered entity's last maintenance and testing date if it occurred after June 18, 2007.

A CEA is to obtain one or more of the following as evidence of the last date of maintenance and testing activity that occurred prior to June 18, 2007 (if such evidence is necessary as discussed above):

1. Actual maintenance and testing records, if available;
2. A simple representation by the registered entity regarding the last known maintenance and testing date and the registered entity's description of the basis for its representation of an actual or estimated date. The basis can refer to the registered entity's actual knowledge, approximate periodicity of established maintenance and testing practices, timing of commissioning of equipment, or any other reasonable basis; or

3. The registered entity's good faith approximation of the previous maintenance and testing date based on best available information and the registered entity's description of the basis for its representation of an actual or estimated date. The basis can refer to the registered entity's actual knowledge, approximate periodicity of established maintenance and testing practices, timing of commissioning of equipment, or any other reasonable basis.

Auditor Notes:

Supplemental Information

Question: How does your company document and confirm that program implementation is on schedule? Include a discussion of defined maintenance and testing intervals, and your process for tracking the dates each protective device was last tested/maintained.

Question: Describe your maintenance program to periodically test protection systems in order to ensure proper performance. Include in your description how your company's program identifies the equipment specified in the NERC Glossary definition of Protection Systems (e.g. Protective relays, associated communication systems, voltage and current sensing devices, station batteries/chargers and DC control circuitry).

Other : The list of questions above is not all inclusive of evidence required to show compliance with the Reliability Standard. Provide additional information here, **as necessary** that demonstrates compliance with this Reliability Standard.

Compliance Finding Summary [Author to update table based on number of Requirements in the standard]

This section must be completed by the Compliance Enforcement Authority

Req.	NF	PV	OEA	NA	Statement
1					
2					

Additional Information:

Reliability Standard

A. Introduction

1. **Title:** **Transmission and Generation Protection System Maintenance and Testing**
2. **Number:** PRC-005-1.1b
3. **Purpose:** To ensure all transmission and generation Protection Systems affecting the reliability of the Bulk Electric System (BES) are maintained and tested.
4. **Applicability**
   - **4.1.** Transmission Owner.
   - **4.2.** Generator Owner.
   - **4.3.** Distribution Provider that owns a transmission Protection System.
5. **Effective Date:** In those jurisdictions where regulatory approval is required, all requirements become effective upon approval. In those jurisdictions where no regulatory approval is required, all requirements become effective upon Board of Trustee's adoption or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

B. Requirements

R1. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation or generator interconnection Facility Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include:

R1.1. Maintenance and testing intervals and their basis.

R1.2. Summary of maintenance and testing procedures.

R2. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation or generator interconnection Facility Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Entity on request (within 30 calendar days). The documentation of the program implementation shall include:

R2.1. Evidence Protection System devices were maintained and tested within the defined intervals.

R2.2. Date each Protection System device was last tested/maintained.

C. Measures

M1. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation or generator interconnection Facility Protection System that affects the reliability of the BES, shall have an associated Protection System maintenance and testing program as defined in Requirement 1.

M2. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation or generator interconnection Facility Protection System that affects the reliability of the BES, shall have evidence it provided documentation of its associated Protection System maintenance and testing program and the implementation of its program as defined in Requirement 2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Entity.

1.2. Compliance Monitoring Period and Reset Time Frame

One calendar year.

1.3. Data Retention

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

The Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation or generator interconnection Facility Protection System, shall retain evidence of the implementation of its Protection System maintenance and testing program for three years.

The Compliance Monitor shall retain any audit data for three years.

1.4. Additional Compliance Information

The Transmission Owner and any Distribution Provider that owns a transmission Protection System and the Generator Owner that owns a generation or generator interconnection Facility Protection System, shall each demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

2. Violation Severity Levels (no changes)

E. Regional Differences

None identified.

Appendix 1 of PRC-005-1.1b

Requirement Number and Text of Requirement
R1. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include: **R1.1.** Maintenance and testing intervals and their basis. **R1.2.** Summary of maintenance and testing procedures. **R2.** Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on request (within 30 calendar days). The documentation of the program implementation shall include: **R2.1** Evidence Protection System devices were maintained and tested within the defined intervals. **R2.2** Date each Protection System device was last tested/maintained.
Question:
Is protection for a radially-connected transformer protection system energized from the BES considered a transmission Protection System subject to this standard?
Response:
The request for interpretation of PRC-005-1 Requirements R1 and R2 focuses on the applicability of the term "transmission Protection System." The NERC Glossary of Terms Used in Reliability Standards contains a definition of "Protection System" but does not contain a definition of transmission Protection System. In these two standards, use of the phrase transmission Protection System indicates that the requirements using this phrase are applicable to any Protection System that is installed for the purpose of detecting faults on transmission elements (lines, buses, transformers, etc.) identified as being included in the Bulk Electric System (BES) and trips an interrupting device that interrupts current supplied directly from the BES. A Protection System for a radially connected transformer energized from the BES would be considered a transmission Protection System and subject to these standards only if the protection trips an interrupting device that interrupts current supplied directly from the BES and the transformer is a BES element.

Appendix 2 of PRC-005-1.1b

Requirement Number and Text of Requirement
R1. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include: **R1.1.** Maintenance and testing intervals and their basis. **R1.2.** Summary of maintenance and testing procedures.
Question:
1. Does R1 require a maintenance and testing program for the battery chargers for the "station batteries" that are considered part of the Protection System? 2. Does R1 require a maintenance and testing program for auxiliary relays and sensing devices? If so, what types of auxiliary relays and sensing devices? (i.e transformer sudden pressure relays) 3. Does R1 require maintenance and testing of transmission line re-closing relays? 4. Does R1 require a maintenance and testing program for the DC circuitry that is just the circuitry with relays and devices that control actions on breakers, etc., or does R1 require a program for the entire circuit from the battery charger to the relays to circuit breakers and all associated wiring? 5. For R1, what are examples of "associated communications systems" that are part of "Protection Systems" that require a maintenance and testing program?
Response:
~~1. While battery chargers are vital for ensuring "station batteries" are available to support Protection System functions, they are not identified within the definition of "Protection Systems." Therefore, PRC-005-1 does not require maintenance and testing of battery chargers.~~ The currently-effective definition of Protection System, includes battery chargers as an element of the definition. As a result of this inclusion, battery chargers must be maintained and tested. Thus, the modified definition of Protection System supersedes Response #1 in Appendix 2 related to battery 2. The existing definition of "Protection System" does not include auxiliary relays; therefore, maintenance and testing of such devices is not explicitly required. Maintenance and testing of such devices is addressed to the degree that an entity's maintenance and testing program for 3 DC control circuits involves maintenance and testing of imbedded auxiliary relays. Maintenance and testing of devices that respond to quantities other than electrical quantities (for example, sudden pressure relays) are not included within Requirement R1.

3. No. "Protective Relays" refer to devices that detect and take action for abnormal conditions. Automatic restoration of transmission lines is not a "protective" function.
4. PRC-005-1 requires that entities 1) address DC control circuitry within their program, 2) have a basis for the way they address this item, and 3) execute the program. PRC-005-1 does not establish specific additional requirements relative to the scope and/or methods included within the program.
5. "Associated communication systems" refer to communication systems used to convey essential Protection System tripping logic, sometimes referred to as pilot relaying or teleprotection. Examples include the following:
   - communications equipment involved in power-line-carrier relaying
   - communications equipment involved in various types of permissive protection system applications
   - direct transfer-trip systems
   - digital communication systems (which would include the protection system communications functions of standard IEC 618501 as well as various proprietary systems)

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria, or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

There are two approaches to sampling: statistical and non-statistical, and choosing which to use depends on the objectives for sampling. (When the population sample to be reviewed is documentation, a statistical approach using RAT-STATS is expected.) Both are represented in the sample guideline in line with standard practices for their use. The Audit Team Lead may determine if the scope of the audit samples should be reduced to levels below those established in the sample guideline. In doing so, the audit team will document the rationale for reducing the scope of the of sample population in the RSAW or audit report.

Additionally, separate from the audit, the registered entity may use this methodology to determine the sample population to test in order to provide themselves reasonable assurance that management's expectations are being met by the organization.

Regulatory Language for Reference Purposes Only (through March 28, 2014)

Order No. 693 [cite]
http://www.nerc.com/files/order_693.pdf

P 1418. Protection and Control systems (PRC) on Bulk-Power System elements are an integral part of reliable grid operation. Protection systems are designed to detect and isolate faulty elements on a system, thereby limiting the severity and spread of system disturbances, and preventing possible damage to protected elements. The function, settings and limitations of a protection system are critical in establishing SOLs and IROLs. The PRC Reliability Standards apply to transmission operators, transmission owners, generator operators, generator owners, distribution providers and regional reliability organizations and cover a wide range of topics related to the protection and control of power systems.

P 1470. PRC-005-1 ensures that all transmission and generation protection systems affecting the reliability of the Bulk-Power System are maintained and tested by requiring the transmission owners, distribution providers, and generator owners to develop, document, and implement a protection system maintenance program that may be reviewed by the regional reliability organization.

P 1474. For the reasons stated in the NOPR, the Commission approves Reliability Standard PRC-005-1 as mandatory and enforceable.

Order Approving Interpretation (September 26, 2011)
http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_approving_PRC-004-1_interp_2011.9.26.pdf

P 7. NERC interprets "transmission Protection System," as it appears in Requirements R1 and R3 of PRC-004-1 and Requirements R1 and R2 of PRC-005-1, to mean "any Protection System that is installed for the purpose of detecting faults on transmission elements (lines, buses, transformers, etc.) identified as being included in the Bulk Electric System (BES) and trips an interrupting device that interrupts current supplied directly from the BES."[Footnote omitted.] In addition, NERC's proposed interpretation states that "[a] Protection System for a radially connected transformer energized from the BES would be considered a transmission Protection System and subject to these standards only if the protection trips an interrupting device that interrupts current supplied directly from the BES and the transformer is a BES element."[Footnote omitted.]

P 11. The Commission approves NERC's interpretation as it is consistent with the intent of Requirements R1 and R3 of PRC-004-1 and Requirements R1 and R2 of PRC-005-1. The interpretation clarifies that the Requirements are "applicable to any Protection System that is installed for the purpose of detecting faults on transmission elements (lines, buses, transformers, etc.) identified as being included in the [BES] and trips an interrupting device that interrupts current supplied directly from the BES."[Footnote omitted.] This

interpretation is consistent with the Commission's understanding that a "transmission Protection System" is installed for the purpose of detecting and isolating faults affecting the reliability of the bulk electric system through the use of current interrupting devices. The Commission further understands that the "interrupting device" referred to in the interpretation is a device that has the performance capability to interrupt full fault current associated with the protected bulk electric system facilities.

Order Approving Modification of Definition for Protection System (February 3, 2012)

P5. The current definition of Protection System includes protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry. The revised definition with the proposed modification states:

> **"**The modified definition approved herein shall supersede the interpretation of Requirement R1 of Reliability Standard PRC-005-1 approved concurrently with this order in Docket No. RM10-5-000 on the effective date of the modified definition (the first day of the first calendar quarter twelve months from approval, i.e., April 1, 2013).
>
> "Protection System –
> - Protective relays which respond to electrical quantities,
> - Communications systems necessary for correct operation of protective functions,
> - Voltage and current sensing devices providing inputs to protective relays,
> - Station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply), and
> - Control circuitry associated with protective functions through the trip coil(s) of the circuit breaker or other interrupting devices."

P6. In the Petition, NERC explains that the modification will improve the definition by clearly identifying the essential elements that constitute a Protection System. NERC states that battery chargers are an essential piece of the bulk power system that should be included in the definition since battery chargers function to assure that batteries associated with protection systems are in a continuous state of readiness.

Order Approving Generator Requirements at the Transmission Interface, Order No. 785, 144 FERC ¶ 61,221 (2013) http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Final%20Rule%20RM12-16-000.pdf

P7. "NERC asserted that the proposed modifications in Reliability Standards PRC-004-2.1a and PRC-005-1.1b are designed merely to clarify that their requirements extend not only to protection systems associated with the generating facility or station itself, but also to any protection systems associated with the generator interconnection facilities."

P10. In the NOPR, "the Commission found that the clarifications proposed in PRC-004-2.1a and PRC-005-1.1b would mitigate the possibility that the standards' requirements could be interpreted to exclude the generator interconnection facilities."

P 30. "We agree with NERC that the changes mitigate the possibility that entities could interpret the standards to exclude generator interconnection facilities."

Revision History

Version	Date	Reviewers	Revision Description
1	December 2009	RSAW Working Group	New Document
1	December 2010	QRSAW WG	Revised Findings Table, modified Supporting Evidence tables, and added Revision History
1	January 2011	Craig Struck	Reviewed for format consistency and content. Added test record annotation remarks for R2 evidence.
1.1	September 2011	Craig Struck	Format update for 2012.
1.1	October 2011	NERC Legal	Updated Excerpts from FERC Orders from March 31, 2009 through and including October 19, 2011.
2	March 2013	RSAW WG	Updated template, added interpretation, revised for new definition of protection system, and updated title.
2.1	March 2014	RSAW Task Force	Added auditor guidance from CAN-0008, CAN-0009, and CAN-0043.
2.2	March 2014	RSAW Task Force	Revised to reflect .1 errata changes. Legal updated Regulatory Language section.
2.3	May 2014	NERC Compliance	Update appendix 2 of standard to delete question excluding battery charges.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

High AC Voltage Can Lead to Remote Terminal Unit (RTU) Failures

Primary Interest Groups
Generator Owners (GOs)
Generator Operators (GOPs)
Transmission Owners (TOs)
Transmission Operators (TOPs)

Problem Statement
High ac voltage delivered to remote terminal unit (RTU) control cards can cause RTU failures. The RTU failure mode caused by this high, applied ac voltage can cause random trips and closure of circuit breakers connected to the RTU, which could lead to large outages on the bulk power system. Three instances of this type of failure have been reported through the NERC Event Analysis process.

Details
If ac voltage is being switched by an RTU control output card, moderately high ac voltage for a prolonged period or very high ac voltage for a short duration can cause the metal oxide varistors (MOVs) on the control card to break down. This varistor breakdown can lead to the equivalent of a control output contacts being shorted. This shorting of output contacts can lead to random operation of devices that are connected to these RTU control outputs. In addition, the breakdown of the varistors can lead to excessive heating, which can melt ribbon cables, leading to random trips and closure of circuit breakers connected to the RTU. This failure mode is not exclusive to one RTU vendor, and the reports submitted identifying this failure mechanism have not been exclusive to one vendor.

Research indicated that most RTUs are susceptible to this type of failure due to high voltage applied to the control board. The cause of the high ac voltage can be varied. For example, a CCVT delivered high voltage for approximately three minutes before failing catastrophically. In another instance, an EHV transmission line conductor fell across a lower-voltage transmission line, causing momentary high voltage from the potential transformer at the lower-voltage substation. Yet, in another case, a programmable logic controller delivered high ac voltage to an RTU, which caused the random trips.

Corrective Actions
The corrective actions implemented by the affected entities are dependent upon the specific situations each event presented. One solution is to apply high voltage protection (i.e., MOVs) on the ac circuits connected to the control boards, external to the RTU. Another solution is to use an external interpose relay for all ac control switching to eliminate any ac on the RTU control output board.

In most instances, RTUs are limited to a certain number of control points per output card. One solution was to try to isolate the ac voltage inputs from the dc control voltages—commonly used for breaker controls—by not having dc and ac signals on the same control output card. In this solution, if high ac voltage were to

cause a breakdown of the MOVs, the shorted MOVs would not be shorting out contacts that had dc (breaker control) on them. In effect, isolating the high ac voltage from dc control voltages would alleviate erroneous breaker trips and closures.

Lessons Learned

If an entity employs a station RTU to switch ac voltages via the RTU control functionality, the entity should consider researching the effects that high ac voltage may have on the RTU control. If random trips and closures are a possible effect of high ac voltages, the entity should consider preventive mitigation if the entity's Station also interacts with dc control voltages.

NERC's goal in publishing lessons learned is to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system. NERC requests that you provide input on this lesson learned by taking the short survey provided in the link below.

Click here for: Lesson Learned Comment Form

For more information, please contact:

NERC – Lessons Learned (via email)	FRCC – Lessons Learned (via email)
Source of Lesson Learned:	Florida Reliability Coordinating Council
Lesson Learned #:	20140501
Date Published:	May 20, 2014
Category:	Relaying and Protection Systems

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing reliability standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Circuit Breaker Modification Leads to Inadvertent Trips

Primary Interest Groups
Transmission Owners (TOs)
Transmission Operators (TOPs)
Generation Owners (GOs)
Generation Operators (GOPs)

Problem Statement
Sulfur hexafluoride (SF6) gas circuit breaker controls were field modified to trip on low gas and air pressure. This field modification resulted in the breakers tripping when direct current (DC) power was removed and then re-applied to the SF6 Gas circuit breaker.

Details
This model of SF6 circuit breaker comes prewired from the manufacturer to lock-on-bus (disable tripping) for falling SF6 gas pressure and for falling air pressure. This is necessary to prevent operation of the circuit breaker when there is not enough stored energy (air pressure) for the operating mechanism or if there is not sufficient SF6 pressure in the interrupter chamber to interrupt a fault. The Entity determined that the risk of locking circuit breakers on the bus had a greater impact to the grid than tripping a circuit breaker under these conditions and reconfigured the circuit breaker to trip on falling SF6 gas pressure or falling air pressure. The modification made to this model of circuit breaker involved connecting manufacturer-provided low-pressure auxiliary relay contacts labeled for use in the primary and secondary trip circuits in parallel with the control switch trip contact.

This scheme worked correctly as long as the DC to the trip circuit was not disconnected. However, when the DC was removed, the low-pressure auxiliary relay coils became de-energized, closing the contacts (“b” contacts) connected to the trip circuits. This set up a trip signal to the trip coils which was initiated as soon as the DC source was turned back on because the operating time of the low-pressure auxiliary relay to re-open the tripping contacts is several cycles.

During construction activities, the DC secondary power source (DC #2) to multiple SF6 gas circuit breakers in a station was temporarily removed to facilitate relocation of a DC disconnect box. The DC #2 source fed the low gas and low air pressure trip circuits. When the DC circuits were re-energized, this resulted in multiple SF6 gas circuit breakers opening upon restoration of the DC power. This action open ended multiple transmission lines and resulted in a generation facility being disconnected from the system.

Corrective Actions
The entity reconfigured/redesigned the pressure switch and auxiliary relay circuit. The pressure switch was changed to energize the auxiliary relay on falling/low pressure. Consequently, the tripping of the circuit breaker is accomplished through an auxiliary relay “a” contact. This alleviated a standing trip on the circuit breaker when DC supply power was removed from the gas circuit breaker. (See attached schematic)

Lesson Learned

When making changes to original factory equipment schemes, entities should analyze the scheme change to ensure that the removal/restoration of DC power to the scheme does not cause an undesirable operation.

NERC's goal in publishing lessons learned is to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system. NERC requests that you provide input on this lesson learned by taking the short survey provided in the link below.

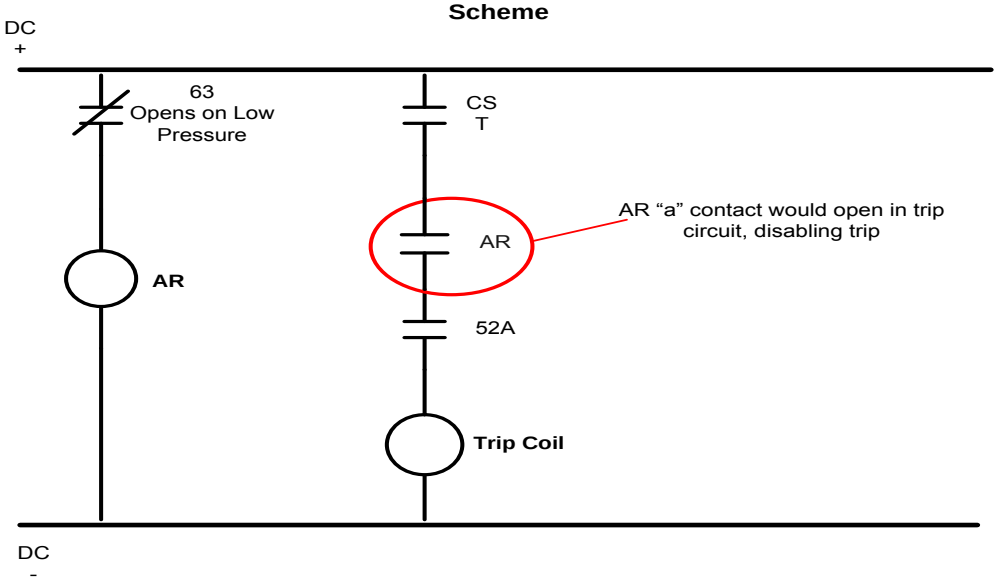
Click here for: Lesson Learned Comment Form

For more information, please contact:

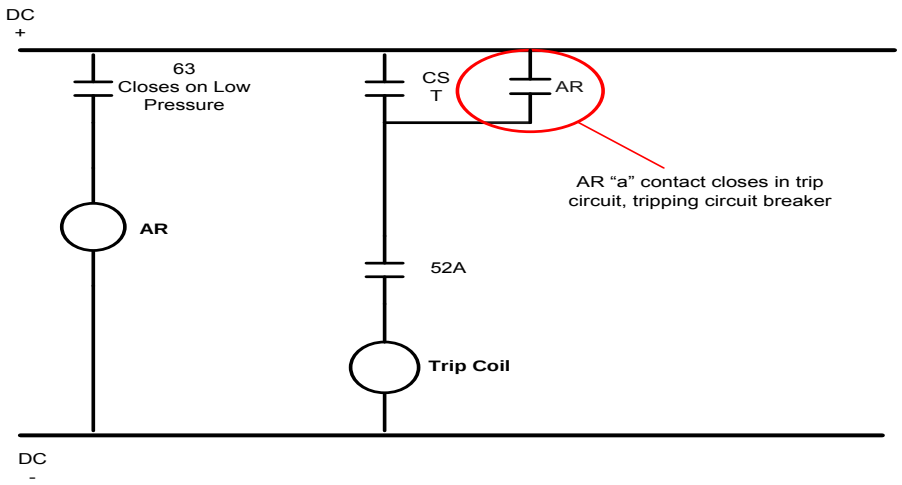
NERC – Lessons Learned (via email)	David Penney (via email) or (512) 583-4958
Source of Lesson Learned:	Texas Reliability Entity
Lesson Learned #:	20140502
Date Published:	May 20, 2014
Category:	Facility Design, Commission and Maintenance

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing Reliability Standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

Original Factory Scheme



Entity 2nd modification



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Improved Contractor Oversight Needed

Primary Interest Groups
Transmission Owners (TOs)
Generation Owners (GOs)
Generation Operators (GOPs)
Distribution Providers (DPs)

Problem Statement
Multiple instances of vendor performed work in stations without a verification method in place for ensuring work quality have caused significant system disturbances.

Details
Following are three examples of events that took place due to the lack of vendor oversight:

1. A generation facility experienced a trip due to an internal fault in a sulfur hexafluoride (SF6) gas breaker. The breaker trip interrupted power to the auxiliary transformer that is the normal feed for a generating plant. The generation facility is equipped with a fast bus transfer scheme that isolates the auxiliary transformer and closes in a startup transformer. Upon closure of the startup transformer a 487/T1 B phase startup transformer differential relay actuated. The 487/T1 relay signal inputs to a 286/T1 lockout relay which when triggered initiates de-energization of the startup transformer, causing it to be isolated.

   Investigation revealed that two splices on the startup transformer's current transformer (CT) were missing insulating sleeves. This created an alternate path for the CT secondary current, which impacted the differential protection scheme operation by causing the 487/T1 to actuate.

   Prior to the event, an inspection of a startup transformer's junction boxes found a leaking substance from the wires within the boxes. A work order was issued to replace the startup transformer's CT penetration blocks. The utility hired a vendor to replace the junction boxes per an aggressive schedule. During this effort, the vendor's scope of work grew to include control cable replacement.

   After the vendor's work was completed, two of the CT penetrations were found to be leaking and the vendor was asked to return in order to replace the leaking CT penetrations. During this replacement two insulating sleeves that are necessary to prevent terminal-to-terminal contact, were inadvertently not installed on the external connections which led to the differential relay action that isolated the start-up transformer.

2. A nuclear generating unit correctly tripped due to the loss of a reactor coolant pump, but then separated from the 230kV switchyard (Loss of Offsite Power, LOOP) due to incorrect logic with the unit's turbine underfrequency protection scheme. The turbine underfrequency protection scheme had been replaced with microprocessor relays, as part of the main generator protective relaying protection upgrade project during the unit's previous refueling outage.

The turbine underfrequency protection scheme protects the turbine. If the grid frequency reaches one of four unacceptable set points, each with a specified time duration, the four 230kV switchyard breakers will open and separate the unit from the grid. The original turbine underfrequency protection scheme had a 'unit offline block' that defeated the scheme if the unit was offline, thus no inadvertent LOOP events had been previously caused by this scheme.

The GO hired a vendor to perform the design, installation, and testing for the turbine underfrequency protection scheme replacement. The 'unit offline block' scheme had been successfully incorporated into three of the four frequency set points. The 'unit offline block' was not incorporated in the settings (logic) of the new microprocessor relays for the instantaneous frequency set point (lowest frequency, no time delay to trip allowed). The GO did not successfully communicate to the vendor the need for the 'unit offline block' to be included with all four frequency set points, although the GO's logic diagrams for the turbine underfrequency protection scheme identified this requirement. The GO had provided the vendor the turbine underfrequency protection scheme design used for a similar scheme replacement from a unit at another plant location. This design had similar logic, but a different voltage restraint set point effectively blocked the turbine underfrequency protection scheme when the unit was offline. Without the 'offline block', a LOOP event could possibly occur anytime the subject unit tripped. Neither the vendor who developed the settings, nor the GO personnel who reviewed and accepted them recognized the settings error.

The GO performed commissioning testing per the scheme's design. The vendor performed Factory Acceptance Testing (FAT testing) prior to shipment of the relaying. The FAT testing validated the panel wiring and relay set points, and also verified proper operation of relays. Since the scheme's design, as defined in the vendor produced calculation, did not address the missing block function, the error was not identified during commissioning.

The primary factors contributing to the LOOP event were the failure to communicate the need for the unit offline block, as identified in the logic diagrams; and, utilizing a design with a similar error.

3. Entity personnel performed a switching operation on Gas Insulated Switchgear (GIS) to remove a capacitor bank and bus section from service for a maintenance activity. This required the operation of the bus section motor operated ground switch for the purpose of safely grounding the capacitor bank. When the section motor operated ground switch was operated, a line-to-ground fault was detected within the GIS bus. The GIS breakers operated properly and successfully cleared the fault.

It was later determined that the GIS manufacturer used incorrect assembly drawings. The manufacturer reversed a bus section disconnect switch and ground switch module. This resulted in two ground switches being installed on one bus section and none on another section. The issue was caused by insufficient handling of a design variation. The position of the affected GIS module was changed by the manufacturer to avoid physical interference with a steel structure. The drawing was modified and the variation order was sent to the switchgear factory, however there were no markings to identify this change. There was no check of the arrangement with the single line diagram (which included the correct configuration) in the process chain that followed. Also, the manufacturer's commissioning engineer did not identify the discrepancy between the physical arrangement of the GIS module and the electrical single line diagram during the final project commissioning performed by the manufacturer.

Lesson Learned

These events highlight the need for vendor oversight policies to include a discussion with the vendor of performance standards, expectations for the work, human error reduction techniques, and verification of completed work. It is common practice in the electric industry for an entity to supplement its workforce with a vendor's specialized skills. As shown by these events the expectations between the entity and vendor with regard to the design, validation of calculations and settings, scheme testing and commissioning must be clear to ensure a successful outcome. Effective oversight of contractor work activities should be in place to help prevent these types of events.

Note: This lesson learned (LL) combines several LLs that have been submitted by different Regions. This subject is also mentioned in LL20140202: A Generating Station Ground Mat Problem Led to the Trip of Two Generating Units (2000 MW), published by NERC on February 25, 2014, and LL20140302: Verification of Alternating Current Quantities during Protection System Commissioning, published by NERC on March 11, 2014.

NERC's goal in publishing lessons learned is to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system. NERC requests that you provide input on this lesson learned by taking the short survey provided in the link below.

Click here for: Lesson Learned Comment Form

For more information, please contact:

NERC – Lessons Learned (via email)	Alan Wahlstrom (via email) 501-688-1624
Source of Lesson Learned:	ReliabilityFirst, SERC Reliability Corporation, and Southwest Power Pool
Lesson Learned #:	20140503
Date Published:	May 20, 2014
Category:	Facility Design, Commission and Maintenance

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing Reliability Standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

FLORIDA RELIABILITY COORDINATING COUNCIL, INC.
3000 BAYPORT DRIVE, SUITE 600
TAMPA, FLORIDA 33607-8411
PHONE 813.289.5644 • FAX 813.289.5646
WWW.FRCC.COM

D R A F T

2015 Business Plan and Budget

Florida Reliability Coordinating Council, Inc.

DATE: 5/16/2014 D R A F T

Table of Contents

Introduction 3

Organizational Overview 3

Membership and Governance 4

Statutory Functional Scope 5

2015 Goals and Key Deliverables (Regional Entity Division) 7

2014 Statutory Budget and Projection and 2015 Budget Comparisons 12

Section A – Statutory Programs 13

Reliability Standards Development Program 14

Compliance Monitoring and Enforcement Program and Organization Registration and Certification Program 18

Reliability Assessment and Performance Analysis Program 24

Training, Education, and Operator Certification Program 29

Situation Awareness and Infrastructure Security Program 33

General and Administrative 36

Section B – Supplemental Financial Information 40

Reserve Balance 41

Breakdown by Statement of Activity Sections 42

Section C – Non-Statutory Activities 48

2014 Member Services Budget and Projection and 2015 Budget Comparisons 55

Section D – Additional Consolidated Financial Statements 58

Introduction

TOTAL RESOURCES (in whole dollars)	2015 Budget	U.S.	Canada	Mexico
Statutory FTEs	30.91			
Non-statutory FTEs	18.35			
Total FTEs	49.26			
Statutory Expenses	$ 7,179,844			
Non-Statutory Expenses	$ 8,422,053			
Total Expenses	$ 15,601,897			
Statutory Inc(Dec) in Fixed Assets	$ (17,611)			
Non-Statutory Inc(Dec) in Fixed Assets	$ (30,071)			
Total Inc(Dec) in Fixed Assets	$ (47,682)			
Statutory Working Capital Requirement*	**(657,395)**			
Non-Statutory Working Capital Requirement**	**122,583**			
Total Working Capital Requirement	**(534,812)**			
Total Statutory Funding Requirement	$ 6,504,838			
Total Non-Statutory Funding Requirement	$ 8,514,565			
Total Funding Requirement	$ 15,019,403			
Statutory Funding Assessments	$ 6,237,838	$ 6,237,838		
Non-Statutory Fees	$ 8,240,106	$ 8,240,106		
NEL				
NEL%				

*Refer to Table B-1 on page 42 in Section B.
**Refer to the Reserve Analysis on page 58 in Section C.

Organizational Overview

The Florida Reliability Coordinating Council (FRCC) is a Florida not-for-profit corporation that was formed in 1996 and is one of the eight regions of the North American Electric Reliability Corporation (NERC). The FRCC's mission is to ensure and enhance the reliability and adequacy of the Bulk Electric System (BES) in Florida now and into the future. The FRCC's Web site is www.frcc.com. The FRCC Region is comprised of all of Florida east of the Apalachicola River. Florida's unique geography and its highly integrated transmission system coupled with its single interface boundary to the rest of the Eastern Interconnection required the development of a reliability focus in the FRCC Region. Membership in the FRCC's Regional Entity Division is open to any entity, without cost, that has a material interest in the reliability of the BES in the FRCC Region. Currently there are 69 Registered Entities within the FRCC

Region. The FRCC is governed by a balanced stakeholder Board of Directors, and accomplishes its activities through qualified professional staff and standing committees which also have balanced stakeholder governance.

The FRCC provides the statutory functions and services for the FRCC Region through its Regional Entity Division. Non-statutory services for the FRCC Region are provided through its Member Services Division. This divisional structure is an efficient and effective means of clearly separating statutory and non-statutory activities and related funding for each. The revised FRCC Bylaws, creating this divisional structure, were first approved by the Federal Energy Regulatory Commission ("FERC") on March 21, 2008.

The FRCC Regional Entity Division works to enhance the reliability of the BES in the FRCC Region pursuant to the approved Regional Delegation Agreement with NERC, as the Electric Reliability Organization ("ERO"), under the authority of the FERC. The functions performed by the FRCC Regional Entity Division include regional reliability standards development, compliance monitoring and enforcement of reliability standards, reliability assessment and performance analysis, event analysis and reliability improvement, training and education, situation awareness and infrastructure security. The Regional Entity division of the FRCC has one standing committee, the FRCC Regional Entity Committee and Compliance Forum (RECCF). This committee provides input to the FRCC in support of the delegated activities and functions.

The Member Services division of the FRCC provides, coordinates and administers a variety of services relating to the reliable planning and operation of the BES within the FRCC Region. These services are carried out by the FRCC Planning Committee (PC) and the FRCC Operating Committee (OC) and their various subcommittees, task forces and working groups, as well as FRCC Staff.

The FRCC PC and OC actively participate in the development and approval of their committee's budget. The budgets reflect activities of each committee's responsibilities, such as reliability coordination, resource adequacy, stability studies, transmission studies, operations tools, telecommunication tools and infrastructure.

Each year, the total FRCC budget is presented to the FRCC Board of Directors early in the second quarter for informational purposes prior to final approval in June. This process gives all FRCC members advanced indication of the funding level, both statutory and non-statutory, which will be required for the coming fiscal year (January 1 – December 31). This allows for timely inclusion of each member's funding responsibility in their individual budgeting process. The final budget is presented for approval to the FRCC Board of Directors in June of each year and is then submitted to NERC for approval by the NERC Board of Trustees and then by FERC.

Membership and Governance

The FRCC's members (in both divisions) include investor-owned utilities, cooperative utilities, municipal utilities, power marketers, independent power producers and others. Membership is currently 30 FRCC members in the Regional Entity Division and 23 FRCC members in the Member Services Division including affiliate and adjunct members.

The FRCC has six (6) membership sectors which include the following:

- Non-Investor Owned Utility Wholesale
- Load Serving Entity
- Generating Load Serving Entity
- Investor Owned Utility
- Suppliers
- General

There are currently two (2) members in the General Sector of the Regional Entity Division and no members in the General Sector of the Member Services Division.

The activities of FRCC are governed by its Board of Directors. The Board is comprised of senior level executives from members of FRCC.

As part of its responsibilities, NERC, as the ERO, delegates its authority to Regional Entities to perform certain functions through delegation agreements. On October 21, 2010, FERC approved revised delegation agreements between NERC and the eight (8) Regional Entities that became effective January 1, 2011 and will expire at the end of 2015. These delegation agreements describe the responsibility and authority delegated to the Regional Entities. NERC and the Regional Entities revised the delegation agreements in 2010 to improve the efficiency, transparency, quality and effectiveness of the combined NERC and Regional Entity operations. The funding for Regional Entities is approved separately with each Regional Entity submitting its own business plan and budget for consideration by NERC and FERC.

Statutory Functional Scope

The FRCC carries out its delegated functions as outlined and detailed in Exhibits A, B, C, D and E of the delegation agreement. NERC and the Regional Entities will continue to work under the existing regulatory framework governing the establishment and enforcement of reliability standards for the BPS. The existing delegation agreements expire on January 1, 2016. NERC and the Regional Entities will work collaboratively to identify any necessary revisions to the delegation agreements as renewal efforts begin in 2014 and continue through 2015. The delegated functions as defined by the NERC Rules of Procedures include:

- Reliability Standards Development (“RSD”) - Section 300
- Compliance Monitoring and Enforcement (“CMEP”) - Section 400
- Organization Registration and Certification - Section 500 (This program budget has been combined with the Compliance Monitoring and Enforcement function budget.)
- Reliability Assessment and Performance Analysis (“RA”) - Section 800 (including necessary data gathering activities and Events Analysis)
- Training, Education and Operator Certification (“TE”) - Section 900
- Situation Awareness and Infrastructure Security (“SA”) - Section 1000

2015 Key Assumptions

The NERC and Regional Entity business plans and budgets reflect a set of common assumptions (see Exhibit A of the 2015 NERC Business Plan and Budget) developed jointly by NERC and the Regional Entities as part of the annual business plan and budget process. The significant assumptions underlying FRCC's 2015 business plan include:

- NERC will provide oversight of the Regional Entities performance of their delegated functions to ensure that the delegated responsibilities are adequately performed. The Regional Entities are expected to continue to have the primary responsibility for day-to-day operations and interactions with Registered Entities. NERC and the Regional Entities will also work to refine and revise procedures and processes to eliminate duplication, increase operational efficiencies, to enhance ERO-wide consistency and to achieve measurable reliability outcomes, consistent with their respective roles and responsibilities.
- Cost pressures may affect some stakeholder resources available to participate in NERC and Regional Entity activities. However, the assumption of continued industry participation in support of key program areas such as event analysis, reliability assessments and standards development is included in this business plan and budget. NERC and the Regional Entities will evaluate projected initiatives involving stakeholder participation to determine the availability and adequacy of industry resources to support these undertakings.
- The effective date for compliance with the CIP Version 5 standards will be April 1, 2016 for High and Medium impact assets and April 1, 2017 for Low impact assets. The transition between V3 to V5 will be a mission critical activity in 2015. The Regional Entities must plan to support the ongoing CIP v5 transition plans and should anticipate an expansion in the number of Registered Entities that require guidance during 2015. For most CIP activities, the resource demands are expected to increase throughout the planning period.
- The implementation of a BES exception process will require the allocation of resource requirements from several FRCC departments. Resources are expected to manage the process execution, technical validation of the definition and exception requests, and requests for registration and certification reviews. However, the long-term impact cannot be fully assessed at this time as the resource requirements will be based on the number and complexity of exception and registration requests received.
- NERC will continue to budget and incur costs to operate and maintain the software applications and systems known as Situational Awareness for FERC, NERC, and Regional Entities ("SAFNR"). Additional resource investments may be required to enhance the capabilities of SAFNR throughout the planning period; however, there will be no increased cost to the Regional Entities. NERC will continue to review the appropriateness of continued funding of existing reliability tools, with any proposed changes thereto subject to review and input from the Regional Entities, appropriate NERC Committees and working groups, and other affected parties.
- NERC and the Regional Entities will collaboratively work to build and develop ERO Enterprise applications supporting both NERC and Regional Entity operations that will maximize efficiency of technology hardware, consistency of application, resources and data security. These will be managed by a single Project Management Office (PMO) at

NERC. ERO Enterprise funding for the development and maintenance of Enterprise applications will be subject to the budget and funding limits set forth in the approved Business Plan and Budget. The FRCC will also continue to fund applications and systems to satisfy our regional business needs.

- Improved disaster recovery mechanisms and improved IT security procedures will increase capital and operating costs at the Regional Entities.

2015 Goals and Key Deliverables (Regional Entity Division)

- Support NERC's goals that will continue to improve the quality and content of Reliability Standards, including a cost effectiveness assessment of proposed standards.
- Continue to encourage stakeholder awareness and participation in the NERC standards development process through educational outreach efforts and participation in Standard Drafting Teams, the NERC Standards Committee and related subcommittees. Support NERC's efforts to develop the bulk power system risk profile and assess standards compared to the profile and address the most important risk gaps.
- Work with NERC and the other Regional Entities, to continue refinement, improvement and prioritization of risk based compliance monitoring efforts. Continue support of the Reliability Assurance Initiative, including providing the necessary training for compliance and enforcement staff.
- Work with NERC and the other Regional Entities to register entities commensurate with risk to the Bulk Power System (BPS). Support the implementation of any changes resulting from the registration review that began in 2014.
- Continue the implementation of the BES exception process which began mid-2014.
- Work with NERC and the other Regional Entities to hold the industry accountable for violations that create serious risk to the BPS. Improve consistency, quality, and timeliness of compliance monitoring and enforcement activities while utilizing more enforcement discretion for those violations that have minimal impact to the reliability of the BES.
- Continue to be a strong enforcement authority that is independent, without conflict of interest, objective and fair, using enforcement discretion when warranted and imposing penalties and sanctions that are commensurate with risk.
- Support an ERO culture of reliability excellence. Work with NERC and the other Regional Entities to facilitate a learning environment throughout the industry. Work to improve event causal analysis, communication of lessons learned, tracking of recommendations, and implementation of best practices.
- Continue to improve consistency, quality, timeliness and cost effectiveness of NERC and Regional Entity data collection, analysis systems and capabilities through process improvements and more effective coordination and collaboration.
- Support NERC's efforts to move toward and implement an outcome based approach in Reliability Assessments to achieve measureable improvements in the BES reliability. Risks will be identified and prioritized based on reliability impacts, cost/practicality assessments, projected resources, and emerging issues.

- Work closely with the other Regional Entities and NERC to ensure that the delegated functions are implemented consistently and rationally and to promote the success of the ERO as a collaborative enterprise. Perform delegated functions with independence, without conflict of interest, with objectivity and fairness and with increased transparency.
- Support the ERO in addressing and mitigating reliability risks. Work with NERC and the other Regional Entities and the industry to effectively address security vulnerabilities and threats. During crisis situations, support ERO sharing of information among industry, Regions, and government.

2015 Overview of Cost Impacts

The FRCC's proposed 2015 Regional Entity budgeted expenses and net fixed assets (see page 12) is $7,162,233, which is a $368,944 or 5.4% increase over the 2014 budget. The major drivers of this increase are the net effect of:

- Increased compliance software maintenance and development to reflect current costs from the vendor, implement changes necessary to implement RAI and for needed portal efficiencies and program improvements.
- Increased allocated General and Administrative expense due to implementing succession plans for key functions involving a temporary increase of 1 FTE for training to succeed an anticipated retirement
- Budgeted 3% annual merit increase.
- Reduced Medical Benefits expense based on actual experience.
- Decrease in legal fees due to in house legal support.

Statutory Accounting Methodology

The FRCC, in order to be consistent with all the regions, has modified its accounting reporting as follows:

- ERO assessments needed to fund working capital are reflected in the General and Administrative Program within Administrative Services.
- The majority of the Operating Expenses are accounted for within their related department's budget. If an expense cannot be specifically linked to a department, it is included in the General and Administrative Program, within Administrative Services.
- All expenses for the Administrative Services Programs, referred to as indirect expenses for 2015, are allocated to the delegated program areas by their respective FTEs and are shown on one line of each delegated program area Statement of Activities as "Indirect Expenses".
- Capital expenditures are broken out as fixed assets at the end of each statement of activities rather than being included in their related lines in the operating expenses section.
- Expenses include depreciation, but since funding is not being requested for depreciation expense, it has been deducted from the funding requirement for capital expenditures.

2015 Key Deliverables by Program

In 2015, FRCC will achieve the following key deliverables:

- **Reliability Standards Development** — Continue support of NERC in its efforts to improve the quality and content of Reliability Standards and to support NERC's implementation of a cost effectiveness assessment of proposed standards. Support NERC in its efforts to evaluate significant BPS events (Category 3 and above) to identify gaps in standards and address any gaps identified. Support NERCs plan to develop or modify the Reliability Standard Audit Worksheets (RSAWs) by the time a Reliability Standard is balloted. Develop regional reliability standards as needed to support NERC's prioritized work plan and provide increased coordination of standards development activities.
- **Compliance Monitoring and Enforcement** — Continue to support the development and implementation of the Reliability Assurance Initiative, including implementation of the ERO Auditor Handbook and Manual and implementation of the common methodology to assess risk and determine the scope of monitoring activities. Ensure timely and thorough mitigation of all violations of mandatory reliability standards with the most focus on those violations that create serious risk to the Bulk Electric System. Promote a strong culture of compliance excellence, reliability improvement, and risk-based methods among all registered entities in the FRCC Region.
- **Event Analysis** — Continue to support improved reliability through reporting and categorizing of system events and security incidents. Consistently analyze events and system performance for sequence, cause, and remediation to identify reliability risks and trend, and to inform standards, compliance, and other programs. Work to ensure that the industry is well informed of system events, emerging trends, risk analysis, lessons learned and expected actions. Provide timely written lessons learned and recommendations from events and provide all BPS system event reports to the industry through a secure portal.
- **Critical Infrastructure Protection and Cyber Security** — Facilitate, educate and support Registered Entities in complying with CIP reliability standards and responding to cyber security alerts. Facilitate a proactive action plan by industry that demonstrates effective identification and mitigation of security risks, including safeguarding of assets, developing mitigation alternatives, and preparing and testing recovery plans. Support the transition from CIP V3 to V5 including provision of necessary training to FRCC staff, and providing education and outreach to stakeholders to ensure their understanding of the technical aspects of the requirements.
- **Reliability Assessments** — Provide annual, seasonal, probabilistic, scenario and special reliability assessments of the reliability of the FRCC BES in accordance with definitions and requirements. Work with NERC and the other Regional Entities to develop and demonstrate BES performance metrics for the purpose of analyzing and trending reliability improvements and benefits, as well as risk/severity based methods. Work with NERC and the other Regional Entities to support the exception process for the evaluation of Exception Requests as permitted by the revised definition of the BES and the NERC Rules of Procedure.

- **Situation Awareness** — Continue to support NERC in maintaining and enhancing the current and future situation awareness capabilities that include near real-time information and communications protocols that meet the needs of FERC, NERC, and applicable Registered Entities. Issue and track security recommendation to protect the Bulk Power System. Share information learned in Situation Awareness with the Events Analysis program to develop relevant lessons learned.
- **Effective Financial Controls** — Continue to provide rigorous cost controls and efficient management of resources to remain an efficient provider of ERO delegated functions.

Long Term Business Planning

NERC and the Regional Entities continue to work together to improve the overall ERO business planning and budgeting process, including long-term resource and financial planning. The 2015 Business Plan and Budget process builds upon the improvements made over the past several years including face-to-face meetings, conference calls and exchanges of documentation among senior management and staff of NERC and Regional Entities regarding budget assumptions, resource requirements, and opportunities to improve operational efficiency and effectiveness.

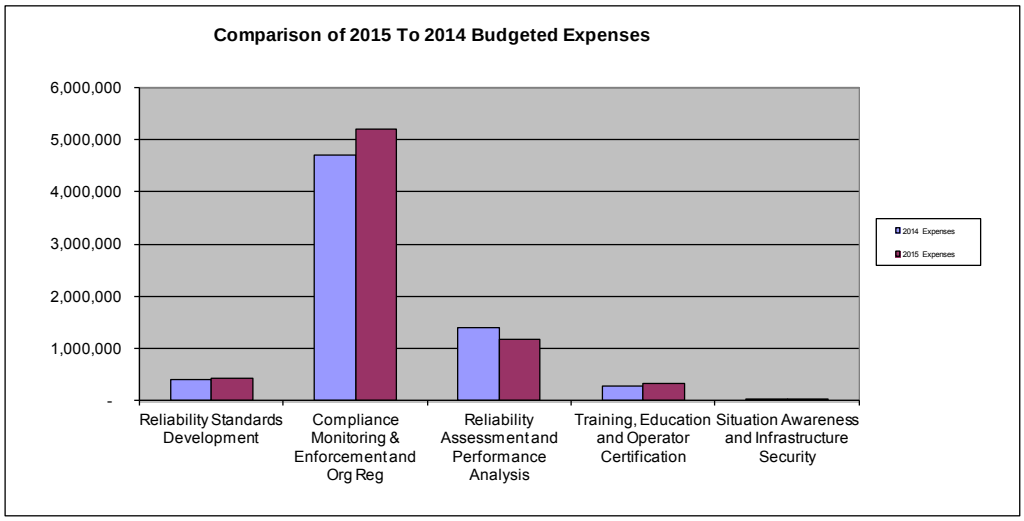
Throughout 2013 and into early 2014, NERC and the Regional Entities worked to develop a common operating model with defined roles and responsibilities that align with business planning goals, objectives, metrics and assumptions for the ERO Enterprise. As part of updating the ERO Strategic Plan, NERC and the Regional Entities consolidated five goals within the existing focus areas of standards; compliance, registration and certification; risks to reliability; and coordination and collaboration. A number of objectives and deliverables expected of the ERO Enterprise were identified. NERC and the Regional Entities added four overarching performance metrics to assess the overall effectiveness of the ERO Enterprise in addressing risk to the Bulk Power System and improving reliability. With the ERO Strategic Plan, the developed performance metrics, and the set of common assumptions, the 2015 Business Plan and Budgets of NERC and the Regional Entities will support and complement each other. The Shared Business Plan and Budget Assumptions (Exhibit A of the 2015 NERC Business Plan and Budget) incorporate assumptions affecting resource demands through the 2017 planning horizon.

NERC and the Regional Entities continue to work together to develop, strengthen and improve an integrated long term ERO business plan and budget that leverages and builds on the combined strengths and resources of NERC and the Regional Entities to improve the overall effectiveness and efficiency of ERO operations and improve the reliability of the BES of North America.

Detailed Business Plans and Budgets by Program

Details of the planning, operation, review, and adjustment for each program area are included in Section A. The corresponding budget details are shown in Section B. Below is an overall summary of the changes by program area.

Funding by Program	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Reliability Standards Development	409,591	409,592	423,143	13,552	3.3%
Compliance Monitoring & Enforcement and Org Reg	4,702,351	4,702,351	5,211,874	509,523	10.8%
Reliability Assessment and Performance Analysis	1,391,299	1,391,299	1,182,409	(208,890)	-15.0%
Training, Education and Operator Certification	272,310	297,679	321,525	49,215	18.1%
Situation Awareness and Infrastructure Security	19,380	19,380	23,281	3,901	20.1%
Total Funding All Sources	6,794,932	6,820,302	7,162,233	367,301	5.4%



This graphical representation does not include an allocation of working capital requirements among the Program Areas.

Total FTE's by Program Area	Budget 2014	Projection 2014	Direct FTEs 2015 Budget	Shared FTEs[1] 2015 Budget	Total FTEs 2015 Budget	Change from 2014 Budget
STATUTORY						
Operational Programs						
Reliability Standards Development	1.74	1.33	1.71		1.71	-0.03
Compliance Monitoring & Enforcement and Org Reg	19.26	18.25	19.77		19.77	0.51
Reliability Assessment and Performance Analysis	5.29	4.26		4.40	4.40	-0.89
Training, Education and Operator Certification	0.67	0.50		0.90	0.90	0.23
Situation Awareness and Infrastructure Security	0.08	0.06		0.09	0.09	0.01
Total FTEs Operational Programs	**27.04**	**24.40**	**21.48**	**5.39**	**26.87**	**-0.17**
Administrative Programs						
General & Administrative	3.36	3.57		4.04	4.04	0.68
Total FTEs Administrative Programs	**3.36**	**3.57**	**0.00**	**4.04**	**4.04**	**0.68**
Total FTEs	**30.40**	**27.97**	**21.48**	**9.43**	**30.91**	**0.51**

[1]A shared FTE is defined by NERC as an employee who performs both Statutory and Non-Statutory functions.

2014 Statutory Budget and Projection and 2015 Budget Comparisons

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital
2014 Budget & Projection, and 2015 Budget

STATUTORY

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 5,488,057	$ 5,488,058	$ 0	6,237,838	$ 749,781
Penalty Sanctions	343,000	343,000	-	153,000	(190,000)
Total ERO Funding	**$ 5,831,057**	**$ 5,831,058**	**$ 0**	**$ 6,390,838**	**$ 559,781**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	24,000	24,000	-	24,000	-
Workshops	90,000	115,369	25,369	90,000	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 5,945,057**	**$ 5,970,427**	**$ 25,369**	**$ 6,504,838**	**$ 559,781**
Expenses					
Personnel Expenses					
Salaries	$ 3,806,631	3,630,346	$ (176,285)	$ 4,082,307	$ 275,676
Payroll Taxes	239,599	231,599	(8,000)	253,874	14,275
Benefits	657,255	608,521	(48,734)	579,483	(77,772)
Retirement Costs	602,881	594,403	(8,478)	666,669	63,788
Total Personnel Expenses	**$ 5,306,366**	**$ 5,064,869**	**$ (241,497)**	**$ 5,582,333**	**$ 275,967**
Meeting Expenses					
Meetings	$ 80,930	$ 48,138	$ (32,792)	$ 69,292	$ (11,638)
Travel	167,209	137,943	(29,266)	191,753	24,544
Conference Calls	18,771	14,732	(4,039)	9,482	(9,289)
Total Meeting Expenses	**$ 266,910**	**$ 200,813**	**$ (66,097)**	**$ 270,527**	**$ 3,617**
Operating Expenses					
Consultants & Contracts	$ 348,768	$ 416,262	$ 67,494	$ 393,718	$ 44,950
Office Rent	555,089	554,412	(677)	547,586	(7,503)
Office Costs	118,343	122,974	4,631	132,069	13,726
Professional Services	116,642	41,315	(75,327)	51,324	(65,318)
Miscellaneous	-	-	-	-	-
Depreciation	110,490	157,036	46,546	202,287	91,797
Total Operating Expenses	**$ 1,249,332**	**$ 1,291,999**	**$ 42,667**	**$ 1,326,984**	**$ 77,652**
Total Direct Expenses	**$ 6,822,608**	**$ 6,557,681**	**$ (264,927)**	**$ 7,179,844**	**$ 357,236**
Indirect Expenses	**$ (1,643)**	**$ -**	**$ 1,643**	**$ 0**	**$ 1,643**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 6,820,965**	**$ 6,557,681**	**$ (263,284)**	**$ 7,179,844**	**$ 358,879**
Change in Assets	**$ (875,908)**	**$ (587,254)**	**$ 288,653**	**$ (675,006)**	**$ 200,902**
Fixed Assets					
Depreciation	$ (110,490)	$ (157,036)	$ (46,546)	$ (202,287)	$ (91,797)
Total Fixed Asset Purchases	82,814	129,422	46,608	184,676	101,862
Change in Fixed Assets	**27,676**	**27,614**	**(62)**	**17,611**	**(10,065)**
TOTAL BUDGET	$ 6,793,289	$ 6,530,067	$ (263,222)	$ 7,162,233	$ 368,944
TOTAL CHANGE IN WORKING CAPITAL	**$ (848,232)**	**$ (559,640)**	**$ 288,591**	**$ (657,395)**	**$ 190,837**
FTEs	30.40	27.97	(2.43)	30.91	0.51

Section A – Statutory Programs
2015 Business Plan and Budget

Reliability Standards Development Program

Reliability Standards Development Program (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	1.74	1.71	(0.03)
Direct Expenses	$ 369,582	$ 370,389	$ 807
Indirect Expenses	$ 40,021	$ 49,808	$ 9,787
Inc(Dec) in Fixed Assets	$ (12)	$ 2,946	$ 2,958
Total Funding Requirement	$ 409,591	$ 423,143	$ 13,552

Program Scope and Functional Description

The FRCC may develop, through the FRCC Regional Reliability Standards Development Process, separate Regional Reliability Standards that are specific to the FRCC Region and go beyond, add detail to, or implement NERC Reliability Standards. FRCC Regional Reliability Standards will not be inconsistent with or less stringent than NERC Reliability Standards.

The FRCC Regional Reliability Standards Development Process is an open, balanced and fair process that ensures all interested and affected parties have an opportunity to participate in the development of FRCC Regional Reliability Standards for the FRCC Region.

While the FRCC may develop separate Regional Reliability Standards, the preference is to support the development of continent wide reliability standards. The FRCC staff follows and participates in NERC's Standards Development Process. This includes FRCC standards staff participation in the NERC Standards Committee, the NERC Standards Committee Process Subcommittee, and NERC standards drafting teams as appropriate. In addition, the FRCC supports and encourages stakeholder awareness and participation in the NERC standards development process through educational outreach efforts at workshops, webinars and committee meetings.

2015 Key Assumptions

The key assumptions included in the Shared Business Plan and Budget Assumptions, Exhibit A, affecting the Reliability Standards Program include:

1. NERC will continue to focus on reaching a steady state, and improving quality and content of Reliability Standards. This will require the allocation of resources from NERC and the Regional Entities. The implementation of a cost effectiveness assessment of proposed standards and other reform activities are expected to require additional resources however the impacts are not fully known at this time.

2. The number of projects contained in NERC's Reliability Standards Development Plan is expected to increase over the planning period reflecting the transformation of standards to

a steady-state. However, the scope of these projects is expected to narrow as regulatory obligations in the form of directives and five-year reviews, Paragraph 81, and other recommendations are addressed.

3. The focus on improving the quality and content of standards will likely increase the demand on NERC, the Regional Entities and stakeholders to review and comment on proposed revisions to standards, support regulatory filings and support successful implementation of new standards as they become effective.

4. The number of interpretation and guidance requests is expected to remain low, reflecting the initiative to reach steady state and implementation of the Reliability Assurance Initiative (RAI).

5. NERC and the Regional Entities must provide sufficient resources to develop or modify the RSAWs by the time a Standard is balloted which is required to support the Reliability Standards Development Plan.

6. Activity associated with FRCC Regional Reliability Standards development is expected to remain low. FRCC will continue to keep several regional standards development projects on hold while NERC development, on standards addressing the same reliability issues, proceeds to a conclusion.

7. NERC and the Regional Entities will continue to provide communication and outreach opportunities, project level communications and will continue education and training for new or revised standards.

2015 Goals and Key Deliverables

The Standards Program objectives for 2015 are outlined below:

- Continue to follow and participate in NERC's Standards Development Process. This includes FRCC standards staff participation in the NERC Standards Committee, the NERC Standards Committee Process Subcommittee and on NERC standards drafting teams as appropriate.
- Continue to encourage stakeholder awareness and participation in the NERC standards development process.
- Continue to monitor the need for development of Regional Reliability Standards that are required by NERC Reliability Standards or are needed for reliability within the FRCC region.
- Assist the FRCC members and registered entities in following and understanding NERC standards development activities by increasing education and outreach programs to include:
    - Development and presentation at Standards Workshops, Webinars and committee meetings to address continent-wide and regional reliability issues.
    - Develop and deliver project level communications, education and training for new or revised reliability standards.
    - Review, analyze and identify potential Regional concerns associated with NERC Reliability Standards under development.

- Establish a stronger relationship with the FRCC Regional Entity Committee to fully vet and identify any concerns and assist in articulating the concern to standard drafting teams as appropriate.

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – The slight decrease in the number of FTEs is due to the expectation of more time being spent in Reliability Assessment program implementing the NERC BES Definition and the BES Definition Exception Process and the expectation of more time being spent in review of Registered Entity registration. The increase in personnel expenses is due to budgeted annual merit increases partially offset by a reduction in Medical Benefit expense.
- **Meeting Expenses** - Less travel is expected in 2015 with the BES Standards Writing Project being complete.
- **Operating Expenses** – The decrease in Operating Expenses is primarily the anticipated decrease in legal fees partially offset by increased contract costs included in Contracts, Consultants and Software for a security improvement initiative.
- **Indirect Expenses -** The increase in Indirect Expense is the result of a succession plan for expected future retirements.
- **Fixed Assets –** The increase in Fixed Assets is due to increased physical and cyber security measures and planned replacement of old computer equipment.

Reliability Standards Development Program

Funding sources and related expenses for the reliability standards section of the 2015 business plan are shown in the table below.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital
2014 Budget & Projection, and 2015 Budget
Reliability Standards Development

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 387,520	$ 387,520	$ 0	$ 413,407	$ 25,887
Penalty Sanctions	$ 22,072	$ 22,072		9,737	(12,335)
Total ERO Funding	**$ 409,591**	**$ 409,592**	**$ 0**	**$ 423,143**	**$ 13,552**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 409,591**	**$ 409,592**	**$ 0**	**$ 423,143**	**$ 13,552**
Expenses					
Personnel Expenses					
Salaries	$ 217,880	$ 173,035	$ (44,845)	$ 225,465	$ 7,585
Payroll Taxes	13,714	11,039	(2,675)	14,021	307
Benefits	33,809	23,651	(10,158)	32,602	(1,207)
Retirement Costs	34,595	28,420	(6,175)	36,074	1,479
Total Personnel Expenses	**$ 299,998**	**$ 236,145**	**$ (63,853)**	**$ 308,162**	**$ 8,164**
Meeting Expenses					
Meetings	$ 2,080	$ 969	$ (1,111)	$ 2,606	$ 526
Travel	24,913	16,324	(8,589)	17,469	(7,444)
Conference Calls	174	456	282	203	29
Total Meeting Expenses	**$ 27,167**	**$ 17,749**	**$ (9,418)**	**$ 20,278**	**$ (6,889)**
Operating Expenses					
Consultants & Contracts	$ 4,529	$ 5,222	$ 693	$ 7,381	$ 2,852
Office Rent	23,230	19,312	(3,918)	21,993	(1,237)
Office Costs	6,324	5,968	(356)	7,681	1,357
Professional Services	7,482	2,257	(5,225)	3,261	(4,221)
Miscellaneous	-	-	-	-	-
Depreciation	852	1,073	221	1,633	781
Total Operating Expenses	**$ 42,417**	**$ 33,832**	**$ (8,585)**	**$ 41,949**	**$ (468)**
Total Direct Expenses	**$ 369,582**	**$ 287,726**	**$ (81,856)**	**$ 370,389**	**$ 807**
Indirect Expenses	**$ 40,021**	**$ 37,186**	**$ (2,835)**	**$ 49,808**	**$ 9,787**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 409,603**	**$ 324,912**	**$ (84,691)**	**$ 420,197**	**$ 10,594**
Change in Assets	**$ (12)**	**$ 84,680**	**$ 84,692**	**$ 2,946**	**$ 2,958**
Fixed Assets					
Depreciation	$ (852)	$ (1,073)	$ (221)	$ (1,633)	$ (781)
Total Fixed Asset Purchases	840	371	(469)	4,579	3,739
Change in Fixed Assets	**$ 12**	**$ 702**	**$ 690**	**$ (2,946)**	**$ (2,958)**
TOTAL BUDGET	$ 409,591	$ 324,210	$ (85,381)	$ 423,143	$ 13,552
TOTAL CHANGE IN WORKING CAPITAL	**$ -**	**$ 85,382**	**$ 85,382**	**$ -**	**$ -**
FTEs	1.74	1.33	(0.41)	1.71	(0.03)

Compliance Monitoring and Enforcement Program and Organization Registration and Certification Program

Compliance Monitoring and Enforcement and Organization Registration and Certification Program (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	19.26	19.77	0.51
Direct Expenses	$ 4,281,909	$ 4,658,890	$ 376,981
Indirect Expenses	$ 442,994	$ 575,856	$ 132,862
Inc(Dec) in Fixed Assets	$ (22,552)	$ (22,872)	$ (320)
Total Funding Requirement	$ 4,702,351	$ 5,211,874	$ 509,523

Program Scope and Functional Description

Monitoring, evaluating, investigating and enforcing compliance with Reliability Standards by owners, operators and users of the BES, as well as the development and adoption of the reliability standards themselves, are at the core of FRCC's mission. Reliable operation of the BES is in the public interest, because it will benefit all owners, operators and users of the BES, and, ultimately, all users and consumers of electric power in the FRCC Region.

Compliance and Enforcement activities are carried out by the FRCC compliance staff and are independent of all users, owners and operators of the BES. Compliance activities are governed by the delegation agreement between the North American Electric Reliability Corporation (NERC) and the FRCC. Through a risk-based program of monitoring, evaluating, enforcing, and if necessary, the imposition of penalties and sanctions for noncompliance with Reliability Standards, FRCC will strive to increase the level of reliable operation of the BES in the FRCC Region.

The NERC Compliance Monitoring and Enforcement Program (CMEP) is the program used by the FRCC to monitor, assess, and enforce compliance with Reliability Standards within the FRCC Region. The FRCC compliance staff works with the compliance staff of the other Regional Entities and with NERC to achieve as much consistency and transparency as possible in the implementation of the CMEP. The development and implementation of the Reliability Assurance Initiative (RAI) throughout 2014 and into early 2015 provides the foundation and guidance for NERC and the Regional Entities in moving to a risk-based environment aimed at focusing on those risks that are most important to the reliability of the BES.

2015 Highlights Compliance Monitoring and Enforcement Processes

In 2015 the FRCC will monitor, assess and enforce compliance with Reliability Standards using seven (7) monitoring processes (Compliance Audits, Self-Certifications, Spot Checking, Compliance Investigations, Self-Reporting, Periodic Data Submittals, and Complaints) to collect information in order to make assessments of compliance to Reliability Standards. However as risk based monitoring activities increase, strong consideration will be given by NERC and the

Regions to modify the current three (3) and six (6) year audit cycles for registered entities. The rigor, scope, depth and recurrence of audits and spot checks will be assessed by the reliability risk and not a predetermined schedule.

Registration and Certification

The FRCC has registered the organizations responsible for complying with Reliability Standards in accordance with Section 500 of the NERC Rules of Procedure. Currently there are 69 Registered Entities with a total of 244 registered functions. Maintaining a complete and accurate registration database will be an ongoing activity. The FRCC will develop, maintain and provide to NERC accurate information on entity registration within the FRCC Region with updates as changes occur. NERC and the Regional Entities began a review of the organization registration process in 2014 which may result in changes to the registration process that could begin in 2015. While expectations of increased activity are associated with the implementation of the BES Exception Process mid-2014, there is some uncertainty in the amount of activity associated with registration and certification of registered entities. The FRCC may consider the reallocation of existing resources should the need arise for additional support in this area.

Enforcement and Mitigation

Enforcement actions taken by FRCC may include the imposition of remedial action directives, sanctions and penalties which are applied per the NERC Rules of Procedure. Mitigation of violations of the approved Reliability Standards remains central to the FRCC's reliability focus. Registered Entities found in violation of a Reliability Standard will be required to fully mitigate the violation regardless of any enforcement actions taken. The year 2014 continued to bring advances in enforcement discretion of violations with minimal impact to the reliability of the BES. This additional discretion will continue in 2015 through the development and implementation of the NERC Reliability Assurance Initiative allowing for more focus being placed on those violations that pose a more serious risk to the reliability of the BES.

2015 Key Assumptions

- Audits are expected to continue under the current three and six year schedules until NERC and the Regional Entities transition to a more risk-based approach to compliance monitoring as developed in the Reliability Assurance Initiative (RAI).
- Reliability risk profiles for all Registered Entities will be developed and audit scopes will be tailored to the risk profiles which may increase the depth and complexity of some audits and decrease the depth and complexity of others. The consistent approach to audit scope methodology being developed as part of the RAI in 2014 is expected to be used in early 2015.
- Integration of the assessment of Registered Entity internal controls programs as part of the compliance monitoring program will allow NERC and the Regional Entities to further prioritize risk based compliance monitoring activities. Greater emphasis on internal controls provides positive incentives for industry to demonstrate effective management of compliance programs that are focused on reliability, as well as place downward pressure on compliance resource requirements for industry, NERC and the Regional Entities.
- The use of spot checks and self-certifications is expected to increase as risk-based monitoring is implemented, but that should have little effect on FRCC's overall resource requirements. The implementation of the Reliability Assurance Initiative and the

expansion of the Find Fix and Track (FFT) process will require resources to complete the design and to begin implementing RAI for both compliance and enforcement.

- The approval of CIP V5 is anticipated to significantly increase the compliance monitoring activities. The effective date for compliance with the CIP Version 5 standards will be April 1, 2016 for High and Medium impact assets and April 1, 2017 for Low impact assets. The transition between V3 to V5 will be a mission critical activity for the ERO Enterprise in 2015. FRCC plans to support the ongoing CIP v5 transition plans and anticipates an expansion in the number of Registered Entities that require guidance during 2015. Additional training requirements will be necessary to support the transition and will affect the annual training commitments. For most CIP activities, the resource demands are expected to increase throughout the planning period.
- The number of non-CIP violations is expected to decrease as most registered entities have been audited and the standards and RSAWs have matured.
- The Technical Feasibility Exception (TFE) program will continue however the processing per the revised Appendix 4D, of the NERC Rules of Procedure, is expected to drive a less onerous process for TFE reporting and reviewing.
- Applications planned to be centralized, such as a common audit management tool, at NERC to improve consistency and efficiency, will require Regional Entity support and resources for development and implementation. A significant multiyear investment will be required to develop and implement the system which will be funded by NERC.
- NERC and the Regional Entities are expected to utilize consistent audit practices and focus on higher target reliability risks to increase efficiency and mitigate overall compliance costs.
- NERC and the Regional Entities will provide sufficient resources to develop or modify the RSAWs by the time a Standard is balloted which is required to support the Reliability Standards Development Plan.
- NERC and the Regional Entities must plan to support the training requirements necessary to meet the criteria set forth by the ERO Auditor Manual and Handbook and the Compliance Auditor Capabilities and Competency Guide. Regional Entities will be expected to provide training documents and other related compliance guidance to compliance staff, review Auditor job descriptions and properly reflect the guidance provided in the Compliance Auditor Capabilities and Competency Guide, perform a gap analysis to identify both individual training needs and organizational compliance resource needs, provide an assessment process to evaluate audit team competencies and capability needs, and put a training program in place that addresses initial and continuing training for capability and competency development.
- NERC will continue to budget and incur the cost of a unified learning management system (LMS) for the regional audit staff and work with the Regional Entities to consolidate training resources and promote better coordination, planning, delivery and management of training efforts across the ERO.
- Additional resources will be required, and increases to NERC and Regional Entity training budgets are expected to support certain training initiatives of the RAI. Regional Entities are expected to allocate resources to meet the training requirements for the compliance and enforcement staff that are associated with the implementation of the RAI.

- Maintaining budgeted qualified compliance and enforcement staff will continue to be a challenge driven by a limited pool of qualified people and an aging work force. Investments in training less experienced personnel are likely to increase.

2015 Goals and Key Deliverables

The Compliance Monitoring and Enforcement Program objectives for 2015 are outlined below:

- Continue to assess and update entity registration and certification. The FRCC will support the implementation of the changes resulting from the registration review that began in 2014.
- Support the development and implementation of NERC's Reliability Assurance Initiative, including providing the necessary training for compliance and enforcement staff. Enforce compliance with mandatory reliability standards in accordance with the CMEP and ROP while improving consistency, quality, timeliness and utilizing more enforcement discretion for those violations that have minimal impact to the reliability of the BES.
- Develop and maintain reliability risk profiles of all registered entities in the FRCC Region for use in the continued transition to a more risk-based compliance monitoring.
- Implement the ERO Auditor Handbook and Manual and continue to work with NERC Compliance staff and other Regional Entity Compliance staff to modify compliance procedures to increase consistency in the determination of violations and penalties.
- Implement the common methodology developed in 2014 to assess risk and determine scope of monitoring activities. Conduct periodic audits, spot checks, self-certifications, and compliance investigations as required by the NERC Compliance Monitoring and Enforcement Program.
- Continue to promote the self-identification of non-compliance by Registered Entities and utilize increased discretion as appropriate. Ensure timely and thorough mitigation of all violations of mandatory reliability standards.
- Promote a culture of compliance excellence through education, transparency, information sharing and incentives.

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – The increase in FTEs and personnel expense can be primarily attributed to expected increased effort in the Organization Registration Program and the effect of having an addition to staff budgeted for May of 2014 for a full year in 2015. The increase in personnel expense is also due to a budgeted annual merit increase. These increases are partially offset by reduced expected benefit expenses based from medical expenses being less than anticipated in the 2014 budget.
- **Meeting Expenses** – Increased travel is expected in 2015 to meet expectations of NERC for meetings to ensure consistent implementation of the Reliability Assurance Initiative (RAI), RAI associated updates to the Auditor Handbook, and to support ERO IT development projects.
- **Operating Expenses** – Anticipated increased cost of the Compliance Software to implement RAI and NERC business rules, increased contract costs included in Contracts,

Consultants and Software for a security improvement initiative and the increased depreciation effect of the additions of same in 2014 and 2015 partially offset by an anticipated decrease in legal fees.

- **Indirect Expenses -** The increase in Indirect Expense is the result of a succession plan for expected future retirements.
- **Fixed Assets –** The increase in Fixed Assets is due to increased cost in enhancements of the Compliance Software, increased physical and cyber security measures and planned replacement of old computer equipment.

Compliance Monitoring and Enforcement Program and Organization Registration and Certification Program

Funding sources and related expenses for the compliance enforcement and organization registration and certification section of the 2015 business plan are shown in the table below.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital 2014 Budget & Projection, and 2015 Budget

Compliance Monitoring & Enforcement and Organization Registration & Certification

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 4,458,040	$ 4,458,040	$ -	$ 5,099,302	$ 641,262
Penalty Sanctions	244,311	244,311	-	112,572	(131,739)
Total ERO Funding	**$ 4,702,351**	**$ 4,702,351**	**$ -**	**$ 5,211,874**	**$ 509,523**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Federal Grants	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 4,702,351**	**$ 4,702,351**	**$ -**	**$ 5,211,874**	**$ 509,523**
Expenses					
Personnel Expenses					
Salaries	$ 2,411,701	$ 2,368,964	$ (42,737)	$ 2,611,174	$ 199,473
Payroll Taxes	151,798	151,129	(669)	162,386	10,588
Benefits	452,812	421,727	(31,085)	385,976	(66,836)
Retirement Costs	382,958	389,089	6,131	431,288	48,330
Total Personnel Expenses	**$ 3,399,269**	**$ 3,330,909**	**$ (68,360)**	**$ 3,590,824**	**$ 191,555**
Meeting Expenses					
Meetings	$ 4,915	$ 7,412	$ 2,497	$ 12,729	$ 7,814
Travel	92,966	81,240	(11,726)	122,194	29,228
Conference Calls	4,565	8,805	4,240	4,390	(175)
Total Meeting Expenses	**$ 102,446**	**$ 97,457**	**$ (4,989)**	**$ 139,313**	**$ 36,867**
Operating Expenses					
Consultants & Contracts	$ 119,235	$ 225,494	$ 106,259	$ 214,984	$ 95,749
Office Rent	406,366	413,633	7,267	404,082	(2,284)
Office Costs	69,926	74,111	4,185	80,150	10,224
Professional Services	83,069	30,900	(52,169)	37,762	(45,307)
Miscellaneous	-	-	-	-	-
Depreciation	101,598	148,536	46,938	191,775	90,177
Total Operating Expenses	**$ 780,194**	**$ 892,674**	**$ 112,480**	**$ 928,753**	**$ 148,559**
Total Direct Expenses	**$ 4,281,909**	**$ 4,321,040**	**$ 39,131**	**$ 4,658,890**	**$ 376,981**
Indirect Expenses	**$ 442,994**	**$ 509,116**	**$ 66,122**	**$ 575,856**	**$ 132,862**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 4,724,903**	**$ 4,830,156**	**$ 105,253**	**$ 5,234,746**	**$ 509,843**
Change in Assets	**$ (22,552)**	**$ (127,805)**	**$ (105,253)**	**$ (22,872)**	**$ (320)**
Fixed Assets					
Depreciation	$ (101,598)	$ (148,536)	$ (46,938)	$ (191,775)	$ (90,177)
Total Fixed Asset Purchases	79,046	127,708	48,662	168,903	89,857
Change in Fixed Assets	**$ 22,552**	**$ 20,828**	**$ (1,724)**	**$ 22,872**	**$ 320**
TOTAL BUDGET	$ 4,702,351	$ 4,809,328	$ 106,977	$ 5,211,874	$ 509,523
TOTAL CHANGE IN WORKING CAPITAL	**$ -**	**$ (106,977)**	**$ (106,977)**	**$ -**	**$ -**
FTEs	19.26	18.25	(1.01)	19.77	0.51

Reliability Assessment and Performance Analysis Program

Reliability Assessment and Performance Analysis Program (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	5.29	4.39	(0.90)
Direct Expenses	$ 1,270,439	$ 1,049,392	$ (221,047)
Indirect Expenses	$ 121,674	$ 127,871	$ 6,197
Inc(Dec) in Fixed Assets	$ (814)	$ 5,146	$ 5,960
Total Funding Requirement	$ 1,391,299	$ 1,182,409	$ (208,890)

Program Scope and Functional Description

The FRCC will assess the reliability of the BES in the FRCC region and will continue to ensure that the planned system is robust, reliable and stable. The FRCC will participate in Event Analysis Teams to analyze any disturbances that may occur within the FRCC region.

The FRCC performs transmission reliability studies in order to provide an assessment to NERC for its periodic NERC Reliability Assessments. These studies evaluate regional and inter-regional facilities. The FRCC prepares a minimum of three reliability assessments each year and a probabilistic assessment every other year in support of NERC Reliability Assessments:

- A 20 year long-term reliability assessment report
- A summer assessment report
- A winter assessment report
- A probabilistic long-term reliability assessment (biennial)

These reports evaluate electricity demand, the adequacy of supply and its deliverability, fuel reliability and the adequacy of the transmission system within the FRCC. The FRCC will prepare special reliability assessment reports as conditions warrant.

The FRCC Reliability Assessment and Performance Analysis Program (RA) will support NERC's efforts to move toward and implement an outcome based approach in Reliability Assessments to achieve measureable improvements in the BES reliability. Risks will be identified and prioritized based on reliability impacts, cost/practicality of assessments, projected resources, and emerging issues. The FRCC will support NERC's efforts for collection and analysis of data, as well as support any of NERC's special reliability assessments and the efforts related to the collection of data via the Generation Availability Data System (GADS), Transmission Availability Data System (TADS) and Demand Response Availability Data System (DADS). In addition, the FRCC will work with NERC to gather data and/or complete

analysis in support of U.S. Federal initiatives, including high impact/low frequency events such as geomagnetic disturbances, system frequency response analysis, climate change and other environmental regulations.

The FRCC will support a new ERO initiative focused on identifying essential reliability services and providing the industry with technical papers and guidelines as appropriate.

The FRCC actively participates in the Eastern Interconnection Reliability Assessment Group (ERAG) which is responsible for the Eastern Interconnection transmission models and inter-regional studies. The FRCC will support NERC's and ERAG's efforts to improve the data quality of the Eastern Interconnection (EI) transmission models and validate the performance of these models compared to system events. The FRCC is an active participant on the NERC Reliability Assessment Subcommittee which is responsible for performing an independent review of reliability assessments.

The FRCC Events Analysis Program will analyze or support the analysis of significant events and system performance that impact the BES within the FRCC Region. The FRCC will facilitate consistent identification of sequence, root cause and remediation to identify reliability risks and trends, and lessons learned. FRCC's analysis will result in the identification of any gaps in standards, compliance effectiveness, registration and risk controls effectiveness. The FRCC will provide lessons learned and recommendations from events and identified risks.

The FRCC will support NERC to improve event causal analysis, communication of lessons learned, tracking of recommendations, and implementation of best practices. The FRCC will support NERC to continue to improve consistency, quality, timeliness and cost effectiveness of NERC and Regional Entity data collection, analysis systems and capabilities through process improvements and more effective coordination and collaboration.

2015 Key Assumptions

- NERC will continue to incrementally improve definitions, refine data reporting requirements for Registered Entities and review adequate level of reliability related metrics used in reliability assessments.
- NERC and Regional Entities will be requested to gather data or perform analysis in support of federal initiatives related to critical infrastructure protection including high impact/low frequency, climate change, environmental regulations, and/or renewable energy initiatives. Generation Availability Data System (GADS), Spare Equipment Database (SED) and Demand Response Data System (DADS) collection will continue to be mandatory in 2015.
- NERC and the Regional Entities are expected to provide independent reviews of assessments to assure a high level of technical rigor.
- Implementation of the BES exception process will require the re-allocation of resources from several NERC and Regional Entity departments. The resources will be expected to manage the process execution, technical validation of the definition and exception requests, self-determined notification submittals and requests for registration and certification review. The resource impacts are not fully known at this time, but are expected to be driven by the number and complexity of exception requests, self-determined notification submittals and registration requests received.

- NERC has established an Essential Reliability Services Task Force that may have an impact on resource requirements in order to support the work of this task force which is expected to have weekly conference calls and two or three in person meetings.
- NERC will sustain a Reliability Assessment and Performance Analysis team with representatives from the Regional Entities to:
    - Develop and implement improved enterprise-based data collection and analysis systems and capabilities
    - Support the integration of RAPA information systems for modeling and data requirements and achieve timelines for delivering high quality reports
    - Develop, verify and validate quality reliability assessment and analyses model and data quality characteristics
    - Address impacts of new technologies, changing resource or demand resource composition, and environmental related regulations or legislation
    - Support the compilation of long-term sustainable Eastern Interconnection models
    - Provide technical resources and expertise to perform analyses as needed for standards development, compliance and enforcement activities
    - Support quality analysis and overall assessment of the geomagnetic disturbance (GMD) vulnerability, planning guides and planning standards.
- The number of "qualified system events" as defined in the NERC Events Analysis Process, is expected to remain steady (approximately 10 per month across North America). Greater collaboration with the region and the registered entity is leading to more detailed analysis and supporting the identification of reliability issues and challenges.

2015 Goals and Key Deliverables

The Reliability Assessment and Performance Analysis Objectives for 2015 are outlined below:

- Perform a reliability assessment of the FRCC Region to determine if the planned resources and proposed transmission expansion plans will meet the needs of the projected demand throughout the planning horizon.
- Support NERC in preparing its reliability assessment reports.
- Support the implementation of the BES exception process. This will include providing a technical review of exception requests that are submitted by the registered entities.
- Support the work of the newly created Essential Reliability Services Task Force by assigning an FRCC Staff person to support this NERC initiative.
- Evaluate, track and assess severity/risk and reliability metrics and risk indices – including providing support to update reliability metrics and risk indices.
- Support data gathering and reporting efforts for the Generating Availability Data System (GADS), the Transmission Availability Data System (TADS), Spare Equipment Database (SED) and Demand Response Availability Data System (DADS).

- Strengthen data collection and validation processes by designing, creating, testing and implementing data checking systems to accommodate the increasing amount of data NERC collects for its long-term, seasonal, operational, scenarios and special reliability assessments along with the databases supporting reliability performance assessments.
- Review and/or analyze significant events that impact the FRCC BES and work with NERC to identify the root causes of events that may be precursors of potentially more serious events.
- Assess past reliability performance for potential lessons learned.
- Maintain relationships with NERC, regulatory and governmental organizations involved with BES reliability (e.g., Florida Public Service Commission (FPSC), Department of Energy (DOE), FERC, Energy Information Administration (EIA), etc.).
- Maintain a databank of power flow, short circuit and dynamic models to use in planning and evaluating future systems and current operating conditions.
- Work with ERAG Multi-Area Modeling Working Group (MMWG) to develop Eastern Interconnection steady-state and dynamics models and develop model validation processes.
- Conduct Loss of Load Probability and the Scenario Analysis studies as needed.

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – In 2014, the committee structure was streamlined to reduce the amount of time that staff spent preparing for meetings and participating in meetings. Previously, the FRCC conducted business associated with Reliability Assessments in both the Operating Committee and the Planning Committee. This approach resulted in staff members attending multiple meetings each month to cover the same topics. With the revised structure, all Regional Entity activities will be conducted in one forum; the new Regional Entity Committee and Compliance Forum (RECCF). In addition to consolidating the Regional Entity activities under the RECCF, it was also determined that the RECCF will not need to meet monthly, but will meet face-to-face six times in 2015. This new construct will allow FRCC staff to complete the Reliability Assessment deliverables much more efficiently and drives the decrease to FTEs and personnel expenses.
- **Meeting Expenses** – With the formation of the RECCF, there will be fewer meetings required to complete the RA deliverables decreasing Meeting Expenses.
- **Operating Expenses** –The decrease is due to an anticipated decrease in legal fees and a reduction in certain consultant expenses which have been consistently over-budgeted.
- **Indirect Expenses -** The increase in Indirect Expense is the result of a succession plan for expected future retirements.
- **Fixed Assets –** The increase in Fixed Assets is due to increased physical and cyber security measures and planned replacement of old computer equipment.

Reliability Assessment and Performance Analysis Program

Funding sources and related expenses for the reliability assessment and performance analysis section of the 2015 business plan are shown in the table below.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital 2014 Budget & Projection, and 2015 Budget

Reliability Assessment and Performance Analysis

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 1,300,196	$ 1,300,196	$ -	$ 1,133,412	$ (166,784)
Penalty Sanctions	67,103	67,103	-	24,997	(42,106)
Total ERO Funding	**$ 1,367,299**	**$ 1,367,299**	**$ -**	**$ 1,158,409**	**$ (208,890)**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	24,000	24,000	-	24,000	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 1,391,299**	**$ 1,391,299**	**$ -**	**$ 1,182,409**	**$ (208,890)**
Expenses					
Personnel Expenses					
Salaries	$ 662,404	$ 552,292	$ (110,112)	$ 580,711	$ (81,693)
Payroll Taxes	41,693	35,234	(6,459)	36,114	(5,579)
Benefits	99,378	84,437	(14,941)	82,646	(16,732)
Retirement Costs	105,185	90,711	(14,474)	92,914	(12,271)
Total Personnel Expenses	**$ 908,660**	**$ 762,674**	**$ (145,986)**	**$ 792,385**	**$ (116,275)**
Meeting Expenses					
Meetings	$ 6,674	$ 1,307	$ (5,367)	$ 1,612	$ (5,062)
Travel	43,265	34,637	(8,628)	47,375	4,110
Conference Calls	8,543	1,437	(7,106)	447	(8,096)
Total Meeting Expenses	**$ 58,482**	**$ 37,381**	**$ (21,101)**	**$ 49,434**	**$ (9,048)**
Operating Expenses					
Consultants & Contracts	$ 192,989	$ 130,637	$ (62,352)	$ 122,547	$ (70,442)
Office Rent	70,623	61,640	(8,983)	56,646	(13,977)
Office Costs	13,480	12,843	(637)	14,617	1,137
Professional Services	22,829	7,204	(15,625)	8,398	(14,431)
Miscellaneous	-	-	-	-	-
Depreciation	3,376	4,213	837	5,365	1,989
Total Operating Expenses	**$ 303,297**	**$ 216,537**	**$ (86,760)**	**$ 207,573**	**$ (95,724)**
Total Direct Expenses	**$ 1,270,439**	**$ 1,016,592**	**$ (253,847)**	**$ 1,049,392**	**$ (221,047)**
Indirect Expenses	**$ 121,674**	**$ 118,694**	**$ (2,980)**	**$ 127,871**	**$ 6,197**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 1,392,113**	**$ 1,135,286**	**$ (256,827)**	**$ 1,177,263**	**$ (214,850)**
Change in Assets	**$ (814)**	**$ 256,013**	**$ 256,827**	**$ 5,146**	**$ 5,960**
Fixed Assets					
Depreciation	$ (3,376)	$ (4,213)	$ (837)	$ (5,365)	(1,989)
Total Fixed Asset Purchases	2,562	1,186	(1,376)	10,511	7,949
Change in Fixed Assets	**$ 814**	**$ 3,027**	**$ 2,213**	**$ (5,146)**	**$ (5,960)**
TOTAL BUDGET	$ 1,391,299	$ 1,132,259	$ (259,040)	$ 1,182,409	$ (208,890)
TOTAL CHANGE IN WORKING CAPITAL	**$ -**	**$ 259,040**	**$ 259,040**	**$ -**	**$ -**
FTEs	5.29	4.26	(1.03)	4.40	(0.89)

Training, Education, and Operator Certification Program

Training, Education and Operator Certification Program (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	0.67	0.91	0.24
Direct Expenses	$ 257,163	$ 295,452	$ 38,289
Indirect Expenses	$ 15,410	$ 26,506	$ 11,096
Inc(Dec) in Fixed Assets	$ (263)	$ (433)	$ (170)
Total Funding Requirement	$ 272,310	$ 321,525	$ 49,215

Program Scope and Functional Description

The FRCC is a NERC-approved Continuing Education (CE) Provider. The FRCC System Operator Subcommittee (SOS) develops and delivers training in which FRCC grants NERC CE hours to those individuals who successfully complete a course. FRCC will utilize the NERC database to accommodate the recordkeeping requirements for the continuing education program. Maintaining the reliability of the BES requires informed and trained personnel. The FRCC supports training activities through its staff and its System Operator Subcommittee which reports to the FRCC Operating Committee.

The FRCC provides educational workshops and web based seminars to improve Registered Entity understanding of the FRCC CMEP, NERC Standards Development and CIP topics and trends. These outreach efforts are aimed at improving the effectiveness, understanding of and adherence to NERC reliability initiatives. The workshops also improve the working relationships between the FRCC Regional Entity program areas and the Registered Entities within the FRCC region.

System Operator Certification Program

The FRCC SOS identifies and manages annual training activities for the FRCC System Operators and provides information to FRCC members regarding the NERC training standards and any issues they may have related to system operators obtaining/retaining required NERC Certification.

The training and education program activities are carried out by FRCC's professional/technical staff and SOS members possessing the appropriate technical knowledge and competencies. In addition, vendors that specialize in System Operator training are also used. Providing the FRCC training and education programs helps to achieve a high level of knowledge and competence among the operating personnel in the performance of their reliability-related functions.

Compliance Workshops

Compliance workshops will be held in the spring and fall of 2015 consisting of three (3) sessions each. These workshops will be aimed at providing updates to the Registered Entities on

compliance procedures, instructions on changes to FRCC compliance website, lessons learned for previous violations and providing sufficient and appropriate evidence in a compliance audit. The entities will also be apprised of changes in rules and expectations of NERC and FERC with regard to the CMEP. The effect on compliance monitoring as a result of on-going changes in the NERC and Regional Reliability Standards will also be addressed.

In addition, there will be at least one (1) CIP Compliance Workshop that will address technical aspects of the CIP Reliability Standards, including, providing quality evidence, lessons learned and compliance processes specific to the monitoring and enforcement of the CIP standards. In addition, particular focus will be made on the transition from CIP V3 to CIP V5 standards.

In addition to the face to face venues, in 2015 FRCC compliance staff projects holding at least three (3) webinars (two sessions each) that will address specific topics that may be identified by registered entities or by emerging trends within the FRCC.

Standards Workshops

The FRCC Standards Department will be supporting and participating in various FRCC sponsored workshops (e.g., FRCC Compliance Workshops and FRCC SOS seminars) throughout 2015. The Standards Department contribution to the workshops will be designed to promote stakeholder awareness of Reliability Standards activities as well as education and training for new or revised Reliability Standards. In addition, the FRCC Standards Department plans to hold at least four (4) workshops or webinars that will educate stakeholders on the NERC Reliability Standards Development Procedure, and specific changes to existing reliability standards or specifics on new reliability standards. To help encourage stakeholder participation at the continent-wide level, the workshops will provide stakeholders with details of associated NERC Reliability Standards Development Projects, identifying key areas that may be of concern or interest to the stakeholders and identifying areas that are in need of industry support.

2015 Key Assumptions

- The Operating Personnel Certification program is expected to remain at steady state therefore no significant changes are expected in System Operator Certification CEH requirements through 2015.
- The System Operator Certification Program and Continuing Education Program will continue to be self-funded through a fee based structure for the exams and applications for approval of continuing education activities.
- The Regional Entities are expected to help determine training needs and anticipate areas of support for standards, compliance monitoring and enforcement and information technology (IT) for their staffs and stakeholders.

2015 Goals and Key Deliverables

The training, education and operator certification program objectives for 2015 are outlined below:

- Provide assistance to Regional Entity members in any issues they may have related to System Operator Certification.

- Conduct the annual system operator training seminars over a five (5) week period, with two (2) days each for the training. The training seminars involve from two (2) to four (4) FRCC staff members, as well as industry volunteers who participate as presenters. This activity is funded primarily through registration fees.
- Host FRCC Compliance Workshops and Webinars open to all FRCC Members and Registered Entities aimed at providing updates on compliance procedures, instructions on changes to compliance tools, changes associated with the implementation of the RAI and guidance on the providing of appropriate and sufficient evidence in a compliance audit.
- Host Reliability Standards Workshops and Webinars open to all FRCC Members and Registered Entities aimed at providing information concerning reliability standards under development, as well as the identification of technical concerns or issues that may impact the reliability of the FRCC BES.
- Conduct FRCC Reliability Standards Department presentations to support multiple training objectives (i.e., FRCC Compliance Workshops and FRCC SOS Seminars) to promote stakeholder awareness of continent wide and regional standards activities.
- Work with NERC and the other Regional Entities to achieve improvements in the coordination, content and manner of internal and external training programs.

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – The increase in FTEs and Personnel Expenses is due to more time planned to be spent on training and education of registered entities in elements pertaining to the Reliability Assurance Initiative and in expectation of the transition to CIP Version 5. The increase in personnel expense is also due to a budgeted annual merit increase.
- **Meeting Expenses** – The decrease in Meeting Expenses is due to the anticipation that the cost for the SOS meeting facility will be less than it has been in the past.
- **Operating Expenses** –The increase in Operating Expenses is due to the cost of a security improvement initiative offset by an anticipated decrease in legal fees.
- **Indirect Expenses -** The increase in Indirect Expense is the result of a succession plan for expected future retirements.

Training, Education, and Operator Certification Program

Funding sources and related expenses for the training, education, and operator certification section of the 2015 business plan are shown in the table below.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital
2014 Budget & Projection, and 2015 Budget
Training, Education and Operator Certification

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 173,812	$ 173,812	$ -	$ 226,344	$ 52,532
Penalty Sanctions	8,499	8,499	-	5,182	(3,317)
Total ERO Funding	**$ 182,310**	**$ 182,310**	**$ -**	**$ 231,525**	**$ 49,215**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	90,000	115,369	25,369	90,000	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 272,310**	**$ 297,679**	**$ 25,369**	**$ 321,525**	**$ 49,215**
Expenses					
Personnel Expenses					
Salaries	$ 83,896	$ 65,388	$ (18,508)	$ 119,243	$ 35,347
Payroll Taxes	5,281	4,171	(1,110)	7,416	2,135
Benefits	11,616	20,293	8,677	14,228	2,612
Retirement Costs	13,325	10,740	(2,585)	19,079	5,754
Total Personnel Expenses	**$ 114,118**	**$ 100,592**	**$ (13,526)**	**$ 159,966**	**$ 45,848**
Meeting Expenses					
Meetings	$ 67,248	$ 38,432	$ (28,816)	$ 52,311	$ (14,937)
Travel	5,996	5,674	(322)	4,616	(1,380)
Conference Calls	5,481	4,013	(1,468)	4,433	(1,048)
Total Meeting Expenses	**$ 78,725**	**$ 48,119**	**$ (30,606)**	**$ 61,360**	**$ (17,365)**
Operating Expenses					
Consultants & Contracts	$ 29,259	$ 51,473	$ 22,214	$ 37,104	$ 7,845
Office Rent	8,945	7,298	(1,647)	11,632	2,687
Office Costs	22,610	26,705	4,095	22,613	3
Professional Services	2,916	853	(2,063)	1,725	(1,191)
Miscellaneous	-	-	-	-	-
Depreciation	590	774	184	1,052	462
Total Operating Expenses	**$ 64,320**	**$ 87,103**	**$ 22,783**	**$ 74,126**	**$ 9,806**
Total Direct Expenses	**$ 257,163**	**$ 235,814**	**$ (21,349)**	**$ 295,452**	**$ 38,289**
Indirect Expenses	**$ 15,410**	**$ 14,055**	**$ (1,355)**	**$ 26,506**	**$ 11,096**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 272,573**	**$ 249,869**	**$ (22,704)**	**$ 321,958**	**$ 49,385**
Change in Assets	**$ (263)**	**$ 47,810**	**$ 48,073**	**$ (433)**	**$ (170)**
Fixed Assets					
Depreciation	$ (590)	$ (774)	$ (184)	$ (1,052)	$ (462)
Total Fixed Asset Purchases	327	140	(187)	619	292
Change in Fixed Assets	**$ 263**	**$ 634**	**$ 371**	**$ 433**	**$ 170**
TOTAL BUDGET	$ 272,310	$ 249,235	$ (23,075)	$ 321,525	$ 49,215
TOTAL CHANGE IN WORKING CAPITAL	**$ -**	**$ 48,444**	**$ 48,444**	**$ -**	**$ -**
FTEs	0.67	0.50	(0.17)	0.90	0.23

Situation Awareness and Infrastructure Security Program

Situation Awareness and Infrastructure Security Program (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	0.08	0.09	0.01
Direct Expenses	$ 19,932	$ 23,058	$ 3,126
Indirect Expenses	$ 1,840	$ 2,621	$ 781
Inc(Dec) in Fixed Assets	$ (2,392)	$ (2,398)	$ (6)
Total Funding Requirement	$ 19,380	$ 23,281	$ 3,901

Program Scope and Functional Description

The FRCC and the other Regional Entities support the ERO's situational awareness, cyber security preparedness and provide independent reliability information to policy makers and regulators. The Reliability Process for the FRCC Bulk Electric System documents the various reliability roles and functions that are coordinated, monitored and established by FRCC to provide situation awareness of the reliability of the FRCC BES. Two of the primary reliability goals of the FRCC are continuous improvement of the situation awareness of the operators within the FRCC and ensuring that adequate physical, operational and cyber security objectives are in place for the Regions' shared communications networks.

The FRCC supports NERC's situation awareness/event analysis coordination conference calls, the Situation Awareness for FERC, NERC and the Regions (SAFNR) Version 2 project and the FRCC satellite phone for situation awareness.

The NERC Rules of Procedure, Section 1000, requires that NERC monitor present conditions on the BES and provide leadership coordination, technical expertise and assistance to the industry in responding to events as necessary.

The Situation Awareness process will be used to support NERC and FERC's efforts for situation awareness of current system conditions.

2015 Key Assumptions

- NERC's Critical Infrastructure Department will have responsibility for the identification and management of the specialized critical infrastructure protection resources needed to support overall ERO CIP goals and objectives, as well as the specialized CIP resources needs of the other program areas (e.g., Standards, Compliance, Situation Awareness)

- NERC will continue to budget and incur costs to operate and maintain the software applications and systems known as Situational Awareness for NERC, FERC and Regions (SAFNR). NERC will also continue to fund the Grid Security Exercise (GridEx) and the Security Readiness Program to help Registered Entities with CIP compliance and security

awareness. The Regional Entities will be expected to provide subject matter experts for support of these activities.

- NERC will continue to fund, operate and maintain the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), with no increased cost to Regional Entities.

- There will be increased need and demand for CIP-related training and workshops. CIP compliance activities are budgeted within compliance. FRCC will continue to support and facilitate the development of NERC's secure portal for the management of alerts and infrastructure security information.

- There will be continued focus on detecting off-normal events to be analyzed by the responsible entity, FRCC or NERC.

2015 Goals and Key Deliverables

- Ensure that FRCC goals and activities support the mission to provide FERC, NERC and the staffs from the eight Regional Entities a visualization tool that enables the appropriate level of situation awareness for the near real-time conditions on the BES. Continue to work with the FRCC Reliability Coordinator to ensure that SAFNR and appropriate hardware and software resources are allocated. Continue to support future development of the situation awareness project capabilities.
- Issue and track security recommendations to protect the Bulk Power System. Share information learned in Situation Awareness with the Events Analysis program to develop relevant lessons learned.

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – There is a de minimus (0.01) increase in FTEs. The increase in personnel expense is due to a budgeted annual merit increase.
- **Operating Expenses** –The increase in Operating Expenses is driven by the cost of a security improvement initiative offset by an anticipated decrease in legal fees.
- **Indirect Expenses -** The increase in Indirect Expense is the result of a succession plan for expected future retirements.

Situation Awareness and Infrastructure Security Program

Funding sources and related expenses for the situation awareness and infrastructure security section of the 2015 business plan are shown in the table below.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital
2014 Budget & Projection, and 2015 Budget
Situation Awareness and Infrastructure Security

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 18,365	$ 18,365	$ -	$ 22,769	$ 4,404
Penalty Sanctions	1,015	1,015	$ -	512	(502)
Total ERO Funding	**$ 19,380**	**$ 19,380**	**$ -**	**$ 23,281**	**$ 3,901**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 19,380**	**$ 19,380**	**$ -**	**$ 23,281**	**$ 3,901**
Expenses					
Personnel Expenses					
Salaries	$ 10,017	$ 7,735	$ (2,282)	$ 12,256	$ 2,239
Payroll Taxes	631	493	(138)	762	131
Benefits	1,387	1,015	(372)	1,463	76
Retirement Costs	1,591	1,270	(321)	1,961	370
Total Personnel Expenses	**$ 13,626**	**$ 10,513**	**$ (3,113)**	**$ 16,442**	**$ 2,816**
Meeting Expenses					
Meetings	$ 13	$ 18	$ 5	$ 34	$ 21
Travel	69	68	(1)	99	30
Conference Calls	8	21	13	9	1
Total Meeting Expenses	**$ 90**	**$ 107**	**$ 17**	**$ 142**	**$ 52**
Operating Expenses					
Consultants & Contracts	$ 209	$ 234	$ 25	$ 401	$ 192
Office Rent	1,068	863	(205)	1,196	128
Office Costs	2,162	1,540	(622)	2,237	75
Professional Services	346	101	(245)	178	(168)
Miscellaneous	-	-	-	-	-
Depreciation	2,431	2,440	9	2,462	31
Total Operating Expenses	**$ 6,216**	**$ 5,178**	**$ (1,038)**	**$ 6,474**	**$ 258**
Total Direct Expenses	**$ 19,932**	**$ 15,798**	**$ (4,134)**	**$ 23,058**	**$ 3,126**
Indirect Expenses	**$ 1,840**	**$ 1,660**	**$ (180)**	**$ 2,621**	**$ 781**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 21,772**	**$ 17,458**	**$ (4,314)**	**$ 25,679**	**$ 3,907**
Change in Assets	**$ (2,392)**	**$ 1,922**	**$ 4,314**	**$ (2,398)**	**$ (6)**
Fixed Assets					
Depreciation	$ (2,431)	$ (2,440)	$ (9)	$ (2,462)	$ (31)
Total Fixed Asset Purchases	39	17	(22)	64	25
Change in Fixed Assets	**$ 2,392**	**$ 2,423**	**$ 31**	**$ 2,398**	**$ 6**
TOTAL BUDGET	$ 19,380	$ 15,035	$ (4,345)	$ 23,281	$ 3,901
TOTAL CHANGE IN WORKING CAPITAL	**$ -**	**$ 4,345**	**$ 4,345**	**$ -**	**$ -**
FTEs	0.08	0.06	(0.02)	0.09	0.01

General and Administrative

General and Administrative (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	3.36	4.04	0.68
Expenses	$ 623,583	$ 782,663	$ 159,080
Inc(Dec) in Fixed Assets	$ (1,643)	$ -	$ 1,643
Total Allocation to Statutory Programs	$ 621,940	$ 782,663	$ 160,723
Working Capital Requirement	$ (849,875)	$ (657,395)	$ 192,480

Program Scope and Functional Description Background

Charges included in General and Administrative are general legal expenses, executive time and expenses, human resources, information technology and accounting and finance. Every effort is made to charge items and time directly to activities and to designate as statutory or non-statutory. Undesignated items are shared costs between the Regional Entity Division and the Member Services Division and are allocated based on actual labor hours charged.

Legal and Regulatory Background

The FRCC General Counsel serves as the chief legal advisor to the President and CEO, Board of Directors, staff and stakeholders on all legal and regulatory matters affecting the FRCC. FRCC may use additional specialized legal resources on an as-needed basis, such as for tax matters, employee benefit plan issues and significant policy or FERC matters.

2015 Goals and Key Deliverables

- Assist the FRCC in carrying out its responsibilities as required by the approved delegation agreement between NERC and FRCC.
- Provide general corporate legal advice, legal training and timely, accurate filings to Regulatory authorities.

2015 Assumptions

In the 2015 Budget, as in the 2014 and 2013 budgets, there are no specific funds for hearings under CMEP Rules.

Information Technology Background

The FRCC maintains a number of tools and other support services for the benefit of its members, Registered Entities, Reliability Coordinator agent(s) and other system operators. These services include the FRCC Load and Resource Database (LRDB), the Compliance Tracking System (CTS), Compliance Issues Tracking System (CITS), Models on Demand (MOD), the FRCC corporate website, as well as other systems for collaboration, communication, data gathering and analysis.

Several years ago, NERC and the eight (8) Regional Entities formed an executive management group (known as the ERO EMG) which has, among other things, concentrated on developing enterprise-wide IT applications; with a goal of improving efficiency and consistency across NERC and the Regional Entities. As enterprise-wide projects are identified and prioritized by the ERO EMG, they are managed through a single Project Management Office (PMO) at NERC. The PMO has developed an ERO Enterprise application roadmap that will identify projects that NERC and the Regional Entities have agreed upon that are necessary to support improved efficiency and consistency across the ERO.

The NERC IT budget does not supplant the FRCC's need for IT expenditures for specific regional projects, but to the extent that agreed –upon ERO Enterprise applications provide greater efficiencies, there is no unnecessary, redundant expenditures contained in the FRCC business plan and budget.

2015 Goals and Key Deliverables

- Maintain IT and telecommunications systems and resources for efficient utilization of FRCC personnel.
- Improve the physical security of the FRCC office with additional access control and logging.
- Implement updated communications tools and technologies.
- Develop and enhance tools to automate and improve FRCC data collection and analysis processes.
- Expand IT support of the FRCC CMEP and provide additional metrics to improve accuracy and tracking within the CMEP processes.
- Continue the process of Document Management conversion in the Operating and Planning and Administrative programs.
- Implement needed changes to improve the FRCC corporate security posture as identified in the security assessment performed in 2014; improve overall security in all programs, enhance access controls with improved authentication mechanisms and increase security awareness and training.
- Improve disaster recovery and business continuity capabilities by implementing new geographically diverse data recovery solutions.

Human Resources Background

The FRCC has assembled an exceptional team of highly qualified employees to carry out the activities of the FRCC. The human resources department, in adherence with applicable federal and state laws, develops plans, and implements human resources policies and procedures, including staffing, compensation, benefits, employee relations, and training and development.

2015 Goals and Key Deliverables

- Recruit successful employees
- Improve human resource policies and procedures

- Provide management and training programs
- Ensure competitive employee compensation and benefits

Finance and Accounting Background

The FRCC will submit its annual budget for statutory and non-statutory activities to the FRCC Board of Directors for approval and then file the approved annual budget for statutory and non-statutory activities to NERC. This includes supporting materials such as a complete business plan and organizational chart, and the proposed expenditure of funds collected in sufficient detail to justify the requested funding collection and budget expenditures.

The Finance and Accounting Department will: direct the overall financial plans and accounting practices of the organization; oversee treasury, accounting, budget preparation and reporting, tax, and audit activities; and oversee financial and accounting system controls and standards.

2015 Goals and Key Deliverables

- Prepare the 2016 statutory and non-statutory budgets
- Report budget variances to the FRCC Corporate Compliance Finance and Audit Committee, the FRCC Board and to NERC on a quarterly basis
- Evaluate and advise on the impact of long-range planning
- Continue to provide on-going training to employees to ensure employees charge their time correctly
- Carry out succession planning and training in anticipation of retirement of key personnel

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – The increase is the result of a succession plan for an anticipated retirement and the training costs associated with that transition. The increase in personnel expense is also due to a budgeted annual merit increase.
- Operating Expenses –The increase in Operating Expenses is driven by the increased contract costs included in Contracts, Consultants and Software for a security improvement initiative.

General and Administrative

Funding sources and related expenses for the general and administrative section of the 2015 business plan are shown in the table below.

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital
2014 Budget & Projection, and 2015 Budget
General and Administrative

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ (849,875)	$ (849,875)	$ -	$ (657,395)	$ 192,480
Penalty Sanctions			-		
Total ERO Funding	**$ (849,875)**	**$ (849,875)**	**$ -**	**$ (657,395)**	**$ 192,480**
Membership Dues	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ (849,875)**	**$ (849,875)**	**$ -**	**$ (657,395)**	**$ 192,480**
Expenses					
Personnel Expenses					
Salaries	$ 420,733	$ 462,932	$ 42,199	$ 533,458	$ 112,725
Payroll Taxes	26,482	29,533	3,051	33,175	6,693
Benefits	58,253	57,398	(855)	62,568	4,315
Retirement Costs	65,227	74,173	8,946	85,353	20,126
Total Personnel Expenses	**$ 570,695**	**$ 624,036**	**$ 53,341**	**$ 714,554**	**$ 143,859**
Meeting Expenses					
Meetings	$ -	$ -	$ -	$ -	$ -
Travel	-	-	-	-	-
Conference Calls	-	-	-	-	-
Total Meeting Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Operating Expenses					
Consultants & Contracts	$ 2,547	$ 3,202	$ 655	$ 11,301	$ 8,754
Office Rent	44,857	51,666	6,809	52,037	7,180
Office Costs	3,841	1,807	(2,034)	4,771	930
Professional Services	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Depreciation	1,643	-	(1,643)	-	(1,643)
Total Operating Expenses	**$ 52,888**	**$ 56,675**	**$ 3,787**	**$ 68,109**	**$ 15,221**
Total Direct Expenses	**$ 623,583**	**$ 680,711**	**$ 57,128**	**$ 782,663**	**$ 159,080**
Indirect Expenses	**$ (623,583)**	**$ (680,711)**	**$ (57,128)**	**$ (782,663)**	**$ (159,080)**
Other Non-Operating Expenses	$ -	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Change in Assets	**$ (849,875)**	**$ (849,875)**	**$ -**	**$ (657,395)**	**$ 192,480**
Fixed Assets					
Depreciation	$ (1,643)	$ -	$ 1,643	$ -	1,643
Total Fixed Asset Purchases	-	-	-	-	-
Change in Fixed Assets	**$ 1,643**	**$ -**	**$ (1,643)**	**$ -**	**$ (1,643)**
TOTAL BUDGET	$ -	$ -	$ 1,643	$ -	$ 1,643
TOTAL CHANGE IN WORKING CAPITAL	**$ (849,875)**	**$ (849,875)**	**$ (1,643)**	**$ (657,395)**	**$ 190,837**
FTEs	3.36	3.57	0.21	4.04	0.68

Section B – Supplemental Financial Information
2015 Business Plan and Budget

Reserve Balance

Table B-1

Working Capital Reserve Analysis 2014-2015		
STATUTORY		
Beginning Working Capital Reserve (Deficit), December 31, 2013		1,966,888
Less: Penalty sanctions being held to be used as offset to 2015 assessments	[1]	**(153,000)**
Plus: 2014 ERO Funding (from LSEs or designees)		5,488,058
Plus: Projected 2014 Other funding sources		139,369
Plus: Penalty Sanctions Applied		343,000
Less: 2014 Projected expenses & capital expenditures		**(6,530,067)**
Projected Working Capital Reserve Surplus/(Deficit), December 31, 2014		**1,254,248**
Desired Working Capital Reserve, December 31, 2015	[2]	596,853
Less: Projected Working Capital Reserve, December 31, 2014		**(1,254,248)**
Increase(decrease) in assessments to achieve desired Working Capital Reserve		**(657,395)**
2015 Assessment for Expenses and Capital Expenditures		7,162,233
Less: Penalty Sanctions	[1]	**(153,000)**
Less: Other Funding Sources		**(114,000)**
Adjustment to achieve desired Working Capital Reserve		**(657,395)**
2015 Assessment		6,237,838

[1] Represents collections prior to June 30, 2014.

[2] On June 26, 2013, the FRCC Board of Directors set a working capital and operating working capital and operating reserve requirement of one (1) month of the total annual budget. The FRCC has a $1.5 million line of credit.

Breakdown by Statement of Activity Sections

The following detailed schedules are in support of the Table on page 13, of the 2015 FRCC Business Plan and Budget. All significant variances have been disclosed by program area in the preceding pages.

Penalty Sanctions

Penalty monies received prior to June 30, 2014 are to be used to offset assessments in the 2015 Budget, as documented in the NERC Policy – ACCOUNTING, FINANCIAL STATEMENT AND BUDGETARY TREATMENT OF PENALTIES IMPOSED AND RECEIVED FOR VIOLATIONS OF RELIABILITY STANDARD. Penalty monies received from July 1, 2014 through June 30, 2015 will be used to offset assessments in the 2016 Budget.

All penalties received prior to June 30, 2014 are detailed below.

Allocation Method: Penalty sanctions received have been allocated to the following statutory programs to reduce assessments: Reliability Standards; Compliance Monitoring & Enforcement and Organization Registration & Certification; Reliability Assessments and Performance Analysis; Training, Education and Operator Certification; and Situation Awareness and Infrastructure Security. Penalty sanctions are allocated based upon the number of FTEs in the Program divided by the aggregate total FTEs in the Programs receiving the allocation.

Table B-2

Penalty Sanctions Received On or Prior to June 30, 2014	Date Received	Amount Received
Penalty #1	10/25/2013	$ 38,000
Penalty #2	11/26/2013	100,000
Penalty #3	12/27/2013	7,000
Penalty #4	1/22/2014	2,000
Penalty #5	1/22/2014	2,000
Penalty #5	3/25/2014	4,000
Total Penalties Received		$ 153,000

Supplemental Funding

Table B-3

Outside Funding Breakdown By Program	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget
Reliability Standards Development				
Total	$ -	$ -	$ -	$ -
Compliance Monitoring, Enforcement & Org. Registration	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ -	$ -
Reliability Assessment and Performance Analysis				
Services & Software Fees	$ 24,000	$ 24,000	$ 24,000	$ -
	-	-	-	-
Total	$ 24,000	$ 24,000	$ 24,000	$ -
Training, Education and Operator Certification				
Workshops	$ 90,000	$ 115,369	$ 90,000	$ -
Total	$ 90,000	$ 115,369	$ 90,000	$ -
Situation Awareness and Infrastructure Security	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ -	$ -
General and Administrative*				
Interest	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ -	$ -
Total Outside Funding	$ 114,000	$ 139,369	$ 114,000	$ -

Assumes that no appreciable excess cash will be in the Bank Accounts and due to current low interest rates, no Interst is being budgeted.

Personnel Expenses

Table B-4

Personnel Expenses	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Salaries					
Total Salaries	$ 3,806,631	$ 3,630,346	$ 4,082,307	$ 275,676	7.24%
Total Payroll Taxes	$ 239,599	$ 231,599	$ 253,874	$ 14,275	5.96%
Benefits					
Workers Compensation	$ 10,241	$ 10,006	$ 11,179	$ 938	9.16%
Medical, LTD, STD Insurances	483,409	418,850	445,548	(37,861)	-7.83%
Employment Fees	-		-	-	
Education	100,319	88,994	100,676	357	0.36%
Employee Welfare & Contract Labor	18,936	55,671	22,080	3,144	16.60%
Relocation	44,350	35,000		(44,350)	-100.00%
Total Benefits	$ 657,255	$ 608,521	$ 579,483	$ (77,772)	-11.83%
Retirement					
Retirement Costs	$ 602,881	$ 594,403	$ 666,669	$ 63,788	10.58%
		-		-	
Total Retirement	$ 602,881	$ 594,403	$ 666,669	$ 63,788	10.58%
Total Personnel Costs	$ 5,306,366	$ 5,064,869	$ 5,582,333	$ 275,967	5.20%
FTEs	30.40	27.97	30.91	0.5	1.68%
Cost per FTE					
Salaries	$ 125,218	$ 129,794	$ 132,071	6,853	5.47%
Payroll Taxes	7,882	8,280	8,213	332	4.21%
Benefits	21,620	21,756	18,747	(2,873)	-13.29%
Retirement	19,832	21,251	21,568	1,736	8.76%
Total Cost per FTE	**$ 174,552**	**$ 181,082**	**$ 180,600**	**$ 6,048**	**3.46%**

Consultants and Contracts

Table B-5

Contracts & Consultants and Software & Licenses	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Contracts & Consultants and Software & Licenses					
Reliability Standards Development	$ 4,529	$ 5,222	$ 7,381	$ 2,852	62.97%
Compliance Monitoring & Enforcement and Org Reg	119,235	225,494	214,984	95,749	80.30%
Reliability Assessment and Performance Analysis	192,989	130,637	122,547	(70,442)	-36.50%
Training, Education and Operator Certification	29,259	51,473	37,104	7,845	26.81%
Situation Awareness and Infrastructure Security	209	234	401	192	91.87%
General and Administrative	2,547	3,202	11,301	8,754	343.70%
Total Contracts & Consultants and Software & Licenses	$ 348,768	$ 416,262	$ 393,718	$ 44,950	12.89%

"The amount for Consultants & Contracts in the Compliance Monitoring and Enforcement Program includes $16,000 in the 2014 budget, $25,500 in the projected 2014 and $3,500 in the 2015 budget estimated by SERC as the costs for SERC to perform compliance monitoring and enforcement responsibilities for the FRCC registered functions."

Office Rent

Table B-6

Office Rent	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Office Rent	$ 555,089	$ 554,412	$ 547,586	$ (7,503)	-1.35%
Total Office Rent	**$ 555,089**	**$ 554,412**	**$ 547,586**	**$ (7,503)**	**-1.35%**

Office Costs

Table B-7

Office Costs	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Telephone	$ 50,931	$ 49,865	$ 43,767	$ (7,164)	-14.07%
Internet	2,618	2,566	4,020	$ 1,402	53.55%
Office Supplies	14,172	19,313	17,719	$ 3,547	25.03%
Computer Supplies	4,226	4,191	9,322	$ 5,096	120.59%
Publications, Subscriptions & Dues	9,710	7,445	13,533	$ 3,823	39.37%
Postage	1,558	1,528	1,523	$ (35)	-2.25%
Equipment Maintenance	930	917	6,750	$ 5,820	625.81%
Copying	-			$ -	
Printing	23,166	26,334	21,069	$ (2,097)	-9.05%
Stationary Forms				$ -	
Commerical Insurance	11,032	10,815	14,366	$ 3,334	30.22%
Miscellaneous				$ -	
Total Office Costs	**$ 118,343**	**$ 122,974**	**$ 132,069**	**$ 13,726**	**11.60%**

Professional Services

Table B-8

Professional Services	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Outside Legal	$ 100,000	$ 25,000	$ 35,000	$ (65,000)	-65.00%
Accounting & Auditing Fees	16,642	16,315	16,324	$ (318)	-1.91%
Total Services	**$ 116,642**	**$ 41,315**	**$ 51,324**	**$ (65,318)**	**-56.00%**

Other Non-Operating Expenses

Table B-9

Other Non-Operating Expenses	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Interest Expense	$ -	$ -		$ -	
Office Relocation	-	-		$ -	
Total Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	

2015, 2016 and 2017 Projections

Table B-10

Statement of Activities and Capital Expenditures
2015, 2016 and 2017 Projections
Regional Entity

	2014 Budget	2015 Budget	$ Change 2015:2014 Over(Under)	% Chg 2015:2014 Over(Under)	2016 Projection	$ Change 2016:2015 Over(Under)	% Chg 2016:2015 Over(Under)	2017 Projection	$ Change 2017:2016 Over(Under)	% Chg 2017:2016 Over(Under)
Funding										
ERO Funding										
ERO Assessments	$ 5,488,057	$ 6,237,838	$ 749,781	13.66%	$ 7,271,064	$ 1,033,226	16.56%	$ 7,506,418	$ 235,354	3.24%
Penalty Sanctions	343,000	153,000	(190,000)	0.00%	-		-100.00%	-	-	
Total ERO Funding	**$ 5,831,057**	**$ 6,390,838**	**$ 559,781**	9.60%	**$ 7,271,064**	**$ 1,033,226**	13.77%	**$ 7,506,418**	**$ 235,354**	3.24%
Membership Dues	$ -	$ -	$ -		$ -	$ -		$ -	$ -	
Testing Fees	-	-	-		-	-		-	-	
Services & Software	24,000	24,000	-	0.00%	24,000	-	0.00%	24,000	-	0.00%
Workshops	90,000	90,000	-	0.00%	90,000	-	0.00%	90,000	-	0.00%
Interest	-	-	-		-	-		-	-	
Miscellaneous	-	-	-		-	-		-	-	
Total Funding	**$ 5,945,057**	**$ 6,504,838**	**$ 559,781**	9.42%	**$ 7,385,064**	**$ 1,033,226**	13.53%	**$ 7,620,418**	**$ 235,354**	3.19%
Expenses										
Personnel Expenses										
Salaries	$ 3,806,631	$ 4,082,307	$ 275,676	7.24%	$ 4,204,776	$ 122,469	3.00%	$ 4,330,919	$ 126,143	3.00%
Payroll Taxes	239,599	253,874	14,275	5.96%	261,490	7,616	3.00%	269,335	7,845	3.00%
Benefits	657,255	579,483	(77,772)	-11.83%	594,062	14,579	2.52%	609,082	15,020	2.53%
Retirement Costs	602,881	666,669	63,788	10.58%	686,264	19,595	2.94%	706,447	20,183	2.94%
Total Personnel Expenses	**$ 5,306,366**	**$ 5,582,333**	**$ 275,967**	5.20%	**$ 5,746,592**	**$ 164,259**	2.94%	**$ 5,915,783**	**$ 169,191**	2.94%
Meeting Expenses										
Meetings	$ 80,930	$ 69,292	$ (11,638)	-14.38%	$ 69,588	$ 296	0.43%	$ 69,892	$ 304	0.44%
Travel	167,209	191,753	24,544	14.68%	192,612	859	0.45%	193,497	885	0.46%
Conference Calls	18,771	9,482	(9,289)	-49.49%	9,564	82	0.86%	9,648	84	0.88%
Total Meeting Expenses	**$ 266,910**	**$ 270,527**	**$ 3,617**	1.36%	**$ 271,764**	**$ 1,237**	0.46%	**$ 273,037**	**$ 1,273**	0.47%
Operating Expenses										
Consultants & Contracts	$ 348,768	$ 393,718	$ 44,950	12.89%	$ 422,443	$ 28,725	7.30%	$ 448,117	$ 25,674	6.08%
Office Rent	555,089	547,586	(7,503)	-1.35%	559,532	11,946	2.18%	571,837	12,305	2.20%
Office Costs	118,343	132,069	13,726	11.60%	134,291	2,222	1.68%	136,578	2,287	1.70%
Professional Services	116,642	51,324	(65,318)	-56.00%	52,864	1,540	3.00%	54,450	1,586	3.00%
Miscellaneous	-	-	-		-	-		-	-	
Depreciation	110,490	202,287	91,797	83.08%	202,897	610	0.30%	203,525	628	0.31%
Total Operating Expenses	**$ 1,249,332**	**$ 1,326,984**	**$ 77,652**	6.22%	**$ 1,372,027**	**$ 45,043**	3.39%	**$ 1,414,507**	**$ 42,480**	3.10%
Total Direct Expenses	**$ 6,822,608**	**$ 7,179,844**	**$ 357,236**	5.24%	**$ 7,390,383**	**$ 210,539**	2.93%	**$ 7,603,327**	**$ 212,944**	2.88%
Indirect Expenses	**$ (1,643)**	$ 0	$ 1,643		**$ 0**	**$ 1,643**	0.00%	**$ -**	**$ 212,944**	-100.00%
Other Non-Operating Expenses	**$ -**	$ -	$ -		**$ -**	**$ -**		**$ -**	**$ -**	
Total Expenses	**$ 6,820,965**	**$ 7,179,844**	**$ 358,879**	5.26%	**$ 7,390,383**	**$ 212,182**	2.93%	**$ 7,603,327**	**$ 425,889**	2.88%
Change in Assets	**$ (875,908)**	**$ (675,006)**	**$ 200,902**	-22.94%	**$ (5,319)**	**$ 821,044**	-99.21%	**$ 17,091**	**$ (190,534)**	-421.32%
Fixed Assets										
Depreciation	$ (110,490)	$ (202,287)	$ (91,797)	83.08%	$ (202,897)	$ (610)	0.30%	$ (203,525)	$ (628)	0.31%
Total Fixed Asset Purchases	82,814	184,676	101,862	123.00%	197,578	12,902	6.99%	220,616	23,038	11.66%
								-	-	
Change in Fixed Assets	**$ 27,676**	**$ 17,611**	**$ (10,065)**	-36.37%	**$ 5,319**	**$ (12,292)**	-69.80%	**$ (17,091)**	**$ (22,410)**	-421.32%
TOTAL BUDGET	$ 6,793,289	$ 7,162,233	$ 368,944	5.43%	$ 7,385,064	$ 224,474	3.11%	$ 7,620,418	$ 448,299	3.19%
TOTAL CHANGE IN WORKING CAPITAL	**$ (848,232)**	**$ (657,395)**	**$ 190,837**	-22.50%	**$ -**	**$ 808,752**	-100.00%	**$ -**	**$ (212,944)**	
FTEs	30.40	30.91	0.51	1.68%	30.91	-	0.00%	30.91	-	0.00%

Section C – Non-Statutory Activities
2015 Business Plan and Budget

Member Services Activities (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	16.8	18.4	1.5
Direct Expenses	7,454,381	8,422,053	967,672
Indirect Expenses	-	-	-
Inc(Dec) in Fixed Assets	1,614	(30,071)	(31,685)
Total Funding Requirement	7,455,995	8,391,982	935,987

Non-Statutory Functional Scope Background

The Member Services (MS) division of the FRCC provides, coordinates and administers a variety of services relating to the reliable planning and operation of the BES within the FRCC Region. These services are carried out by the FRCC Member Services Planning Committee (PC) and the FRCC Member Services Operating Committee (OC), various subcommittees, task forces and working groups, as well as FRCC Staff.

Member Services Objectives

- Ensure the reliability of the BES in the FRCC region.
- Coordination, planning, operation and maintenance of reliable bulk electricity supply in the FRCC region.

Membership and Governance

The FRCC's Members in the Member Services Division include investor-owned utilities, cooperative utilities, municipal utilities, power marketers and independent power producers. Current membership is 23 FRCC Members in 2014 and is not expected to change in 2015.

The activities of FRCC are directed by its Board of Directors. The Board is comprised of senior level executives from the FRCC membership.

Planning Committee (PC) Functional Scope

The PC promotes the reliability of the BES within the FRCC Region by assessing and encouraging generation and transmission adequacy. The PC assesses generation adequacy by performing a reliability assessment taking into account projected load and resources. The PC, through the FRCC Regional Transmission Planning Process, provides a vehicle for ensuring that transmission planning within the FRCC will provide for the development of a robust transmission network within the FRCC Region. The Regional Transmission Planning Process is a coordinated transmission planning process that evaluates all BES and non-BES transmission facilities. The major goal of this process is to ensure that the planning of transmission facilities

will meet the needs of all market participants in a coordinated, open and transparent transmission planning environment.

The FRCC will continue to develop, on an annual basis, a Regional Transmission Plan following the Regional Transmission Planning Process. The Regional Transmission Planning process will be revised to incorporate the planning principles from FERC Order 1000. The Regional Plan is based on the Ten Year Site Plans that are required to be submitted to the Florida Public Service Commission (FPSC) on April 1st of each year. The FRCC participates in an annual Ten Year Site Plan Workshop held by the FPSC where the results of resource and transmission adequacy assessments are presented.

The FRCC PC relies on the following subordinate groups to achieve its goals: Resource Working Group (RWG), Stability Working Group (SWG), and the Transmission Working Group (TWG).

The PC, supported by FRCC MS staff, has the primary responsibility of the Planning Authority (PA) function including implementation of all applicable PA NERC Reliability Standards.

Resource Working Group
The RWG performs reliability assessments of FRCC resource adequacy for the future 10-year period for peninsular Florida based on individual utility information that was the basis of their respective EIA-411 and Ten Year Site Plan filings with the Florida Public Service Commission. These reliability assessments are based upon the FRCC resource adequacy criteria.

Stability Working Group
The SWG is responsible for assessing the dynamic performance of the FRCC BES under various credible system conditions. In addition, the SWG performs the following assessments and studies: Coordination and performance of Special Protection Systems, the effectiveness of FRCC under-frequency load shedding program and coordination with other protection and control systems, Extreme Event Study and other assessments in support of the FRCC Regional Transmission Planning Process. The SWG annually develops FRCC dynamic models.

Transmission Working Group
The TWG engages in active coordination of transmission planning within the FRCC Region under the direction of the FRCC Planning Committee in support of the FRCC Regional Transmission Planning Process. The TWG annually performs a FRCC Long Range Study, sensitivity studies as directed by the PC, evaluates Transmission Service Requests and evaluates Generator Interconnection Service Requests. In addition, the TWG annually develops a FRCC Transmission Map, FRCC power flow models and FRCC short circuit models.

Operating Committee (OC) Functional Scope

The primary goal of the OC is to promote the reliability of the BES within the FRCC Region. The OC is responsible for the coordination, operations planning, operation and maintenance of the interconnected systems operating in the Region. The OC's primary reliability goals include effective implementation of the Regional Reliability Plan (*Reliability Process for the FRCC Bulk Electric System*), continuous improvement of operator awareness and communications and ensuring that adequate physical, operational and cyber security objectives are in place for the Region's shared communications network. The OC subordinate groups include the Operating

Reliability Subcommittee (ORS), Data Exchange Working Group (DEWG), Fuel Reliability Working Group (FRWG), Operations Planning Working Group (OPWG), Telecommunications Subcommittee (TS), System Protection and Control Subcommittee (SPCS) and the Critical Infrastructure Protection Subcommittee (CIPS). The OC ensures reliable operations are maintained through the implementation and oversight of the FRCC Reliability Coordinator (RC) functions as established in the Regional Reliability Plan.

The FRCC RC responsibilities include the real-time operating function and the next-day operations planning function. The RC tasks are performed by a designated agent of the FRCC with direction and oversight by FRCC committees and support staff. The designated agent performs real-time operations and next-day planning operations. FRCC staff supports Regional reliability by performing the roles of the Operations Planning Coordinator (OPC), and State Capacity Emergency Coordinator (SCEC) as defined in the *Reliability Process for the FRCC Bulk Electric System* document.

The FRCC RC function is accountable to the FRCC OC who has overall responsibility of the administration, development and implementation of operating procedures provided by the ORS for the NERC Operations & Planning (Non-CIP) Standards.

The FRCC continues to improve FRCC PA and RC compliance management programs under the Member Services Division based on the evolving regulatory requirements. The FRCC has improved its oversight of PA and RC functions by creating an independent Member Services Regulatory Department with a dedicated Regulatory Director who reports directly to the FRCC President and CEO and who has direct access to the FRCC Board of Directors. This position is responsible for the implementation, maintenance and oversight of the FRCC Internal Compliance Program (ICP) including all compliance activities for the FRCC registered entity functions and is the primary interface for all regulatory activities associated with the FRCC Member Services committees and is the FRCC liaison between external Compliance Enforcement Authorities.

Operating Reliability Subcommittee (ORS)

The ORS provides overall administration for the development and implementation of operating procedures and other reliability matters including the oversight of the FRCC RC function for Operating and Planning (non-CIP) NERC Standards. The ORS reviews and assesses regional import and export limits, scheduled transmission outages, real-time system reliability, events analysis, information and data exchange and other reliability issues. The ORS provides formal oversight and implementation of the Reliability Process for the FRCC Bulk Electric System which establishes the reliability responsibilities of the various entities within the Region and specifically monitors the agent responsible for performing the RC functions.

Data Exchange Working Group (DEWG)

The DEWG, subordinate to the ORS, supports the real-time data needs of the FRCC Reliability Coordinator and other operating entities. It is also responsible for developing methodologies to facilitate the exchange of real-time, modeling and other operational data to help ensure reliable electric power system operations. Accurate modeling of the FRCC BES is essential to maintaining situation awareness and ensuring reliability. Within the FRCC, operating entities provide system data via the FRCC Reliability Data Link (RDL). The FRCC RDL receives electric system reliability data from the operating entities on a real-time basis and allows the data to be made available.

Fuel Reliability Working Group (FRWG)
The FRWG, also subordinate to the ORS, has been established to deal with matters relating to fuel and impacts to BES reliability. Specifically, the FRWG provides the administrative oversight of a Regional fuel reliability forum that studies the interdependencies of fuel availability and electric reliability and supports coordinated Regional responses to fuel issues and fuel emergencies.

Operations Planning Working Group (OPWG)
The OPWG, as a part of the ORS, has been established to provide oversight, guidelines and procedures to the FRCC Operations Planning Coordinator (OPC) in accordance with the Reliability Process for the FRCC BES document. The OPWG focuses on BES reliability and developing processes and documentation that support regional reliability and adherence to the NERC Reliability Standards as they relate to the OPC function.

FRCC Telecommunications Subcommittee (TS)
The TS provides oversight for the TS budget which is included in the OC budget. The primary purpose of the TS is to ensure that adequate and redundant communications facilities are made available to the operating entities within the FRCC, including the FRCC Reliability Coordinator. The TS administers the FRCC Hotline program, Satellite phone program, and also ensures that reliable and redundant communications are maintained by the Eastern Interconnect Data Sharing Network, Inc. (EIDSN). All TS programs are non-statutory and support the Reliability Coordinator functions; with the exception of the FRCC satellite phone (located at the FRCC office) which is a tool that can be used by the Regional Entity to perform situation awareness and thus is budgeted as statutory.

FRCC System Protection and Control Subcommittee (SPCS)
The FRCC System Protection and Control Subcommittee (SPCS) has primary responsibility for the coordination of protection and control systems within the FRCC region, including regional disturbance monitoring equipment, review of protective mis-operations, protection related disturbance analysis and implementation of specific regional programs and procedures including the assessments of the FRCC Under-Frequency Load Shedding Program. The SPCS also reviews and coordinates system protection and control equipment installations, settings, protection philosophies and testing criteria within the region, when installations impact multiple entities. The SPCS serves as an important forum for sharing subject matter expert guidance and lessons learned / best practices for equipment issues and protection coordination.

FRCC Critical Infrastructure Protection Subcommittee (CIPS)
The purpose of the FRCC CIPS is to enhance the physical and cyber security of the critical BES infrastructure in the FRCC Region, with an emphasis on protecting, preventing, limiting and recovering from malicious activities directed at the FRCC critical energy infrastructure. The CIPS provides guidance to the OC on matters of critical energy infrastructure security, including cyber and physical security. The CIPS provides advice to the OC including implementation of all applicable FRCC RC CIP-002 through CIP-009 Reliability Standards.

Major 2015 Cost Impacts

The FRCC's proposed 2015 Members Services budgeted expenses and net fixed assets are $8,391,982, which is a $935,987 or 12.6% increase over the 2014 budgeted expenses. The cost impacts by function of this increase are:

Planning Committee (PC)
The Member Services Planning Committee (PC) expenses for 2015 are made up of the PC Committee budget, as well as the administrative costs to provide support personnel for implementation of the FRCC Planning Authority (PA) functions and all other Member Services PC activities. In 2015, staff will spend additional time enhancing FRCC steady state planning studies and has budgeted $150,000 for additional stability studies to prepare to meet the requirements of the new NERC Transmission Planning (TPL) Standard. In addition, staff is expected to add one FTE in 2015 to support the implementation of FERC Order 1000 as recommended by the PC.

The 2015 PC budget is developed based on the activities of the Resource Working Group (RWG), the Stability Working Group (SWG) and the Transmission Working Group (TWG). These budgets are primarily for the labor involved in coordination activities performed by member representatives, software and meeting costs.

Operating Committee (OC)
The Member Services Operating Committee (OC) expenses for 2015 are made up of a 2015 OC budget as well as the administrative costs to provide support personnel for implementation of the FRCC Reliability Coordinator (RC) functions and other Member Services OC activities. In 2015, staff will spend additional time coordinating activities with member companies to ensure continued reliability and compliance with changing NERC Reliability Standards.

The 2015 OC budget is developed based primarily on the activities of the Operating Reliability Subcommittee (ORS), the Telecommunications Subcommittee (TS), the Fuel Reliability Working Group (FRWG) and the Critical Infrastructure Protection Subcommittee (CIPS). These budgets are related to, or in support of both the FRCC Reliability Coordinator (RC) and Member Services entity's reliability functions and includes consulting costs, contract costs, computer software purchases and expenses to support the associated activities. These budgets do not include FRCC staff salaries or associated personnel costs.

The administrative costs associated with the FRCC OC support personnel include FRCC staff that support implementation of the FRCC RC functions and staff that support overall OC activities. The staff includes dedicated employees as well as shared employees.

Funding Sources and Requirements — Explanation of Increase (Decrease)

- **Personnel Expenses** – The increase in FTEs is attributed to an additional employee in the planning area to support new long range planning activities, the effect of a complete year for the 2014 addition to staff to support the Reliability Coordinator function that was budgeted to be filled in mid-2014 and the result of the implementation of a succession plan for a key accounting position.
- **Operating Expenses** – The increase in Operating Expenses is attributed to increases in consultant and contractor costs for the RC and PA functions.

2014 Member Services Budget and Projection and 2015 Budget Comparisons

Statement of Activities, Fixed Assets Expenditures and Change in Working Capital
2014 Budget & Projection, and 2015 Budget
NON-STATUTORY MEMBER SERVICES

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ -	$ -	$ -	$ -	$ -
Penalty Sanctions	-	-	-	-	-
Total ERO Funding	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Membership Dues	$ 6,916,762	$ 6,916,762	$ -	8,240,106	1,323,344
Testing Fees	-	-	-	-	-
Services & Software	277,419	312,531	35,112	254,459	(22,960)
Workshops	-	-	-	20,000	20,000
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ 7,194,181**	**$ 7,229,293**	**$ 35,112**	**$ 8,514,565**	**$ 1,320,384**
Expenses					
Personnel Expenses					
Salaries	$ 2,108,824	$ 2,134,834	$ 26,010	$ 2,423,514	$ 314,690
Payroll Taxes	132,734	136,193	3,459	150,716	17,982
Benefits	350,795	320,232	(30,563)	351,746	951
Retirement Costs	328,267	343,386	15,119	387,762	59,495
Total Personnel Expenses	**$ 2,920,620**	**$ 2,934,645**	**$ 14,025**	**$ 3,313,738**	**$ 393,118**
Meeting Expenses					
Meetings	$ 37,515	$ 39,955	$ 2,440	$ 26,582	$ (10,933)
Travel	63,716	55,451	(8,265)	60,205	(3,511)
Conference Calls	27,108	30,959	3,851	45,286	18,178
Total Meeting Expenses	**$ 128,339**	**$ 126,365**	**$ (1,974)**	**$ 132,073**	**$ 3,734**
Operating Expenses					
Consultants & Contracts	$ 3,657,668	$ 3,843,855	$ 186,187	$ 4,260,160	$ 602,492
Office Rent	224,835	238,262	13,427	236,403	11,568
Office Costs	419,112	472,831	53,719	375,314	(43,798)
Professional Services	79,910	35,385	(44,525)	45,476	(34,434)
Miscellaneous	-	75,000	75,000	-	-
Depreciation	23,897	45,496	21,599	58,889	34,992
Total Operating Expenses	**$ 4,405,422**	**$ 4,710,829**	**$ 305,407**	**$ 4,976,242**	**$ 570,820**
Total Direct Expenses	**$ 7,454,381**	**$ 7,771,839**	**$ 317,458**	**$ 8,422,053**	**$ 967,672**
Indirect Expenses	$ -	$ -	**$ -**	**$ -**	**$ -**
Other Non-Operating Expenses	$ -	$ -	**$ -**	**$ -**	**$ -**
Total Expenses	**$ 7,454,381**	**$ 7,771,839**	**$ 317,458**	**$ 8,422,053**	**$ 967,672**
Change in Assets	**$ (260,200)**	**$ (542,546)**	**$ (282,346)**	**$ 92,512**	**$ (352,712)**
Fixed Assets					
Depreciation	$ (23,897)	$ (45,496)	$ (21,599)	$ (58,889)	$ (34,992)
Total Fixed Asset Purchases	25,511	78,929	53,418	28,818	3,307
	-	-			
Change in Fixed Assets	**$ (1,614)**	**$ (33,433)**	**$ (31,819)**	**$ 30,071**	**$ 31,685**
TOTAL BUDGET	$ 7,455,995	$ 7,805,272	$ 349,277	$ 8,391,982	$ 935,987
TOTAL CHANGE IN WORKING CAPITAL	**$ (261,814)**	**$ (575,979)**	**$ (314,165)**	**$ 122,583**	**$ 384,397**
FTEs	16.84	15.73	(1.11)	18.35	1.51

Personnel Analysis

Total FTE's by Program Area	Budget 2014	Projection 2014	Direct FTEs 2015 Budget	Shared FTEs[1] 2015 Budget	Total FTEs 2015 Budget	Change from 2014 Budget
NON-STATUTORY						
Operational Programs						
Operations Committee	10.48	9.94		10.27	10.27	-0.21
Planning Committee	3.27	3.52		4.57	4.57	1.30
Total FTEs Operational Programs	**13.75**	**13.46**	**0.00**	**14.84**	**14.84**	**1.09**
Administrative Programs						
General & Administrative	3.09	2.99		3.51	3.51	0.42
Total FTEs Administrative Programs	**3.09**	**2.99**	**0.00**	**3.51**	**3.51**	**0.42**
Total FTEs	**16.84**	**16.45**	**0.00**	**18.35**	**18.35**	**1.51**

[1]A shared FTE is defined by NERC as an employee who performs both Statutory and Non-Statutory functions.

Member Services Reserve Analysis — 2014 – 2015

Working Capital Reserve Analysis 2014-2015 NON-STATUTORY MEMBER SERVICES		
Beginning Working Capital Reserve (Deficit), December 31, 2013		587,073
Change in Post Retirement Benefit Obligation - Noncash Item		565,655
2014 Funding (from members)		6,916,762
2014 Projected Other funding sources		312,531
Total Cash Available 2014		8,382,021
Less: '2014 Projected expenses & capital expenditures		**(7,805,272)**
Projected Working Capital Reserve Surplus/(Deficit), December 31, 2014		**576,749**
Desired Working Capital Reserve, December 31, 2015	[1]	699,332
Less: Projected Working Capital Reserve, December 31, 2014		**(576,749)**
Increase(decrease) in assessments to achieve desired Working Capital Reserve		**122,583**
2015 Funding for Expenses and Capital Expenditures		8,391,982
Less: Other Funding Sources		**(274,459)**
Adjustment to achieve desired Working Capital Reserve		**122,583**
2015 Funding (reserve adjustment)		8,240,106

[1] On June 26, 2013, the FRCC Board of Directors set a working capital and operating working capital and operating reserve requirement of one (1) month of the total annual budget. The FRCC has a $1.5 million line of credit.

Section D – Additional Consolidated Financial Statements

2015 Business Plan and Budget

Section D — 2015 Additional Consolidated Financial Information

Statement of Activities and Capital Expenditures by Program 2014 Budget	Total	Functions in Delegation Agreement							Non-Statutory Functions		
		Statutory Total	Reliability Standards Development (Section 300)	Compliance Monitoring and Org Reg % Cert(Section 400 & 500)	Reliability Assessment and Performance Analysis (Section 800)	Training and Education (Section 900)	Situation Awareness and Infrastructure Security (Section 1000)	General and Administrative	Non-Statutory Total	Operating Committee	Planning Committee
Funding											
ERO Funding											
ERO Assessments	$ 6,237,838	$ 6,237,838	$ 413,407	$ 5,099,302	$ 1,133,412	$ 226,344	$ 22,769	$ (657,395)	$ -	$ -	$ -
Penalty Sanctions	153,000	153,000	9,737	112,572	24,997	5,182	512		-	-	-
Total ERO Funding	**6,390,838**	**6,390,838**	**423,143**	**5,211,874**	**1,158,409**	**231,525**	**23,281**	**(657,395)**	**-**	**-**	**-**
Membership Dues	$ 8,240,106	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 8,240,106	$ 6,792,087	$ 1,448,019
Testing Fees	-	-							-		
Services & Software	278,459	24,000			24,000				254,459	254,459	
Workshops	110,000	90,000				90,000			20,000	20,000	
Interest	-	-							-		
Miscellaneous	-	-							-		
Total Funding	**$ 15,019,403**	**$ 6,504,838**	**$ 423,143**	**$ 5,211,874**	**$ 1,182,409**	**$ 321,525**	**$ 23,281**	**$ (657,395)**	**$ 8,514,565**	**$ 7,066,546**	**$ 1,448,019**
Expenses											
Personnel Expenses											
Salaries	$ 6,505,821	$ 4,082,307	$ 225,465	$ 2,611,174	$ 580,711	$ 119,243	$ 12,256	$ 533,458	$ 2,423,514	$ 1,676,219	$ 747,295
Payroll Taxes	404,590	253,874	14,021	162,386	36,114	7,416	762	33,175	150,716	104,243	46,473
Benefits	931,229	579,483	32,602	385,976	82,646	14,228	1,463	62,568	351,746	235,709	116,037
Retirement Costs	1,054,431	666,669	36,074	431,288	92,914	19,079	1,961	85,353	387,762	268,195	119,567
Total Personnel Expenses	$ 8,896,071	$ 5,582,333	**$ 308,162**	**$ 3,590,824**	**$ 792,385**	**$ 159,966**	**$ 16,442**	**$ 714,554**	$ 3,313,738	$ 2,284,366	$ 1,029,372
Meeting Expenses											
Meetings	$ 95,874	$ 69,292	$ 2,606	$ 12,729	$ 1,612	$ 52,311	$ 34		$ 26,582	$ 18,286	$ 8,296
Travel	251,958	191,753	17,469	122,194	47,375	4,616	99		60,205	53,700	6,505
Conference Calls	54,768	9,482	203	4,390	447	4,433	9		45,286	30,491	14,795
Total Meeting Expenses	$ 402,600	$ 270,527	**$ 20,278**	**$ 139,313**	**$ 49,434**	**$ 61,360**	**$ 142**	**$ -**	$ 132,073	$ 102,477	$ 29,596
Operating Expenses											
Consultants & Contracts	$ 4,653,878	$ 393,718	$ 7,381	$ 214,984	$ 122,547	$ 37,104	$ 401	$ 11,301	$ 4,260,160	$ 4,036,905	$ 223,255
Office Rent	783,989	547,586	21,993	404,082	56,646	11,632	1,196	52,037	236,403	163,508	72,895
Office Costs	507,383	132,069	7,681	80,150	14,617	22,613	2,237	4,771	375,314	351,537	23,777
Professional Services	96,800	51,324	3,261	37,762	8,398	1,725	178		45,476	31,435	14,041
Miscellaneous	-	-							-		
Depreciation	261,176	202,287	1,633	191,775	5,365	1,052	2,462		58,889	50,230	8,659
Total Operating Expenses	$ 6,303,226	$ 1,326,984	**$ 41,949**	**$ 928,753**	**$ 207,573**	**$ 74,126**	**$ 6,474**	**$ 68,109**	$ 4,976,242	$ 4,633,615	$ 342,627
Total Direct Expenses	**$ 15,601,897**	**$ 7,179,844**	**$ 370,389**	**$ 4,658,890**	**$ 1,049,392**	**$ 295,452**	**$ 23,058**	**$ 782,663**	**$ 8,422,053**	**$ 7,020,458**	**$ 1,401,595**
Indirect Expenses	-	-	**49,808**	**575,856**	**127,871**	**26,506**	**2,621**	**(782,663)**			
Other Non-Operating Expenses	-	-	-	-	-	-	-	-	-	-	-
Total Expenses	**$ 15,601,897**	**$ 7,179,844**	**$ 420,197**	**$ 5,234,746**	**$ 1,177,263**	**$ 321,958**	**$ 25,679**	**$ -**	**$ 8,422,053**	**$ 7,020,458**	**$ 1,401,595**
Change in Assets	**$ (582,494)**	**$ (675,006)**	**$ 2,946**	**$ (22,872)**	**$ 5,146**	**$ (433)**	**$ (2,398)**	**$ (657,395)**	**$ 92,512**	**$ 46,088**	**$ 46,424**
Fixed Assets											
Depreciation	$ (261,176)	$ (202,287)	$ (1,633)	$ (191,775)	$ (5,365)	$ (1,052)	$ (2,462)	$ -	$ (58,889)	$ (50,230)	$ (8,659)
Total Fixed Asset Purchases	213,494	184,676	4579	168,903	10,511	619	64		28,818	11,545	17,273
Change in Fixed Assets	**$ 47,682**	**$ 17,611**	**$ (2,946)**	**$ 22,872**	**$ (5,146)**	**$ 433**	**$ 2,398**	**$ -**	**$ 30,071**	**$ 38,685**	**$ (8,614)**
TOTAL CHANGE IN WORKING CAPITAL	**$ (534,812)**	**$ (657,395)**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ (657,395)**	**$ 122,583**	**$ 84,773**	**$ 37,810**

Statement of Financial Position

Statement of Financial Position
2013 Audited, 2014 Projection, 2015 Budget and 2016 Projected

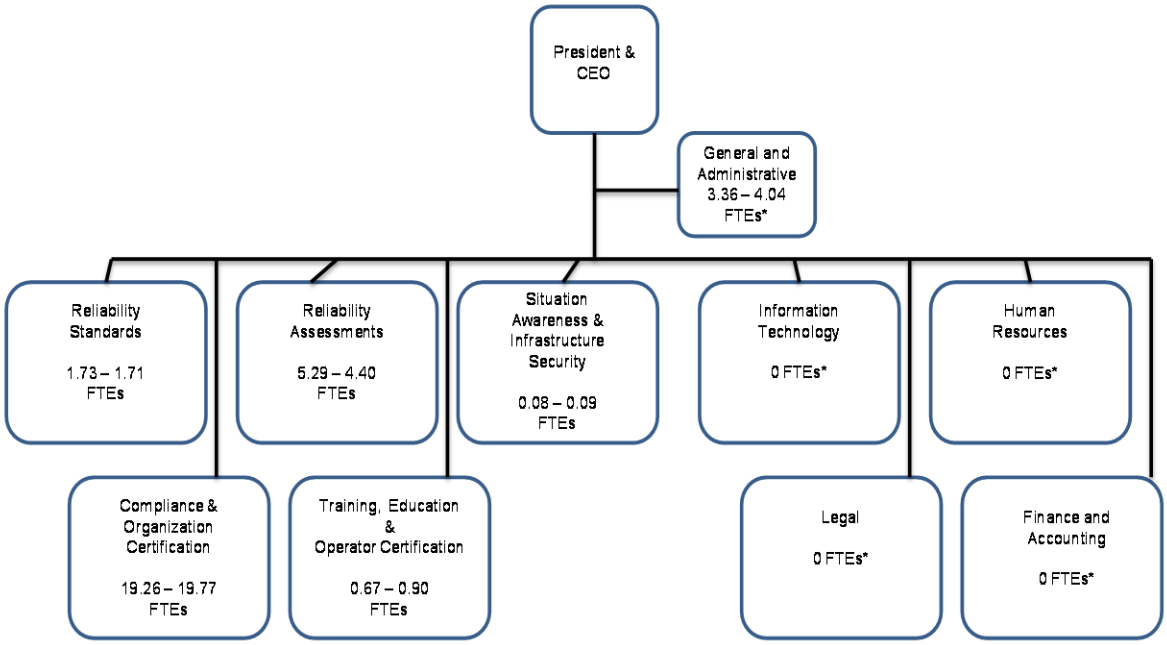
STATUTORY and NON-STATUTORY

	(Per Audit) 12/31/2013	Projected 12/31/2014	Budget 12/31/2015	Projected 12/31/2016
ASSETS				
Cash	6,558,632	4,763,059	3,577,263	3,665,908
Accounts receivable	2,855,070	2,955,070	3,155,070	3,355,070
Other receivables	-	-	-	-
Prepaid expenses and other current assets	18,526	15,000	15,000	15,000
Other Assets	259,175	150,000	150,000	150,000
Property and equipment (net of depreciation)	418,454	300,000	300,000	300,000
Total Assets	**10,109,857**	**8,183,129**	**7,197,333**	**7,485,978**
LIABILITIES AND NET ASSETS				
Liabilities				
Accounts payable and accrued expenses	2,556,119	2,540,000	1,800,000	1,900,000
Deferred income	3,111,955	3,657,736	3,846,312	3,957,406
Compliance Penalty Assessment	481,000	-	-	-
Accrued postretirement benefits obligation	1,406,822	1,477,163	1,551,021	1,628,572
Total Liabilities	**7,555,896**	**7,674,899**	**7,197,333**	**7,485,978**
Net Assets - unrestricted	2,553,961	508,230	-	-
Total Liabilities and Net Assets	**10,109,857**	**8,183,129**	**7,197,333**	**7,485,978**

Statutory Organizational Chart

Florida Reliability Coordinating Council, Inc.
Statutory Organization Chart

2014 Budgeted FTEs 30.40
2015 Budgeted FTEs 30.91



*All FTEs for Information Technology, Legal, Finance, and Human Resources, are recorded within General and Administrative

FRCC
Florida Reliability Coordinating Council, Inc.

FRCC 2015 Business Plan & Budget

(As Submitted to NERC and Posted for Comments on 5/16/2014)

(Not Approved by the FRCC Board of Directors)

NERC and Regional Entity Meeting with the NERC FAC

May 21, 2014

Reva R. Maskewitz - Controller

2015 Regional Entity Division Personnel Comparison

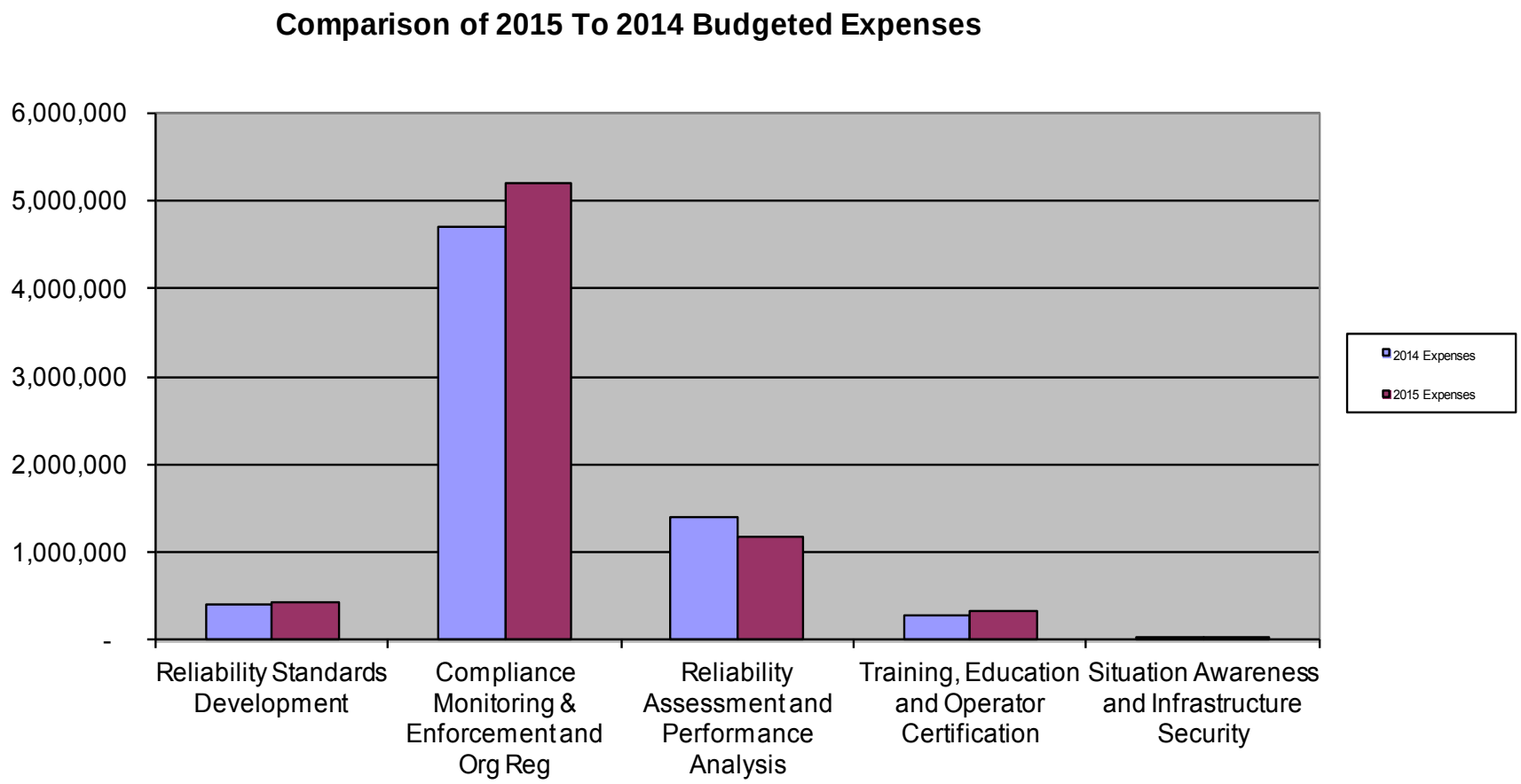
Total FTE's by Program Area	Budget 2014	Projection 2014	Direct FTEs 2015 Budget	Shared FTEs[1] 2015 Budget	Total FTEs 2015 Budget	Change from 2014 Budget
STATUTORY						
Operational Programs						
Reliability Standards Development	1.74	1.33	1.71		1.71	-0.03
Compliance Monitoring & Enforcement and Org Reg	19.26	18.25	19.77		19.77	0.51
Reliability Assessment and Performance Analysis	5.29	4.26		4.40	4.40	-0.89
Training, Education and Operator Certification	0.67	0.50		0.90	0.90	0.23
Situation Awareness and Infrastructure Security	0.08	0.06		0.09	0.09	0.01
Total FTEs Operational Programs	**27.04**	**24.40**	**21.48**	**5.39**	**26.87**	**-0.17**
Administrative Programs						
General & Administrative	3.36	3.57		4.04	4.04	0.68
Total FTEs Administrative Programs	**3.36**	**3.57**	**0.00**	**4.04**	**4.04**	**0.68**
Total FTEs	**30.40**	**27.97**	**21.48**	**9.43**	**30.91**	**0.51**

[1]A shared FTE is defined by NERC as an employee who performs both Statutory and Non-Statutory functions.

2015 RE Division Total Funding by Program Area

	2014	2015	% Change 2015:2014	$ Change 2015:2014
Reliability Standards Development	409,591	423,143	3.3%	13,552
Compliance Monitoring and Enforcement	4,700,708	5,211,874	10.9%	511,166
Reliability Assessment & Performance Analysis	1,391,299	1,182,409	-15.0%	(208,890)
Training, Education and Operator Certification	272,310	321,525	18.1%	49,215
Situational Awareness & Infrastructure Security	19,380	23,281	20.1%	3,901
Total Statutory Expenses & Net Fixed Assets	6,793,288	7,162,232	5.4%	368,944
Funding:				
Total Statutory Funding Assessment	5,488,056	6,237,837	13.7%	749,781
Pass ThruTraining & Education	90,000	90,000	0.0%	-
Pass Thru Software Maintenance	24,000	24,000	0.0%	-
Cash Reserve Refund (Requirement)	848,232	657,395	-22.5%	(190,837)
Penalty Assessment Allocation	343,000	153,000	-55.4%	(190,000)
Total Statutory Funding (Equals Total Expenses)	6,793,288	7,162,232	5.4%	368,944

2015 to 2014 RE Division Comparative Budgeted Funding



2015 RE Division Overview

- The FRCC will continue to evaluate the adequacy of its resources and to evaluate efficiencies in its processes in order to continue to carry out its delegated responsibilities.

- The FRCC will continue to align itself and support the ERO Strategic Plan for goals, activities and major activities which include:
  - Support of the RAI with training and implementation for compliance and enforcement staff.
  - Support NERC's plan to develop RSAW's concurrent with Reliability Standards.
  - Work with NERC and the other RE's to provide guidance to registered entities on CIP V5.
  - Work to refine and revise procedures and processes to eliminate duplication, increase operating efficiencies, enhance ERO-wide consistency and to achieve measurable reliability outcomes.

2015 RE Division Risks

- Roll out of RAI may require significantly more staff time than budgeted
- Compliance Software costs may be higher than budgeted due to RAI or unplanned NERC projects
- Additional costs may be incurred to implement recommendations from the FRCC Security Assessment Initiative
- As always, there could be a Compliance Hearing

2015 Proposed RE Division Working Capital Policy

- Working Capital and operating reserve requirements shall be one (1) month of the total annual budget
- A 1.5 million line of credit is available for short term and other risks that may be needed to bridge budget cycles and approved assessments.
- Working Capital shall be utilized to satisfy projected annual cash flow and cash balance requirements.
- Operating reserves shall be utilized to satisfy known contingencies where the specific timing and amount is uncertain.

FRCC Proposed 2015 Total Budget Compared to 2014

	2015 Budget	2014 Budget	$ Change	% Change
Regional Entity Division Expenses W/Fixed Assets	$ 7,162,233	$ 6,793,289	$368,944	5.4%
Member Services Division Expenses W/Fixed Assets	8,391,982	7,455,995	935,987	12.6%
Total Expenses	$15,554,214	$14,249,283	$1,304,931	9.2%
Other Funding – Workshops & Fees	388,459	391,419	2,960	(0.8%)
Cash Reserve (Requirement)/(Surplus)	534,812	1,110,046	575,234	(51.8%)
Penalty Sanctions	153,000	343,000	190,000	(55.4%)
Total FRCC Funding Assessment	$14,477,943	$12,404,818	$2,073,125	16.7%

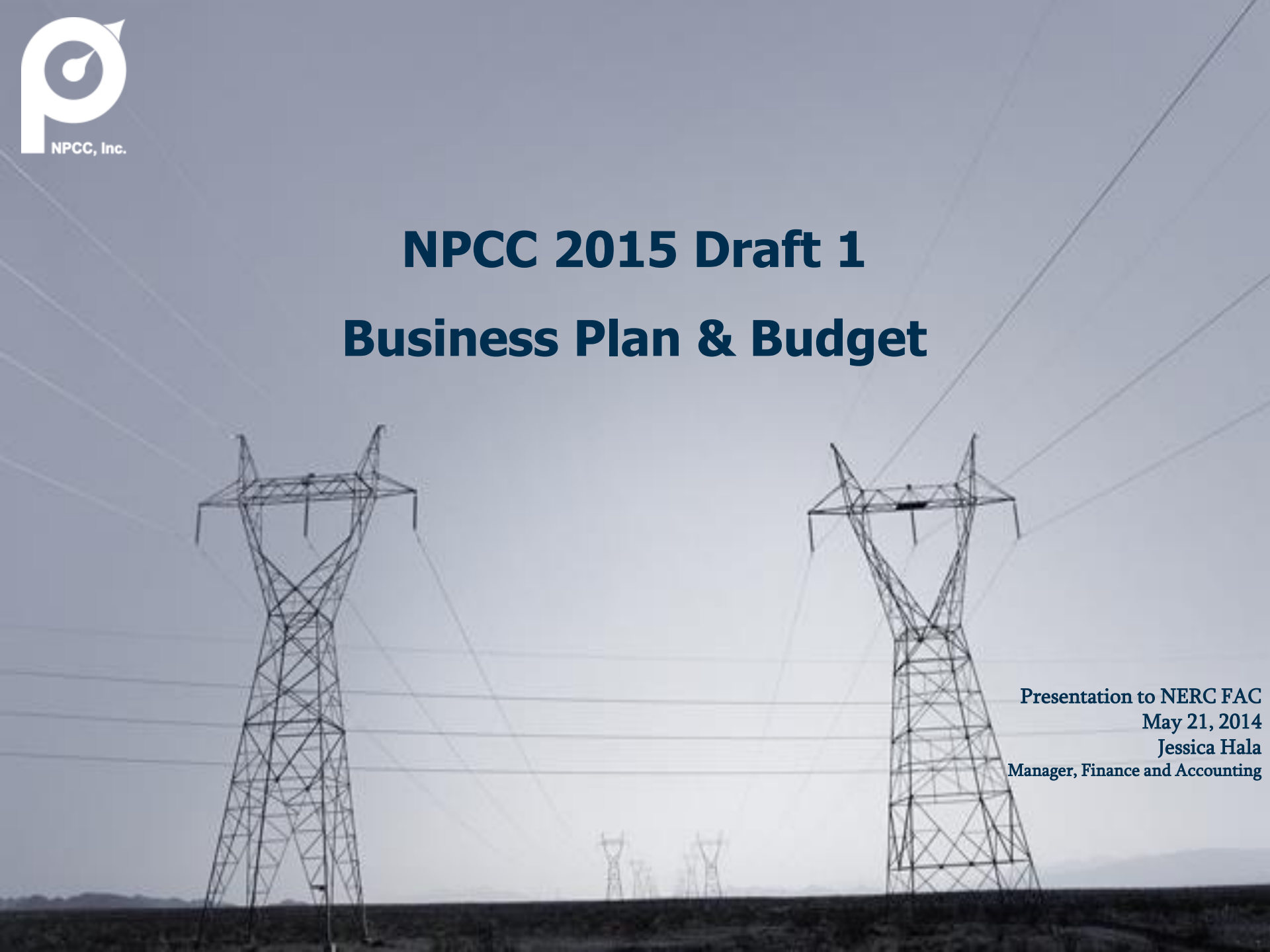
2015 BP&B Summary

- **Regional Entity**
  - Budget increase of 5.4%
  - 0 new Staff
  - 0.5 increased FTEs

- **Member Services**
  - Budget increase of 12.6%
  - 1 new Staff
  - 1.5 increased FTEs

FRCC

QUESTIONS?



NPCC 2015 Draft 1

Business Plan & Budget

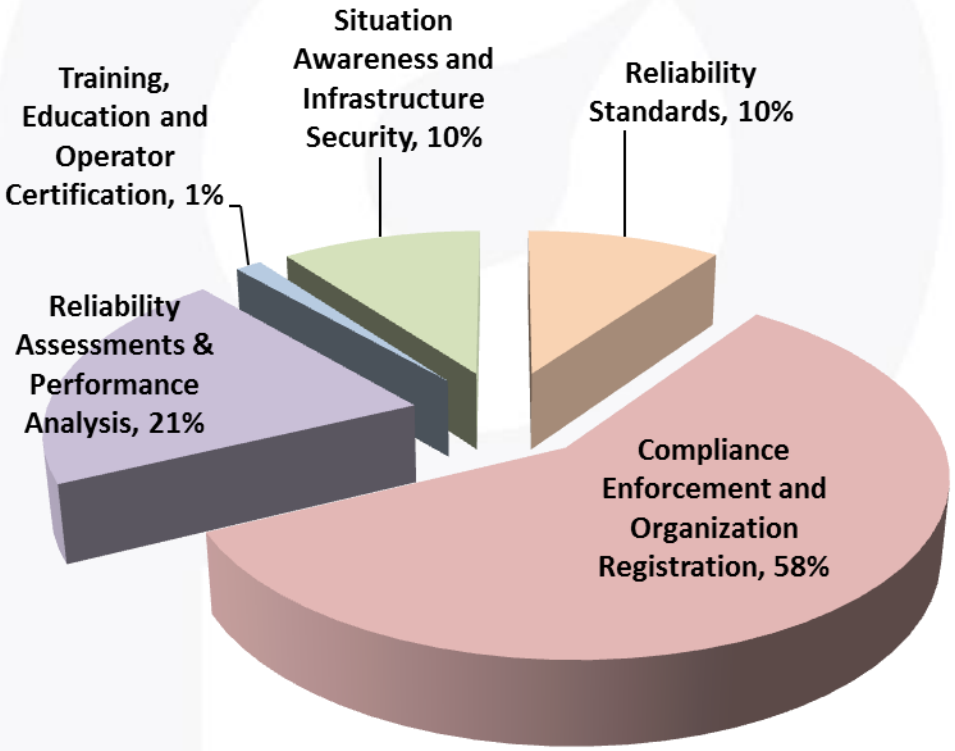
Presentation to NERC FAC
May 21, 2014

Jessica Hala
Manager, Finance and Accounting

2015 Budget Overview

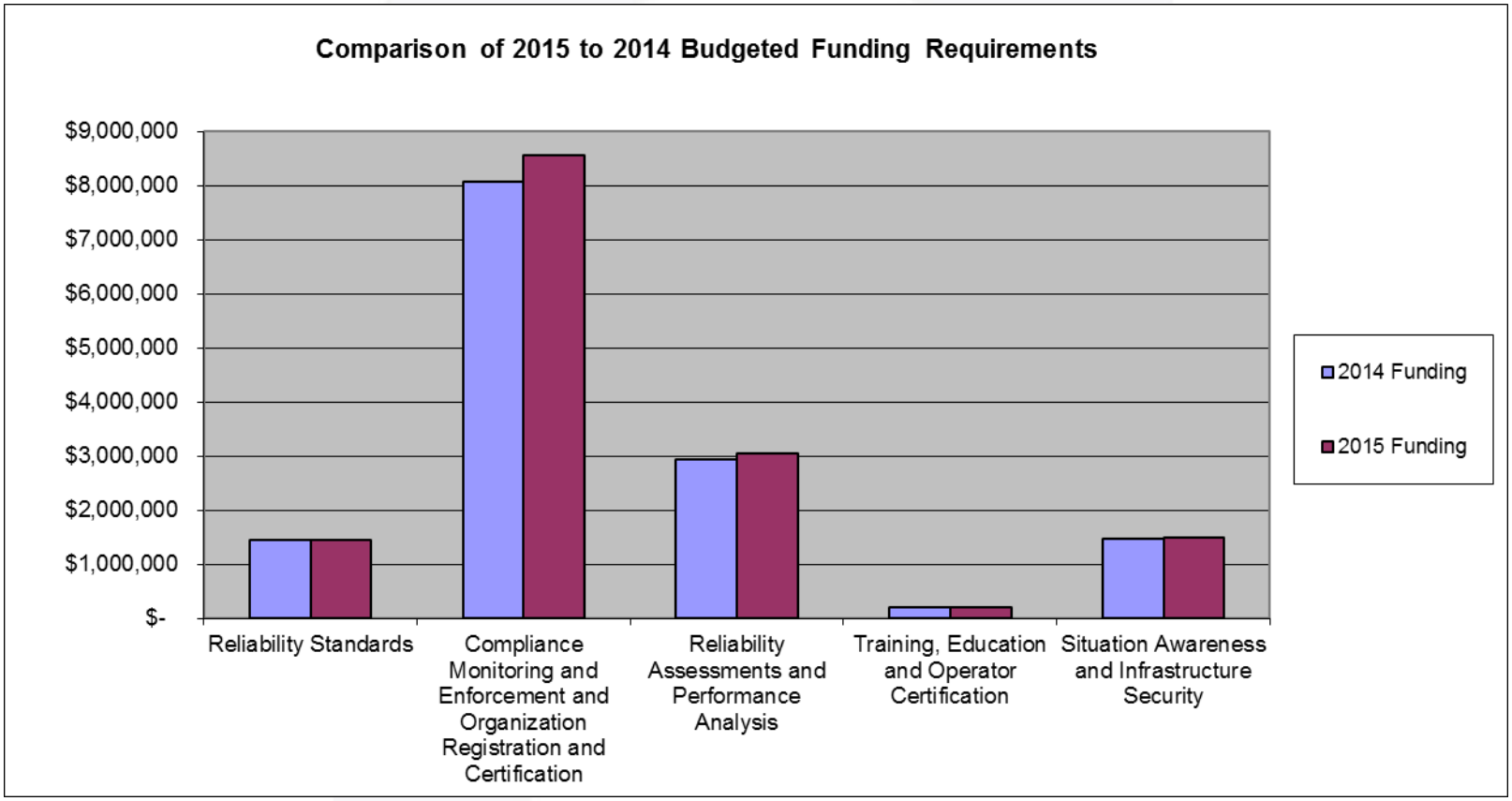
- Staffing Flat
  - 39 FTEs (Regional Entity Division 36.86, Criteria Services Division 2.14)
  - Currently one open position in Standards program area
- Salaries
  - Average wage package increase of 3%
  - Vacancy rate of 2% based on recent trends (currently one open position after 6 months fully staffed)
- Change in Operating Reserves requirement from fixed 8.33% (30 days) to a range between 8.33% and 25.00% (90 days) to provide more stability in annual funding assessments

2015 Total Resources by Program Area Regional Entity (RE) Division



Summary Comparison by Program

Regional Entity (RE) Division



2014-2015 RE Budget Comparison

	2015	2014	Variance	% Variance	Explanation
Funding					
Assessments	14,078,378	13,611,880	466,498	3.43%	
Penalties	281,000	153,000	128,000	83.66%	
Other Income	64,000	64,000	-	0.00%	
Total Funding	14,423,378	13,828,880	594,498		
Expenses					
Personnel Expenses	8,929,241	8,850,160	79,081	0.89%	3% average wage package increase; 2% vacancy rate
Meetings	365,000	365,000	-	0.00%	
Travel	890,000	890,000	-	0.00%	
Conference Calls	45,000	77,000	(32,000)	-41.56%	Lower negotiated rate with a new vendor
Consultants and Contracts	2,342,000	1,924,433	417,567	21.70%	Increase in compliance and RAPA
Rent & Improvements	751,500	737,272	14,228	1.93%	
Office Costs	578,700	536,500	42,200	7.87%	Increase in computer/network maintenance costs
Professional Services	1,025,000	966,500	58,500	6.05%	
Miscellaneous	40,000	80,000	(40,000)	-50.00%	Continuing efforts to control costs
Depreciation	202,019	250,000	(47,981)	-19.19%	Assets becoming fully depreciated in 2014
Indirect Expenses	(409,902)	(405,859)	(4,043)	1.00%	
Other Non-Operating Expenses	-	-	-		
Total Expenses	14,758,558	14,271,006	487,552	3.42%	
Increase(Decrease) in Fixed Assets	19,981	(142,000)	161,981		
Total Budget	14,778,539	14,129,006	649,533	4.60%	
Change in Working Capital	(355,161)	(300,126)	(55,035)		

FTE Comparison

Total FTE's by Program Area	Budget 2014	Projection 2014	Direct FTEs 2015 Budget	Shared FTEs[1] 2015 Budget	Total FTEs 2015 Budget	Change from 2014 Budget
REGIONAL ENTITY DIVISION						
Operational Programs						
Reliability Standards	2.93	2.93	2.00	0.93	2.93	0.00
Compliance Monitoring and Enforcement and Organization Registration and Certification	16.00	16.00	16.00	0.00	16.00	0.00
Training, Education, and Operator Certification	0.10	0.10	0.10	0.00	0.10	0.00
Reliability Assessment and Performance Analysis	5.83	5.83	4.90	0.93	5.83	0.00
Situation Awareness and Infrastructure Security	3.00	3.00	3.00	0.00	3.00	0.00
Total FTEs Operational Programs	**27.86**	**27.86**	**26.00**	**1.86**	**27.86**	**0.00**
Administrative Programs						
Technical Committees and Member Forums	0.50	0.50	0.50	0.00	0.50	0.00
General and Administrative	2.50	2.50	2.50	0.00	2.50	0.00
Information Technology	3.00	3.00	3.00	0.00	3.00	0.00
Legal and Regulatory	1.00	1.00	1.00	0.00	1.00	0.00
Human Resources	1.00	1.00	1.00	0.00	1.00	0.00
Accounting and Finance	1.00	1.00	1.00	0.00	1.00	0.00
Total FTEs Administrative Programs	**9.00**	**9.00**	**9.00**	**0.00**	**9.00**	**0.00**
Total FTEs	**36.86**	**36.86**	**35.00**	**1.86**	**36.86**	**0.00**

[1]A shared FTE is defined as an employee who performs both Regional Entity and Criteria Services division functions.

Resource Adequacy

- Resource assessment and reprioritization from the 2014 Business Plan and Budget has been conducted and will continue through 2015.

- Full impact of Reliability Assurance Initiative (RAI), Risk Assessment, Internal Control Evaluation, and CIP V5 implementation is currently unknown
  - Compliance staffing, in combination with increase in contractors, is expected to be adequate
- Full impact of revised BES definition implementation is currently unknown
  - RAPA staffing, in combination with increase in contractors, is expected to be adequate to address BES identification/exception requests

Process Improvements

- Implementation of CEAP in NERC Standards Development Process
- Utilization of consistent audit checklist and handbook with audits informed by evaluation of entity risk profile
- Enhanced FFT and introduction of compliance exception principles
- Expedited processing of self-reports
- Increased scheduling rigor in settlement processing
- Implementation of efficient BES Notification and Exception Processing
- Improved integration of Events Analysis processing across ERO

Alignment of RE and ERO

- Fully aligned with ERO Enterprise Strategic Plan and Performance Metrics
- Functional initiatives/activities within program areas references applicable ERO goals within the business plan using footnotes
- CS Division continues to support international, interconnected BPS reliability through compliance monitoring with more-stringent, regionally-specific reliability criteria

Efficiency and Controlling Costs

- Ongoing efforts to hold more meetings on site and via conference call or webinar.
- Limiting number of staff attending offsite meetings.
- Continued expansion of pre-audit processing to contain the time required of an audit team to be on-site in order to complete an audit and, therefore, to complete audits more cost-efficiently.

Working Capital and Operating Reserves

- Change in Operating Reserves requirement from fixed 8.33% (30 days) to a range between 8.33% and 25.00% (90 days) to provide more stability in annual funding assessments.

- Working Capital requirement remains unchanged with a targeted level of 8.33% (30 days) of the annual budget.

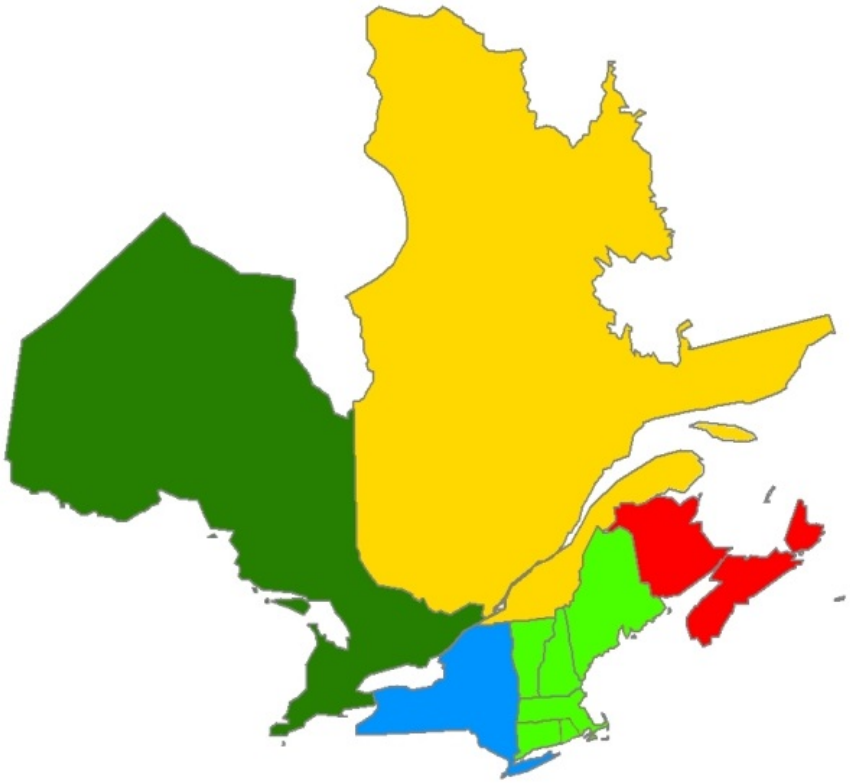
- No utilization of reserves is contemplated; Board authorization would be required

Questions?

NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Northeast Power Coordinating Council, Inc. (NPCC)

Preliminary Draft 2015 Business Plan and Budget



Draft 1
Submitted to NERC
May 14, 2014

Table of Contents

Introduction 3
Personnel Analysis 12
Section A — 2015 Business Plan 15
Reliability Standards Program 15
Compliance Monitoring and Enforcement and Organization Registration and Certification Program 26
Reliability Assessment and Performance Analysis Program 36
Training, Education, and Operator Certification Program 51
Situation Awareness and Infrastructure Security Program 56
Administrative Services 63
Technical Committees and Member Forums 65
General and Administrative 67
Legal and Regulatory 68
Information Technology 69
Human Resources 71
Finance and Accounting 72
Regional Entity Assessment Analysis 74
Section B — Supplemental Financial Information 78
Reserve Balance 78
Breakdown by Statement of Activity Sections 79
Section C —2015 Criteria Services Division Business Plan and Budget 89
Personnel Analysis 96
Reserve Analysis 2014 - 2015 97
Section D 99
Statement of Financial Position 99

Introduction

Total NPCC Resources (in whole dollars)	2015 Budget	U.S.	Canada	Mexico
Regional Entity Division FTEs	36.86			
Criteria Services Division FTEs	2.14			
Total FTEs	**39.0**			
Regional Entity Division Expenses	$14,758,558			
Criteria Services Division Expenses	$1,139,452			
Total Expenses	**$15,898,011**			
Regional Entity Division Inc(Dec) in Fixed Assets	**$19,981**			
Criteria Services Division Inc(Dec) in Fixed Assets	**($10,011)**			
Total Inc(Dec) in Fixed Assets	**$9,970**			
Regional Entity Division Working Capital Requirement**	**($355,161)**			
Criteria Services Division Working Capital Requirement***	**($94,220)**			
Total Working Capital Requirement	**($449,381)**			
Total Regional Entity Division Funding Requirement	$14,423,378			
Total Criteria Services Division Funding Requirement	$1,035,221			
Total Funding Requirement	**$15,458,599**			
Regional Entity Division Assessments	**$14,078,378**	$XXX,XXX	$XXX,XXX	
Regional Entity Division Assessments Percentage	**100.0%**	XX.X%	XX.X%	
Criteria Services Division Membership Fees	**$760,033**	$XXX,XXX	$XXX,XXX	
Total NPCC Assessments & Membership Fees	**$15,113,599**	$XXX,XXX	$XXX,XXX	
NEL	XX	XX	XX	
NEL %	100%	XX.XX%	XX.XX%	

** Refer to Table B-1 on page 78 in Section B.
*** Refer to the Reserve Analysis on page 97 in Section C.

2015 Overview of Total NPCC Resource Requirements

Due to the international nature of NPCC, the total resource requirements including both Regional Entity division and Criteria Services division are identified above. The individual divisional explanations are contained in subsequent sections.

NPCC proposes to increase its total funding requirement from $14,818,588 to $15,458,599 in 2015, an increase of $640,011 or 4.3%. The proposed 2015 funding requirements will be satisfied by a Regional Entity division assessment of $14,078,378 and Criteria Services division fees of $1,035,221, an overall increase of 3.5% compared to the 2014 total assessments and fees of $14,601,588. NPCC believes that the Region remains an effective provider of Regional Entity and Criteria Services division functions. NPCC's corporate culture centers on consistent delivery of excellent results at a cost that is considerate of the longstanding tradition in the Northeast of affordable and reliable electricity.

Organizational Overview

Northeast Power Coordinating Council, Inc. (NPCC) is a 501(c)(6) not-for-profit corporation in the state of New York responsible for promoting and improving the reliability of the international, interconnected bulk power systems in Northeastern North America through (i) the development of Regional Reliability Standards and compliance assessment and enforcement of continent-wide and Regional Reliability Standards, coordination of system planning, design and operations, and assessment of reliability (collectively, Regional Entity activities), and (ii) the establishment of Regionally-specific criteria, and monitoring and enforcement of compliance

with such criteria (collectively, criteria services activities). NPCC provides the functions and services for Northeastern North America of a cross-border Regional Entity through a Regional Entity division, as well as Regionally-specific criteria services for Northeastern North America through a criteria services division. NPCC's website is www.npcc.org.

The NPCC Region covers nearly 1.2 million square miles and is populated by more than 56 million people. NPCC U.S. includes the six New England states and the state of New York. NPCC Canada includes the provinces of Ontario, Québec and the Maritime provinces of New Brunswick and Nova Scotia. In total, from a net energy for load perspective, NPCC is approximately 45% U.S. and 55% Canadian. With regard to Canada, approximately 70% of Canadian net energy for load is within the NPCC Region.

Effective January 1, 2012, NPCC executed an Amended and Restated Regional Delegation Agreement with the North American Electric Reliability Corporation (NERC) that delegates to NPCC certain responsibilities and authorities of a cross-border Regional Entity as defined by *Section 215* of the Federal Power Act in the U.S. In addition, NPCC has executed Memoranda of Understanding or Agreements with Canadian provincial regulatory and/or governmental authorities in Ontario, Québec, New Brunswick and Nova Scotia.

In this 2015 business plan, NPCC has included activities consistent with NERC initiatives including the implementation of the revised BES definition, risk-based registration, the Reliability Assurance Initiative, and expanded training for compliance auditing.

It is imperative that NPCC maintain its ability to carry out delegated authorities and responsibilities. NPCC has a flat 2015 targeted staffing level of 39 power industry professionals and support personnel. Details of the 2015 business plans and budget for each program area are included in Section A for the Regional Entity division. The 2015 Regional Entity division schedules are shown in Section B. Section C details the 2015 criteria services division business plan and budget.

Membership and Governance

NPCC monitors approximately 300 registered entities and some 602 functions in the Region for compliance with mandatory Reliability Standards. NPCC currently has approximately 78 members. There are two categories of membership, General and Full. The two categories distinguish between Regional Entity delegated services that are provided in support of the U.S. FERC and Canadian provincial MOUs or Agreements with regulatory and/or governmental authorities, and Criteria Services which FERC references as U.S. non-delegated activities.

General Membership is voluntary and is open to any person or entity, including any entity participating in the Registered Ballot Body of the Electric Reliability Organization (ERO) that has an interest in the reliable operation of the Northeastern North American bulk power system. General Members which are also registered entities within the NPCC Region are subject to compliance with Reliability Standards, consistent with their registration, and also receive additional services from the Regional Entity division of NPCC.

Full Membership is available to Members which are already General Members and participate in electricity markets in the Northeast. Independent system operators (ISOs), Regional transmission organizations (RTOs), Transcos and other organizations or entities that perform the Balancing Authority function operating in Northeastern North America are expected to be Full Members of NPCC. The New York State Reliability Council and any other sub-regional

reliability councils which may be formed are also expected to be Full Members. Full Members are subject to compliance with Regionally-specific more stringent reliability criteria for their generation and transmission facilities on which faults or disturbances can have a significant adverse impact outside of the local area and which are identified utilizing a reliability impact-based methodology, in addition to Reliability Standards, and receive additional services from the Criteria Services division of NPCC, which is not funded through the ERO.

Since January 1, 2012 NPCC is governed by a Board of Directors consisting of seven stakeholder voting sectors consisting of a maximum of two directors per sector, an independent sector consisting of two independent directors, an independent Board Chair with voting rights to preclude board deadlocks, and the President and CEO. Within NPCC, no two sectors can control and no one sector can block action. The voting sectors on the NPCC Board of Directors include:

Sector 1) Transmission Owners
Sector 2) Reliability Coordinators
Sector 3) Transmission Dependent Utilities, Distribution Companies, Load Serving Entities
Sector 4) Generator Owners
Sector 5) Marketers, Brokers and Aggregators
Sector 6) Regulators
Sector 7) Sub-Regional Reliability Councils, Customers, other Regional Entities and Interested Entities
Sector 8) Independent

A Finance and Audit Committee (FAC), a Pension Committee (PC), a Corporate Governance and Nominating Committee (CGNC), and a Management Development and Compensation Committee (MDCC) advise the Board on finance, governance, compensation and human resource matters. The Board endorses a non-employee, Certified Public Accountant for election by the NPCC Members as Treasurer of the corporation. The Treasurer chairs the FAC and works with the Chief Operating Officer who provides oversight of the finances of the corporation. The Treasurer reports to the Board on the corporation's financial position, on FAC activities, on tax code requirements, and on independent annual audit results and accounting practices.

The Regional Standards Committee (RSC), the Compliance Committee (CC), the Reliability Coordinating Committee (RCC), and the Public Information Committee, consistent with their approved scopes, are responsible for various reliability issues. The RSC, CC and RCC also provide technical policy recommendations to the Board. All General and Full Members are eligible for representation on the technical committees.

Industry technical experts from within the membership provide valuable input to the Board through various working groups and task forces as well as the committees. The *Amended and Restated Bylaws* establishes NPCC's independence from users, owners and operators of the bulk power system through the enhanced governance structure while providing fair stakeholder representation in the election of the Board of Directors and officers. The members, from each of the seven stakeholder voting sectors, vote to elect directors in their respective sector. The *Amended and Restated Bylaws* establish criteria for board service for both stakeholder and independent directors. Independent Directors are drawn from diverse backgrounds and possess a broad range of industry expertise, perspectives, experiences, skill sets and knowledge to contribute to the effective functioning of a hybrid board structure.

Compliance and enforcement activities are carried out by the NPCC compliance staff and are independent of all users, owners and operators of the international bulk electric system. Compliance activities are governed in the United States by the *Amended and Restated Regional Delegation Agreement* between NERC and NPCC, delegating portions of NERC's authority as the ERO to NPCC. NPCC compliance activities in Canada are governed by an individual provincial Memorandum of Understanding (MOU) or Agreements with each province providing the unique parameters for compliance and enforcement activities for each of the provinces. A MOU between the Independent Electricity System Operator in Ontario (IESO), NERC and NPCC establishes roles and responsibilities with regard to that province. NPCC, NERC and the New Brunswick Energy and Utilities Board are parties to a MOU that sets forth reliability activities for New Brunswick. The Régie de l'énergie, NERC and NPCC executed an Agreement regarding the development of electric power transmission Reliability Standards and a program for the monitoring of the application of these standards for Québec. NPCC, NERC and Nova Scotia executed a MOU that sets forth the mutual understanding of the parties in relation to the approval and implementation of NERC Reliability Standards and NPCC Regional reliability criteria for the province of Nova Scotia.

International Foundation

The Regional Entity functions and services differ according to particular regulatory backstop:

a) U.S. Foundation

The Federal Energy Regulatory Commission (FERC) certified NERC as the Electric Reliability Organization (ERO) on July 20, 2006. The ERO is responsible for developing and enforcing reliability standards within the United States. In executing part of its responsibilities, NERC delegates authority to the Regional Entities to perform certain functions through delegation agreements. Ensuring the reliability of the bulk power system in the state of New York and the six New England States was delegated from NERC to NPCC through the Amended and Restated Regional Delegation Agreement.

b) Ontario

On February 5, 2010, NERC, NPCC and the IESO amended and restated their earlier MOU, dated November 29, 2006, setting forth their mutual understanding as regards NERC's and NPCC's status in Ontario with respect to standard and criteria development, compliance enforcement, and other related matters. The IESO, whose statutory responsibilities include making and enforcing reliability standards, and making and enforcing Ontario market rules that govern the IESO-controlled grid and the wholesale electricity market, was established April 1, 1999 as the Independent Electricity Market Operator in Ontario under the *Electricity Act, 1998* (Ontario). The IESO is subject to the regulatory oversight of the Ontario Energy Board (OEB).

Among other things, the MOU recognizes that NERC and NPCC are standards authorities under the *Electricity Act, 1998* (Ontario). Additionally, under the authority of that same legislation, and as memorialized in the MOU, the NERC reliability standards and NPCC reliability criteria have effect in Ontario. However a 2008 amendment to the Electricity Act, 1998 (Ontario) allows the OEB to review these standards and criteria and issue orders preventing their implementation and remanding them back to NERC and NPCC.

The IESO is subject to compliance monitoring and enforcement by NPCC. The IESO is also subject to compliance monitoring and enforcement of the Ontario market rules by the IESO's Market Assessment and Compliance Division (MACD) that operates at arm's length from the IESO's business units. The MOU notes that where MACD, NERC, and NPCC engage in

investigations pursuant to their respective mandates regarding compliance, MACD can request to take the lead. Moreover, of the three, MACD is the only entity that can assess financial penalties for any Ontario market participant's or the IESO's non-compliance with Ontario market rules, which includes non-compliance with NERC standards and NPCC criteria.

The MOU provides for a peer review process to promote the common compliance and enforcement objectives of NERC/NPCC and MACD. From the perspective of NPCC and NERC, this process, in part, is meant to assure registered entities outside of Ontario that the MACD program is rigorous, thorough and reliable.

The IESO is subject to NPCC assessments of compliance, including audits, as well as NPCC remedial action directives to correct non-compliance. In the event that the IESO disagrees with NPCC's finding of a violation or associated assessment of sanctions in connection with standards and criteria, the IESO has a right to a compliance hearing with NPCC.

c) Québec

The Régie de l'énergie, NERC and NPCC are parties to the May 8, 2009 *Agreement on the Development of Electric Power Transmission Reliability Standards and of Procedures and a Program for the Monitoring of the Application of These Standards for Québec* (the Agreement). Under the terms of the Agreement, the Régie de l'énergie , which is charged with ensuring the reliability of the electric transmission in Québec, retained NPCC and NERC as experts to develop reliability standards and monitoring program procedures for the Province.

The Régie de l'énergie is a public body established by the *Act respecting the Régie de l'énergie* (the Act). Pursuant to its authority under the Act, the Régie de l'énergie, through a series of decisions in 2007, designated Hydro-Québec TransÉnergie (HQTE) as the Reliability Coordinator for Québec. In accordance with its mandate and as recognized in the Agreement, it is this entity that is responsible for the filing with the Régie de l'énergie for approval of reliability standards in Québec. HQTE has filed for the approval of certain reliability standards and the Régie de l'énergie has begun the proceedings required to make such reliability standards mandatory in Québec.

The Agreement contemplates the execution of a second agreement that will detail the mandates granted by the Régie de l'énergie to NPCC and NERC with respect to the implementation of the procedures and program for the monitoring of the application of electric power transmission Reliability Standards in Québec and the provision of opinions and recommendations to the Régie in this regard. The second agreement is currently being negotiated by the Régie de l'énergie, NPCC and NERC. The intent, once all the appropriate authorizations are in place, is that NPCC and NERC will act as the Régie's agents in all compliance monitoring and enforcement activities through the implementation of a Québec specific compliance monitoring and enforcement program.

Currently, as there are only a limited number of mandatory standards that have come into effect, and as the second agreement and all the appropriate authorizations covering compliance monitoring and enforcement arrangements are not in place, there has been limited mandatory compliance activity under the formal Québec regime. However, the Hydro-Québec companies, including Hydro-Québec TransÉnergie and Hydro-Québec Production have been subject to voluntarily compliance monitoring, including comprehensive audits by NPCC. Additionally, NPCC has and continues to proceed with its reliability assurance activities within Québec,

including but not limited to events analysis, Reliability Assessment and Performance Analysis and compliance investigations, consistent with the NPCC *Amended and Restated Bylaws*.

d) New Brunswick

The New Brunswick Energy and Utilities Board ("EUB") and NPCC entered into an Agreement dated October 1, 2013, whereby NPCC provides services for the EUB. The EUB is a not-for-profit corporation which was established on October 1, 2004 under the Electricity Act (NB) and charged with developing and administering the wholesale electricity market and maintaining reliability of the integrated power system in New Brunswick.

Effective October 1, 2013, the Electricity Act (NB) and implementing regulations (together, "NB Electricity Act") amended how Reliability Standards are approved, monitored, and enforced in the province of New Brunswick. The NB Electricity Act designates NPCC as a compliance body and NERC as a standards body within the meaning of the NB Electricity Act. The October 1, 2013 Agreement between NPCC and the EUB is intended to be the preliminary step with respect to the implementation of the NB Electricity Act.

With respect to the approval of reliability standards, the NB Electricity Act provides that all of the NERC Reliability Standards that were effective in New Brunswick prior to October 1, 2013 continue to be effective in New Brunswick after October 1, 2013. Additionally, the New Brunswick Power Corporation (formed from several amalgamating corporations) ("NBPC") is required to file for approval, modification, or retirement of NERC Reliability Standards 60 days after a NERC Reliability Standard is approved, modified, or retired by the Federal Energy Regulatory Commission ("FERC"). The EUB rules on the filed Reliability Standard after considering (a) the potential impact on the reliability of the bulk power system, (b) the potential cost and benefits (c) the public interest, and (d) any other factors that the NBUEB considers relevant. The Electricity Act requires the NBEUB to notify NPCC and NERC of an application by the NBPC with respect to reliability standards and provide for a 60 day comment period. The NBEUB is required to approve the reliability standards if there are not substantive modifications proposed from the FERC approved NERC Reliability Standard and there were no substantive comments filed. Amendments to the reliability standard to make them compatible with New Brunswick or Canadian law are considered non-substantive. The approval of reliability standards may be subject to a hearing for several reasons, including substantive comments from NPCC or NERC.

With respect to the monitoring and enforcement of the Reliability Standards in New Brunswick, the NB Electricity Act requires NPCC to identify entities that must register with the EUB in the New Brunswick specific registry. Additionally, NPCC is required to carry out the compliance monitoring and assessment for the EUB and assist and advise the enforcement for the EUB, including financial penalties. NPCC is also permitted to carry out or exercise any power in the implementing regulations that is specific to the EUB. Additionally, NPCC has the powers of an inspector, which permits NPCC to audit and spot check entities within New Brunswick.

e) Nova Scotia

Nova Scotia Power Incorporated (NSPI), NPCC and NERC are parties to a May 11, 2010 Memorandum of Understanding regarding the approval and implementation of mandatory NERC reliability standards and NPCC Regional reliability criteria. Pursuant to the MOU's terms, NERC and NPCC filed standards and criteria with the Nova Scotia Utility and Review Board (NSUARB) for approval on June 30, 2010 and June 29, 2010, respectively. A decision from the NSUARB on both NERC and NPCC filings was rendered on July 20, 2011. Hence, the

standards and criteria are mandatory in Nova Scotia and NSPI will be subject to the NERC compliance monitoring and enforcement program, as implemented by NPCC.

NPCC will conduct compliance activities with respect to the standards and then forward any non-compliance information and recommendations to the NSUARB for use in enforcement proceedings. Enforcement will be administered by the NSUARB which will, among other things, determine whether a violation has occurred and, if so, what remedial measures or non-monetary penalties should be imposed.

Regional Entity Division Functional Scope

NPCC's Regional Entity division functions in support of the ERO include:

- Active participation in the development of North American Reliability Standards for the bulk electric system, and as needed development of Reliability Standards applicable within the NPCC cross-border Regional Entity
- Monitoring and enforcement of approved Reliability Standards, including the registration of responsible entities, and as needed certification of such entities
- Assessment of the present and future reliability of the bulk power system
- Operational coordination and situation awareness support
- Event analysis and identifying lessons learned to improve reliability
- Effective training and education of reliability personnel
- Promoting the protection of critical electric infrastructure

In recognition of the delegated compliance role of Regional Entities as an important means to enhancing reliability, NPCC has designated a significant percentage of its staff resources to compliance monitoring and enforcement. NPCC has also developed and deployed a robust set of online tools for gathering data, analysis, and tracking of compliance information to support its ability to carry out its responsibilities in a cost effective manner.

NPCC has organized the remaining staff into program areas consistent with EPAct 2005 to address the other functions listed above. These experts in operations, planning and reliability analysis assist registered entities in assessing and improving reliability. It is in support of these areas that NPCC engages the majority of industry experts on its technical committees.

2015 Key Assumptions and 2015 Goals and Key Deliverables

NERC and the eight Regional Entities collaborated in the development of a common operating model with complementary roles and responsibilities, an ERO Enterprise Strategic Plan, and a set of business planning assumptions, goals, metrics and key deliverables for the 2014 through 2017 period. The results from that collaboration are included as a set of Shared Business Plan and Budget Assumptions that will be contained in Exhibit A to the NERC 2015 Business Plan and Budget and may be referenced by the users of this document. In each of the following program area sections footnotes are used to reference the specific ERO Enterprise Goals that NPCC's activities support.

2015 Overview of Regional Entity Division Cost Impacts

NPCC proposes to increase its Regional Entity division funding requirement from $13,828,880 to $14,423,378 in 2015, an increase of $594,498 or 4.3%. The proposed Regional Entity division assessment of $14,078,378 to support the budget is an increase of 3.4% compared to the 2014 assessment of $13,611,880.

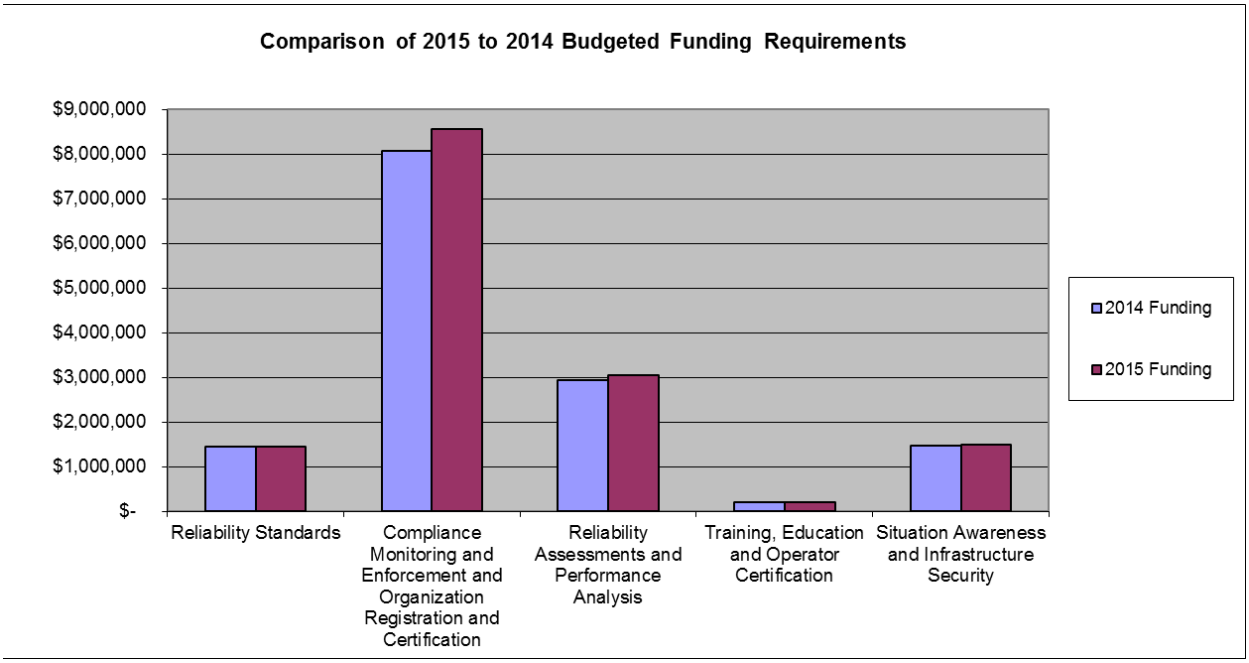
2014 Projections

Current year projections are taken into consideration in development of the budget. Expenses are currently projected to be on budget or slightly under budget in all areas. 2014 Projections reflect expectations based on the first quarter statement of activities. It is anticipated that projections could change throughout 2014 and would be reflected in each subsequent quarter's statement of activities.

Summary by Program

Program	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Reliability Standards	$ 1,447,330	$ 1,447,330	$ 1,456,129	$ 8,799	0.6%
Compliance Monitoring and Enforcement and Organization Registration and Certification	$ 8,079,371	$ 8,079,371	$ 8,568,145	$ 488,774	6.0%
Reliability Assessments and Performance Analysis	$ 2,942,339	$ 2,942,339	$ 3,053,923	$ 111,585	3.8%
Training, Education and Operator Certification	$ 195,855	$ 195,855	$ 199,010	$ 3,154	1.6%
Situation Awareness and Infrastructure Security	$ 1,464,111	$ 1,464,111	$ 1,501,332	$ 37,221	2.5%
Total	$ 14,129,006	$ 14,129,006	$ 14,778,539	$ 649,533	4.6%

This chart does not include allocation of working capital requirements among the Program Areas.



This chart does not include allocation of working capital requirements among the Program Areas.

Personnel Analysis

Total FTE's by Program Area	Budget 2014	Projection 2014	Direct FTEs 2015 Budget	Shared FTEs[1] 2015 Budget	Total FTEs 2015 Budget	Change from 2014 Budget
REGIONAL ENTITY DIVISION						
Operational Programs						
Reliability Standards	2.93	2.93	2.00	0.93	2.93	0.00
Compliance Monitoring and Enforcement and Organization Registration and Certification	16.00	16.00	16.00	0.00	16.00	0.00
Training, Education, and Operator Certification	0.10	0.10	0.10	0.00	0.10	0.00
Reliability Assessment and Performance Analysis	5.83	5.83	4.90	0.93	5.83	0.00
Situation Awareness and Infrastructure Security	3.00	3.00	3.00	0.00	3.00	0.00
Total FTEs Operational Programs	**27.86**	**27.86**	**26.00**	**1.86**	**27.86**	**0.00**
Administrative Programs						
Technical Committees and Member Forums	0.50	0.50	0.50	0.00	0.50	0.00
General and Administrative	2.50	2.50	2.50	0.00	2.50	0.00
Information Technology	3.00	3.00	3.00	0.00	3.00	0.00
Legal and Regulatory	1.00	1.00	1.00	0.00	1.00	0.00
Human Resources	1.00	1.00	1.00	0.00	1.00	0.00
Accounting and Finance	1.00	1.00	1.00	0.00	1.00	0.00
Total FTEs Administrative Programs	**9.00**	**9.00**	**9.00**	**0.00**	**9.00**	**0.00**
Total FTEs	**36.86**	**36.86**	**35.00**	**1.86**	**36.86**	**0.00**

[1]A shared FTE is defined as an employee who performs both Regional Entity and Criteria Services division functions.

2014 Budget and Projection and 2015 Budget Comparisons

Statement of Activities and Capital Expenditures
2014 Budget & Projection, and 2015 Budget

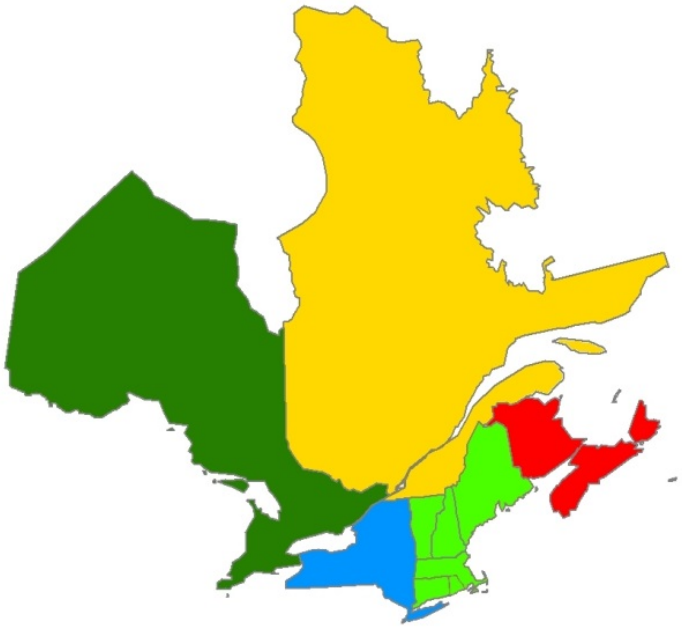
REGIONAL ENTITY DIVISION

		2014 Budget	2014 Projection	Variance[2] 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding						
ERO Funding						
	ERO Assessments	$ 13,611,880	$ 13,611,880	$ -	$ 14,078,378	$ 466,498
	Penalty Sanctions[1]	153,000	153,000	-	281,000	128,000
Total ERO Funding		**$ 13,764,880**	**$ 13,764,880**	**$ -**	**$ 14,359,378**	**$ 594,498**
	Membership Dues	-	-	-	-	-
	Testing Fees	-	-	-	-	-
	Services & Software	-	-	-	-	-
	Workshops	64,000	64,000	-	64,000	-
	Interest	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
Total Funding (A)		**$ 13,828,880**	**$ 13,828,880**	**$ -**	**$ 14,423,378**	**$ 594,498**
Expenses						
Personnel Expenses						
	Salaries	$ 5,911,227	$ 5,911,227	$ -	$ 6,195,425	$ 284,198
	Payroll Taxes	384,311	384,311	-	387,209	2,898
	Benefits	1,430,261	1,430,261	-	1,256,595	(173,666)
	Retirement Costs	1,124,361	1,124,361	-	1,090,013	(34,348)
Total Personnel Expenses		**$ 8,850,160**	**$ 8,850,160**	**$ -**	**$ 8,929,241**	**$ 79,081**
Meeting Expenses						
	Meetings	$ 365,000	$ 365,000	$ -	$ 365,000	$ -
	Travel	890,000	890,000	-	890,000	-
	Conference Calls	77,000	77,000	-	45,000	(32,000)
Total Meeting Expenses		**$ 1,332,000**	**$ 1,332,000**	**$ -**	**$ 1,300,000**	**$ (32,000)**
Operating Expenses						
	Consultants & Contracts	$ 1,924,433	$ 1,924,433	$ -	$ 2,342,000	$ 417,567
	Office Rent	737,272	737,272	-	751,500	14,228
	Office Costs	536,500	536,500	-	578,700	42,200
	Professional Services	966,500	966,500	-	1,025,000	58,500
	Computer & Equipment Leases	-	-	-	-	-
	Miscellaneous	80,000	80,000	-	40,000	(40,000)
	Depreciation	250,000	250,000	-	202,019	(47,981)
Total Operating Expenses		**$ 4,494,705**	**$ 4,494,705**	**$ -**	**$ 4,939,219**	**$ 444,514**
	Total Direct Expenses	**$ 14,676,865**	**$ 14,676,865**	**$ -**	**$ 15,168,460**	**$ 491,595**
Indirect Expenses		**$ (405,859)**	**$ (405,859)**	**$ -**	**$ (409,902)**	**$ (4,043)**
Other Non-Operating Expenses		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)		**$ 14,271,006**	**$ 14,271,006**	**$ -**	**$ 14,758,558**	**$ 487,552**
Change in Assets		**$ (442,126)**	**$ (442,126)**	**$ -**	**$ (335,180)**	**$ 106,946**
Fixed Assets						
	Depreciation	$ (250,000)	$ (250,000)	$ -	$ (202,019)	$ 47,981
	Computer & Software CapEx	108,000	108,000	-	222,000	114,000
	Furniture & Fixtures CapEx	-	-	-	-	-
	Equipment CapEx	-	-	-	-	-
	Leasehold Improvements	-	-	-	-	-
	Allocation of Fixed Assets	(0)	(0)	-	(0)	-
Inc(Dec) in Fixed Assets (C)		**(142,000)**	**(142,000)**	**-**	**19,981**	**161,981**
TOTAL BUDGET (=B+C)		**$ 14,129,006**	**$ 14,129,006**	**$ -**	**$ 14,778,539**	**$ 649,533**
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)		**$ (300,126)**	**$ (300,126)**	**$ -**	**$ (355,161)**	**$ (55,035)**

[1] $281,000 of penalty sanctions collected to date and prior to June 30, 2014.

[2] 2014 Projections reflect expectations based on the 1st quarter statement of activities. It is anticipated that projections could change throughout 2014 and would be reflected in each subsequent quarter's statement of activities.

Section A – Regional Entity Division
2015 Business Plan and Budget



Section A — 2015 Business Plan

Reliability Standards Program

Reliability Standards Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	2.93	2.93	0.00
Direct Expenses	$917,936	$905,638	($12,299)
Indirect Expenses	$555,686	$561,221	$5,535
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	($26,292)	($10,729)	$15,563
Total Funding Requirement	$1,447,330	$1,456,129	$8,799

Program Scope and Functional Description

The NPCC Reliability Standards program operates in accordance with NPCC's filed and approved Delegation Agreement "Exhibit C", and NERC Rules of Procedure Section 300. The program supports the ERO standards program area roles and responsibilities by providing supporting activities for the development of clear, concise, sustainable, high quality and technically sound mandatory "results based" reliability standards which provide for an adequate level of reliability in a timely and efficient manner. The primary objective of NPCC's program area is to support the development of ERO standards which establish threshold requirements for ensuring the bulk electric system is planned, operated, and maintained in a manner that minimizes risks of cascading failures, avoids damage to major equipment, is responsive to risks, or limits interruptions of bulk power supply. At a Regional level, the program develops Regional Reliability Standards and ensures that Regional reliability criteria, contained in the form of Directories, are not inconsistent with any applicable NERC and Regional Reliability Standards. The NPCC Reliability Standards program also supports and participates in the development, revision, and maintenance of NERC Reliability Standards, initiates new regional or continent wide reliability standards when necessary, and provides a forum for the comprehensive review and improvement of existing and developing standards.

The NPCC Reliability Standards Program Area supports the reliability of the bulk electric system by:

- Facilitating active participation of NPCC Regional industry stakeholders in all NERC Reliability Standards activities to promote the development of results based, cost effective quality standards in a timely and efficient manner.
- Promote awareness by holding workshops and conducting Regional Standards Committee meetings to inform and educate stakeholders.
- Internally and informally training staff for the new and developing standards through meetings.
- Regional coordination activities with Standards Program Areas from other Regions.

- Development and maintenance of Regional Standards as necessary to address Regional reliability related issues or risks and ensure those standards are not inconsistent with the NERC continent wide standards. These Regional standards contain requirements that are more stringent, add specificity to or augment the NERC Continent-wide standards.
- NPCC maintains and abides by the NPCC Regional Standards Processes Manual assuring compliance with all FERC filed documents with respect to standards development.

Funding Drivers and Reliability Benefits

- Expanded Scope of Standards activities
    - Utilize NPCC RSC, Task Forces and Working Groups to comment on developing NERC Standards to ensure they are results based and directionally consistent with the Independent Experts Review Panel Report (IERP)[1]
    - Develop process for ensuring lessons learned from Event Analysis are evaluated for any gaps in standards or criteria[2]
    - Responding to increasing amount of FERC Rulings, NOPRs, preliminary staff assessments, and FERC issued Directives[3]
    - Providing support for increased standard development activities as outlined in the NERC 2014-2016 Reliability Standards Development Plan and assuming an active role in the newly formed NERC Project Management Oversight Subcommittee ("PMOS")
    - Participating in informal activities of standards development to promote consensus early in project development and provide technical guidance
    - Providing a forum for all NPCC representatives on the NERC drafting teams
    - Actively coordinating and reviewing Reliability Standards Audit Worksheets (RSAW) for correctness
    - Provide NPCC Regional point of contact for the new Reliability Issues Steering Committee ("RISC") to provide emerging and existing BES reliability related risks and potential gaps in the existing NERC standards
- Increased Number of Standards Projects
    - Active NERC Projects in the standards area are also expected to increase to address FERC outstanding directives.
    - The concept of informal development was introduced in 2013 and will be expanded to include more standards development projects in 2015 requiring more technical support, participation, and facilitation.
    - NERC has developed procedures and processes to allow it to revise standards in a more expeditious manner that may need clarification or address some deficiency.
    - NPCC is assisting with the Project Management Oversight Subcommittee (PMOS) which is responsible for managing the development of NERC standards projects and tracking Paragraph 81 Phase 2 retirement candidates

[1] In support of ERO Goal 1a Develop Standards which are clear, responsive to reliability and security risks, practical to implement, and cost-effective

[2] In support of ERO Goal 1aDevelop Standards which are clear, responsive to reliability and security risks, practical to implement, and cost-effective

[3] In support of ERO Goal 1a Develop Standards which are clear, responsive to reliability and security risks, practical to implement, and cost-effective

  - Promote and assist with the Cost Effective Analysis Process ("CEAP") to ensure standards have the most cost effective requirements which meet the reliability objectives of standards under development[4]

- Further resources required to evaluate the standards from a "cost benefit" and also a "cost effectiveness" perspective will be required.
- NERC Reliability Standards will continue to require Violation Risk Factors (VRFs) to be developed and NERC is reviewing additional levels of VRF and development of a Sanction Matrix which is envisioned to replace the Violation Severity Levels (VSLs).
- Expanded efforts to educate and inform stakeholders in the areas of NERC and NPCC Regional Standards through NPCC Workshops and with anticipated additional forums such as increases in the amount of Internet based meetings and technical conferences. [5]

2015 Key Assumptions

- Facilitate stakeholder review, comment on, and develop ballot recommendations or list of Regional issues, for all NERC Reliability Standards Projects under informal or formal development or revision prior to the end of ballots
  - NERC and NPCC benefit from NPCC's Regional coordination consisting of a broad stakeholder review process and development of consensus recommendations to assure proposed standards will support international reliability and provide appropriate reliability objectives for the Continent-wide standards
  - Coordinate a comprehensive review of the results based standards initiative processes and standards being implemented
  - Conduct and obtain training for performing Quality Reviews of standards at both the Regional level and to assist the ERO with analysis of the continent wide standards
  - Coordinate the review of all Reliability Standards Audit Worksheets during their postings for comment for potential expansion of their associated standard's requirements
  - Refine the NPCC triage process to assess posted standards and related material to ensure it is properly routed to and addressed by the appropriate NPCC technical or process resources.
- Participate in the stakeholder efforts to develop Standards Authorization Requests (SARs) and Regional SARs to further improve standards in response to any potential inadequacies in reliability or to improve standards
- Monitor and participate in the drafting of key NERC Reliability Standards-CIP, Protections Systems, Balancing Control Performance, and Frequency Response, etc.
  - The NPCC monitoring of the development of standards helps to ensure reliability requirements that are clear, measureable, and enforceable and support international reliability in the Northeast
- Continue with the development and maintenance of a set of NPCC Phase II Directories not inconsistent with the NERC Reliability Standards which clearly delineate the more stringent NPCC criteria requirements

[4] In support of ERO Goal 1a Develop Standards which are clear, responsive to reliability and security risks, practical to implement, and cost-effective

[5] In support of ERO Goal 1a Develop Standards which are clear, responsive to reliability and security risks, practical to implement, and cost-effective

  - The combination of North American and Regional Reliability Standards with the more-stringent NPCC Regional criteria provides for consistency and operational clarity while providing robust defense in–depth, results based, standards to ensure BES reliability
  - Ensure no redundancies exist between the criteria found in the NPCC Directories and the ERO standards
  - Retire Directories that have been overtaken by improved NERC standards
  - Continually file the more stringent requirements with the New York State Department of Public Service and Canadian Provinces as applicable
- Review reliability requirements of ERO and NPCC Regional Standards, NPCC Criteria and ensure consistency, remove redundancies, adopt Functional Model language and ensure requirements are "results based"
  - The unambiguous assignment of reliability requirements to specific functional entities benefits international reliability
  - Participate in the continuing refinement of the Functional Model to capture evolving issues essential to reliability and new objectives in the industry, i.e. demand resource operator, planning functions, new activities yet to be identified such as those associated with Smart Grid, "Synchro-Phasor" technology, etc.
  - Participate in the continual improvement of the NERC standards development processes and initiatives such as the CEAP, PMOS and Single Portal Project.
  - Contribute to the improvement of process related to NERC providing interpretations.
- Review all FERC orders and Provincial regulations as they relate to the standards, their revision and adoption
  - Northeast reliability benefits from careful analyses of governmental orders or actions adopting standards to assure consistency in interpretation
  - Review rulings that are issued and all FERC Directives for potential reliability related issues
  - Conduct and support Regulatory/Governmental Provincial filings on a periodic basis based on individual Provincial Laws and requirements outlined in the Memorandum of Understandings for each Province.
- Enhance NPCC standards website pages to provide uniform and clear information to the stakeholders while also providing the historical and archived information to support NERC and FERC approvals and expanding requirements

2015 Goals and Key Deliverables

The Reliability Standards program goals and objectives for 2015 are grouped into seven categories:

1) Participate in the ERO Results-Based Standards Development

- Participate in the development and revision of the NERC three year work plan through review, commenting and drafting activities
- Participate in the Standards Committee Strategic initiatives to develop results based standards that will provide a defense in depth, complete the standards due for 5 year review, and address all existing and outstanding FERC Directives.
- Support the implementation of the NERC Board of Trustees ("BOT") resolutions specifically supporting the timeliness, cost effectiveness, timely development, and quality of new standards

- Coordinate the development of ERO Reliability Standards within NERC's three-year standards work plan with the emphasis placed on reducing the amount of new FERC Directives issues by closer coordination with the Commission staff
- Conduct thorough reviews of all NERC standards being developed or revised and coordinate comments for Northeastern North America driving consensus to the extent possible
- Facilitate and enhance the NERC Cost Effective Analysis Procedure both within NPCC throughout the industry
- Conduct thorough reviews of all Industry requested NERC Formal Interpretations of standards and develop and promote the NERC Informal Guidance Process, a comprehensive process to deal with all standards related questions, e.g. Single Portal
- NPCC staff along with NPCC solicited Regional drafting team volunteers, will participate in the drafting of all ERO standards affecting or potentially affecting reliability in the Eastern Interconnection and provide support for review and development of comments and propose improvements with specific emphasis on CIP
- NPCC and its members will review and coordinate potential comment on FERC preliminary staff assessments as appropriate
- Participate in ballots for ERO standards and provide consensus recommendations to the NPCC Members of the NERC Registered Ballot Body or provide a list of issues to allow the Members to cast a ballot based on Regional concerns prior to the end of the ballots
- Review and develop issues on FERC Notice of Proposed Rulemakings for any and all standards related issues as appropriate
- Coordinate and evaluate proposed standards utilizing NPCC's Regional technical task forces, working groups and committees
- Educate and notify stakeholders and regulators about issues related to standards development through various means such as webinars and workshops
- Provide outreach to industry trade groups to educate and drive consensus such as the North American Generator Forum and North American Transmission Forum
- Provide a forum for NPCC review of proposed and posted documents from the NERC Critical Infrastructure Protection Committee (CIPC) and NPCC Task Force on Infrastructure Security and Technology (TFIST)
- Provide support to NERC's strategy in the prioritization, identification, scheduling and development of NERC directed Regional Reliability Standards
- Participate in NERC's Standards Committee standards prioritization process, to identify immediate standards needs and prioritization based on need
- Participate in the NERC RISC by providing a Regional point of contact for all potential reliability related risks and gaps within the Northeast or as noted by NPCC stakeholders
- Participate in and provide support to critical standards, such as UVLS, Voltage and Reactive Control, Real Time Tools, Frequency Response, etc.
- Identify and initiate Regional Variances to the NERC Reliability Standards as soon as possible, allowing incorporation into the continent wide standard at its inception
- Identify potential drivers for standards revisions based on revisions to the BES to a bright line criteria and any document revisions required as a result of consideration of the "Exception Process".
- Support additional standards workload from further economic stimulus, i.e. standards on integrating variable generation resources or EHV backbone, Smart Grid, Electric Vehicles or "Synchro-Phasor" projects as necessary

- Provide continued input and leadership to NERC, based on NPCC experiences, regarding strategy for developing cost effectiveness analysis for standards and support activities to enhance this to identify "benefits" for the draft standards.
- Provide support and assistance to the ERO for conducting Quality Review activities on NERC continent-wide standards as possible
- Continually file the NPCC Directories with the Canadian Provincial Regulatory Authorities within the NPCC "footprint", on an as needed basis, as the directories are developed and revised and as the Provinces establish procedures and agreements with NPCC.
- Continue to develop new and innovative processes to better utilize the limited internal and external resources in the Region to enable sufficient technical review of posted standards and related materials
- Support the ERO and the relationships with FERC and the provincial governmental authorities for standards development activities as necessary to accomplish the ERO goals and objectives
- Support the development of system protection and control, communication, transmission operation standards and other critical standards efforts.

2) Regional Standards Development

- NPCC does not anticipate developing further Regional Standards but reserves the right to do so if a reliability issue exists that is not appropriate for Continent-wide development and also will perform clarifications as needed to existing approved Regional Standards.
- Draft any additional standard NERC directs NPCC to develop to meet an urgent reliability related needs, i.e. Geomagnetic disturbance system hardening
- Accomplish all directives of ERO and governmental and/or regulatory authorities with regard to Regional Standards development and procedures
- Adhere to and surpass, where practical, the 2014-2016 NERC Work plan milestones as they pertain to targets for the Regional Standards
- Respond to any FERC Directives that may arise as a result of the filing of NPCC's Regional Standards with the FERC or any Provincial "directives" that may be issued by the Canadian Regulatory Authorities

3) Standards Improvement

- Achieve NPCC reliability goals and objectives by initiating, participating in, and efficiently completing standards related activities
- Leverage internet and web based tools functionality to ensure inter-Regional consistency and quality of Regional Reliability Standards
- Establish long-term strategy for standards improvement and initiate implementation
- Continually identify additional future Regional Standard opportunities if Continent-wide standards are not an appropriate solution
- Ensure the topics addressed by the Reliability Standards parallel changing industry needs
- Participate in reliability metrics activities to identify potential measures for benchmarking of reliability to determine if an adequate level of reliability is being achieved
- Support and develop cost-benefit analysis activities to determine if any potential incremental increases in costs of implementing a standard have sufficient enough reliability benefit to implement that standard

4) Coordination of review of RSAWs

- Develop a process to review the RSAWs consisting of subject matter experts to determine if the RSAWs are technically representative of the standard's requirements and also to review the evidence suggested in the RSAW for satisfactory compliance assessment
- The Regional Standards Committee ("RSC") will oversee and provide the results of the coordination to the appropriate NERC SDT charged with development of the RSAW

5) Business Practices Interface

- Coordinate the review of standards through NPCC RSC, staff, and other members participating in activities of the North American Electric Standards Review Board (NAESB)
- Identify potential market related issues for Regional Standards through NPCC RSC coordination and reviews

6) Opportunities for Process Improvement

- Identify efficiencies for a coordinated NERC standards development process and NPCC Regional Standards Development Procedure and recommend revisions as applicable to either process
- Refine the NERC and NPCC CEAP s to evaluate the costs and effectiveness of proposed new and revised reliability standards to achieve an adequate level of reliability and a steady state set of standards
- Participate in any potential revision and redrafting of the NERC Standards Development Process to consider expedited standards development and cost effectiveness analysis and maintaining the ANSI Accreditation for standards development
- Participate in the enhancement of the Single Portal on the NERC website to provide one stop shopping for stakeholders seeking answers to questions.
- Identify potential future processes to obtain expedited interpretations
- Identify expedited processes for adjusting NERC glossary terms
- Identify refinements for credentialing standard drafting team members to ensure the correct subject matter experts are developing the standards at both the Regional level and the ERO level.
- Establish targets for NERC and NPCC standards procedure improvement and support initiation of implementation of the strategy
- Streamline and improve the Regional Standards program tools and IT based solutions
- Refine the records retention programs to ensure sufficient documentation exists for regulatory approvals
- Develop document management systems to allow the efficient and effective revisions of documents, control of authorship and security of documents
- Identify improvements in process for feedback loops to ensure that event analysis and investigation lessons learned and compliance issues involving violations are fed into the standards program area, as appropriate for review and potential consideration when revising standards
- Support the creation of an ERO standards database, available to industry and online, to identify and review issues related to all approved and developing standards
- Participate in the Functional Model Working Group activities to refine functions, tasks and responsibilities of applicable entities
- Solicit and provide outreach to FERC in the Regional Standards Development Processes

7) Communications

- Improve automated notifications process to assure awareness of dates and proceedings of all standard development activities
- Strengthen the relationship with the industry's technical committees to ensure adequate input to standards development, such as the North American Generator Forum.
- Participate in NPCC and NERC workshops as necessary, to promote awareness and educate the industry
- Develop and institute a consensus building and notification process(es) for engaging stakeholders and providing immediate notification for the need to review standards. Provide the associated coordination for this review utilizing subject matter experts, both internal and external to the Regional Entity staff
- Promote the reliability objectives of the NERC standards as appropriate to the NPCC members of the NERC Registered Ballot Body in order to achieve consensus and support of beneficial standards and to promote the "One-Enterprise" model.

Technically excellent, results based standards that enhance reliability and are developed in a timely and efficient fashion, require the full participation of the right industry experts from all Regional Entities when developing Reliability Standards. The NPCC RSC promotes the drafting team process and solicits drafting team members from appropriate NPCC technical bodies and others in the industry and adjoining Regional Entities. In addition the NPCC RSC works with the individual NERC standards developers to participate in Regional outreach and coordination of issues at each NPCC RSC meeting.

NPCC RSC will also assist in providing notifications and announcements to NPCC participants in the Northeastern North America NERC Registered Ballot Body of important applicable deadlines for ballot pool registration and for casting ballots thereby enhancing participation, promulgation of important information and increasing awareness. In the fourth quarter of 2014 NERC will "roll out" a new Standards Balloting System (SBS). This new system will require training and an implementation communication plan. NERC will develop the training and NPCC will assist in providing it throughout the Northeast. The SBS will require all users to reregister to cast ballots as well as submit comments. This support will enhance efficiency of the NERC procedure and help to ensure the necessary quorums are present at ballot and help to clean up the registered ballot body list. NPCC will also, when practical, promote important standards and the requirements of those standards through various communications.

NPCC will also participate in the development and revision of standards as directed by FERC, Canadian provincial and other regulatory and/or governmental authorities. FERC to date has identified numerous NERC Reliability Standards needing further work and has issued numerous Directives appearing in FERC Orders. In 2013 FERC also issued remanded interpretations and standards which require NERC to address commissions concerns as outlined in the associated Orders. These remands have created a need for NERC to review existing processes and determine approaches going forward. NPCC will support these efforts and will lead the review and potential revision of the NERC Interpretation process. These standards needing revision are delineated in the 2014 – 2016 NERC Reliability Standards Development Plan, and will be ready to be reviewed and revised throughout 2015.

NPCC will provide support and coordination of NERC standards development activities as outlined in the 2014-2016 Reliability Standards Development Plan and the Standards Committee and ERO strategic goals and initiatives.

Regional Standards Development

The NPCC currently has two FERC approved Regional standards, Disturbance Monitoring and Underfrequency Load Shedding. NPCC has undertaken the review of the Disturbance Monitoring standard for adequacy from the perspective of a "bright line" BES definition and currently developing PRC-002-2 Disturbance Monitoring continent wide standard. This review of the standard and proposed revision to the standard will be performed in the 2014-2015 timeframe. In addition there are two other Regional standards that NPCC may review to determine if they should move forward into active formal development. These Regional Standards will include, but not be restricted to the following:

- Special Protection Systems (SPS) scheduled to begin development in 2014
  Balancing Authority Controls (BA - Reserve Sharing)

Whether NPCC pursues these Regional standard will depend in large part to how comprehensive their associated continent-wide standards are. NPCC will review the continent wide standards as they are develop, participating in those activities and providing supporting subject matter expertise as it is available.

Based on the portion of professional/technical staff time and other resources devoted to Reliability Standards development, NPCC estimates that it will expend approximately 10 percent of its resources on this activity.

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- U.S. Penalty Sanctions remitted from 7/1/13 through 6/30/14 reduce U.S. LSE designee assessments for 2015.

Personnel Expenses

- NPCC anticipates no need to hire additional personnel in this program area in 2015.
- Salaries expense reflects implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Retirement expense decreased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.

Meeting and Travel Expenses

- Meeting expenses will be minimized due to a continued effort to keep costs down by holding more meetings via WebEx and teleconferences, at the NPCC offices or member facilities when possible, as well as lower meeting space rental rates through negotiations. However, meeting volume is expected to increase in 2015. Travel expenses due to continued practice of advance bookings, adjustments to class of hotel used, increased meetings at NPCC's offices, and meetings conducted via teleconference will be held to a minimum. Conference calls and Internet meetings, which are budgeted as a part of G&A and then allocated to the direct programs through indirect expenses, will be conducted for business when practical.

Operating Expenses and Indirect Expenses

- 2015 Reliability Standards program funding is driven by the need for additional activities to support NERC standards activity to achieve a results based, adequate, set of steady state standards, FERC activity and increased number of rulings and directives are anticipated as a result of the NERC three year work plan. NPCC anticipates expanded activity and plans to prioritize the efforts of existing resources to meet this expanded workload to support reliability and the ERO Strategic Goals. In addition, as standards reviews increase in number, there may be a need to have contractors assist due to constrained resources of NPCC Staff and members.

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Reliability Standards Program

Funding sources and related expenses for the Reliability Standards section of the 2015 business plan are shown in the table below.

Statement of Activities and Capital Expenditures 2014 Budget & Projection, and 2015 Budget						
Reliability Standards						
		2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding						
ERO Funding						
	ERO Assessments	$ 1,431,239	$ 1,431,239	$ -	$ 1,426,577	$ (4,663)
	Penalty Sanctions	16,091	16,091	-	29,552	13,462
Total ERO Funding		**$ 1,447,330**	**$ 1,447,330**	**$ -**	**$ 1,456,129**	**$ 8,799**
	Membership Dues	-	-	-	-	-
	Testing Fees	-	-	-	-	-
	Services & Software	-	-	-	-	-
	Workshops	-	-	-	-	-
	Interest	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
Total Funding (A)		**$ 1,447,330**	**$ 1,447,330**	**$ -**	**$ 1,456,129**	**$ 8,799**
Expenses						
Personnel Expenses						
	Salaries	$ 502,840	$ 502,840	$ -	$ 535,458	$ 32,618
	Payroll Taxes	31,305	31,305	-	31,420	115
	Benefits	131,342	131,342	-	93,684	(37,658)
	Retirement Costs	87,449	87,449	-	85,075	(2,374)
Total Personnel Expenses		**$ 752,936**	**$ 752,936**	**$ -**	**$ 745,638**	**$ (7,299)**
Meeting Expenses						
	Meetings	$ 25,000	$ 25,000	$ -	$ 20,000	$ (5,000)
	Travel	110,000	110,000	-	115,000	5,000
	Conference Calls	-	-	-	-	-
Total Meeting Expenses		**$ 135,000**	**$ 135,000**	**$ -**	**$ 135,000**	**$ -**
Operating Expenses						
	Consultants & Contracts	$ 30,000	$ 30,000	$ -	$ 25,000	$ (5,000)
	Office Rent	-	-	-	-	-
	Office Costs	-	-	-	-	-
	Professional Services	-	-	-	-	-
	Computer & Equipment Leases	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
	Depreciation	-	-	-	-	-
Total Operating Expenses		**$ 30,000**	**$ 30,000**	**$ -**	**$ 25,000**	**$ (5,000)**
	Total Direct Expenses	**$ 917,936**	**$ 917,936**	**$ -**	**$ 905,638**	**$ (12,299)**
Indirect Expenses		**$ 555,686**	**$ 555,686**	**$ -**	**$ 561,221**	**$ 5,535**
Other Non-Operating Expenses		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)		**$ 1,473,622**	**$ 1,473,622**	**$ -**	**$ 1,466,858**	**$ (6,764)**
Change in Assets		**$ (26,292)**	**$ (26,292)**	**$ -**	**$ (10,729)**	**$ 15,563**
Fixed Assets						
	Depreciation	$ -	-	$ -	-	$ -
	Computer & Software CapEx	-	-	-	-	-
	Furniture & Fixtures CapEx	-	-	-	-	-
	Equipment CapEx	-	-	-	-	-
	Leasehold Improvements	-	-	-	-	-
	Allocation of Fixed Assets	(26,292)	(26,292)	-	(10,729)	15,563
Inc(Dec) in Fixed Assets (C)		**(26,292)**	**(26,292)**	**-**	**(10,729)**	**15,563**
TOTAL BUDGET (=B+C)		**$ 1,447,330**	**$ 1,447,330**	**$ -**	**$ 1,456,129**	**$ 8,799**
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)		**$ -**	**$ -**	**$ -**	**$ 0**	**$ (0)**

Compliance Monitoring and Enforcement and Organization Registration and Certification Program

Compliance Monitoring and Enforcement and Organization Registration and Certification Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	16.00	16.00	0.00
Direct Expenses	$5,080,485	$5,440,048	$359,564
Indirect Expenses	$3,034,462	$3,064,686	$30,225
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	($35,575)	$63,410	$98,985
Total Funding Requirement	$8,079,371	$8,568,145	$488,774

Program Scope and Functional Description

The Compliance Monitoring and Enforcement and Organization Registration and Certification Program (CORC) Program scope covers: 1) the identification, registration and certification of those entities responsible for meeting the NERC Reliability Standards and any approved Regional Standards; 2) the implementation of the NERC Compliance Monitoring and Enforcement Program (CMEP) in the United States, including the compliance monitoring, assessment and enforcement of NERC Reliability Standards and Regional Reliability Standards. and 3) the implementation of compliance monitoring, assessment and enforcement recommendations in accordance with individual executed MOUs or Agreements in the Canadian Provinces of Ontario, Québec, New Brunswick and Nova Scotia.

The NPCC Compliance Committee (CC) is charged with providing objective stakeholder policy input to NPCC's implementation of the CMEP in the U.S. and compliance related activities under the above mentioned MOUs in the NPCC portion of Canada. With regard to NERC Reliability Standards and Regional Reliability Standards, the CC provides an oversight role of the independent NPCC compliance staff's implementation of the CMEP. In this oversight role the CC will review and endorse the processes used by the NPCC compliance staff in the conduct of the CMEP.

The NPCC compliance staff makes the initial and final determination of alleged violations and determines appropriate penalties and sanctions in accordance with the NERC *Sanction Guidelines*. To accomplish this objective, NPCC's compliance staff is further divided into four sub- program areas: Compliance Implementation and Registration; Compliance Audit Program; Compliance Enforcement; and Compliance Investigation:

Compliance Implementation and Registration

The Compliance Implementation and Registration sub-program is responsible for:

a) Identifying for registration, using a risk based registration model, all entities that are required to meet the NERC and Regional Reliability Standards. During the course of this activity, regular communication with registered entities is promoted through face-to face meetings, compliance workshops, teleconferences and email;
b) Development and maintenance of all CMEP Compliance Procedures, Compliance Instructions and all other CMEP related documentation;
c) Development and maintenance of Performance Metrics that are used to measure the quality and effectiveness of CMEP Implementation and its impact on the reliability of the Bulk Electric System;
d) Coordinating the implementation of NPCC Compliance Staff responsibilities as they pertain to the executed MOU with each of the Canadian Provinces in the NPCC Region.
e) Day-to-day implementation of the CMEP;
f) Development of annual CMEP Implementation Plan;
g) Monitoring and assessment of self-certification, self-report, exception reporting, periodic data and complaint submittals;
h) Development and maintenance of CMEP Data Administration Application (CDAA);
i) Development and maintenance of compliance website.
j) Support the anticipated expansion of the number of registered entities in NPCC due to the implementation of the FERC Order related to the definition of Bulk Electric System
k) Conduct Entity Impact Evaluations. Conduct certification(s) of newly identified Transmission Operators (TOPs), as needed.
l) Maintain database of BES assets subject to NERC and NPCC Reliability Standards
m) Participation on various NERC and NPCC working groups to remain apprised of changes to Compliance processes, and commonality of registration, monitoring, auditing, and enforcement approaches.

Compliance Audit Program

The Compliance Audit Program is charged with conducting both on-site and off-site compliance audits, and spot checks, of NERC Reliability Standards in accordance with the NERC Rules of Procedure and associated NPCC procedures developed under the NPCC Compliance Implementation Program. These audits are performed on the basis of risk to the BES. The yearly schedule is produced consistent with Risk Assessment of registered entities and the frequency of their last audit. The schedule is posted annually on NERC and NPCC public websites. Flexibility may be used in the predefined frequency based on the risk assessment and performance based assessment of each entity scheduled for an audit, and changes requiring certification. The audits are led by qualified senior NPCC Staff and the audit teams prepare public and non-public audit reports with their findings, including the identification of any possible violations. Contents and processing of the reports are in accordance with NERC directives for audit reporting. Specific lessons learned are factored into the audit program to promote continuous improvement and are presented at workshops in conjunction with the Compliance Implementation Program. The comprehensive spot-check program is established based on the NERC actively monitored list, NPCC's assessment of self-certifications, follow–ups on entities who have previously violated a Reliability Standard, follow-up on entities that have been involved in a significant system event, and other requirements which at the discretion

of NPCC could pose a higher risk to reliability if not followed properly. The schedule for Spot Checks is not public.

Resources from the Compliance Audit Program are also used to implement the Certification process for entities intending to register as new TOPs, BAs or RCs, as well as certification reviews of changes made by existing TOPs, BAs and RCs that meet the threshold requiring same. These actions are performed in support of the Compliance Registration Program which encompasses the Certification process. Resources for this activity, which is independent of the audit process, depend on the scope, function, and location of the entity being certified.

Compliance Investigation

A Compliance Investigation (CI) may be initiated at any time by NPCC in response to a system disturbance, complaint, or possible violation of a Reliability Standard identified by any other means. The CI process requires the establishment of an investigation team that coordinates with NERC and FERC as necessary; and also coordinates with the Situation Awareness Program Area.

Compliance Enforcement

In processing identified violations NPCC Compliance Enforcement will strive to promote both timeliness and transparency of compliance results, including those efforts associated with meeting the enforcement metrics described below. In addition NPCC will promote the use of self-identification of non-compliance and implementation of discretion, including increased utilization of streamlined tracks such as FFT and discretion as shown below.

Compliance Enforcement responsibilities:

a) Issuing all Notices as described in the CMEP including the Notice of Possible Violation (NOPV), Notice of Find, Fix and Track (FFT) Treatment; Notice of Alleged Violation (NOAV), and the Notice of Confirmed Violation (NOCV);
b) Conducting comprehensive enforcement investigations based on the facts and circumstances related to all possible violations of Reliability Standards, whether identified in an audit, a self-report, complaint, or other source, and determining whether further action is warranted;
c) Reviewing, approving, submitting to NERC and tracking the progress of all mitigation plans /mitigating activities associated with confirmed violations;
d) Coordinating settlement activities once they have been initiated and submitting settlement agreements to NERC for approval;
e) Identifying and processing candidates for the FFT Process;
f) Participating in the Hearing Process by representing NPCC before the Hearing Body. Compliance Hearings would be conducted at NPCC under the supervision of a qualified, independent hearing officer contracted by NPCC;
g) Issuing Remedial Action Directives when appropriate; and
h) Implementing of the Reliability Assurance Initiative (RAI), including :
    i. Notifying the registered entity, within 60 days on average, whether a non-compliance will proceed through enforcement, be treated as a compliance exception or additional information is needed (“Triage”);
    ii. Utilizing the Aggregation of Minimal Risk Process; and
    iii. Utilizing the Enforcement Discretion Process.

A set of enforcement metrics, that include those metrics included in the ERO Corporate Goals, are produced that cover the following:

a. Caseload Index and Violation Aging
b. Mitigation Aging
c. Percentage of self-identified violations
d. Percentage of minimal and moderate risk violations through FFT, SNOP or discretion

Each of these metrics will have target values defined that are consistent with those target values identified in the ERO Corporate Goals.

2015 Key Assumptions and Cost Impacts

2014	Projected 2015
3 Large On-Site Audits	4 Large On-Site Audits
0 Medium On-Site Audits	0 Medium On-Site Audits
3 Small On-Site Audits	3 Small On-Site Audits
12 On-Site CIP Audits	4 On-Site CIP Audits
20 Large Off-Site Audits	8 Large Off-Site Audits
7 Medium Off-Site Audits	21 Medium Off-Site Audits
7 Small Off-Site Audits	10 Small Off-Site Audits
22 Off-Site CIP Audits	24 Off-Site CIP Audits
300 Spot Checks	350 Spot Checks
8 On-site TFE Part B reviews	4 TFE Part B Reviews
200 Violations (Estimated)	200 Violations (Estimated)
Settlements Covering 100 Violations	Settlements Covering 100 Violations
2 Hearings (Unbudgeted)	2 Hearings (Unbudgeted)
1 CI (Estimated)	1 CI (Estimated)
0 Entity Certifications	2 Entity Certifications

- Regarding the Compliance Audit Program, Technical Feasibility Exception (TFE) reviews are conducted both on-site at the entity's facility and at the NPCC offices when possible. TFE's continue to be requested as entities replace and install new equipment/devices/components that meet the criteria set forth in Rules of Procedure Appendix 4D. Compliance estimates 4 on-site reviews will be performed in 2015.

- Increases in Audit costs reflect Risk Assessment activity that is the basis for audit scoping. The Risk Assessment includes an assessment of an entity's Internal Controls which will be used for future audits in the scoping and frequency of engagements.
- Potential increases due to the newly identified role related to implementing the QCMEP in Quebec and the continuing role of implementing the NB CMEP in New Brunswick.

- The 2015 Business Plan projects no increases in Enforcement Processing activities over the 2014 Budget.
- The 2015 Business Plan projects the need for 1 Compliance Investigation. These Compliance Investigations are manpower intensive for NPCC staff (requiring allocation of more resources and potentially higher than normal costs) since previous Compliance Investigations have also included entities outside of NPCC's footprint for which NPCC is the Compliance Enforcement Authority.

2015 Goals and Key Deliverables

- Conduct 2015 CMEP consistent with the Reliability Assurance Initiative, incorporating Risk Assessment; Internal Control assessment; Aggregation of Minimal Risk Violations; and Enforcement Discretion and all NERC Reliability Standards contained in the NERC actively-monitored list for 2015 and any approved and applicable Regional Reliability Standards
  - Process identified violations as effectively as possible, including the timely identification of a violation, timely issuance of violation notices including the NOPV; the Notice of Alleged Violation and the NOCV
  - Implement settlement process when applicable and send proper notifications to NERC and FERC
  - Conduct necessary Hearings related to resolution of outstanding disputes regarding violations and/or sanctions. Send results of hearings to NERC and FERC[17];
- Continue to enhance the settlement process by modifying existing practices and adopting new practices to reduce the duration of settlement negotiations without sacrificing the rigor and quality of the negotiated settlements. Develop and analyze appropriate performance metrics that track settlement process duration and utilize results of analysis to further enhance process.
- Implement compliance responsibilities identified in the approved Canadian MOUs[18];
- Annual report to NERC and Régie on NPCC implementation of QCMEP
- Annual report to NERC and New Brunswick Electric Utility Board (EUB) on NPCC implementation of NB CMEP.
- Review and revise NPCC Compliance Registry based on a risk-based approach[19] ;
- Evaluate CMEP and Canadian entity compliance program implementation with the objective of establishing a long-term strategy for compliance improvement, and initiate the implementation of the long term strategy[20];
- Provide NPCC Regional Entity input, through participation in appropriate NERC compliance committees, on policy and implementation issues related to compliance and enforcement including the development of compliance elements for all new or revised NERC Reliability Standards[21];

[17] In support of ERO Goal 2. Be a strong enforcement authority that is independent, without conflict of interest, objective and fair.
[18] In support of ERO Goal 3. Promote a culture of compliance that supports reliability excellence within industry.
[19] In support of ERO Goal 2. Be a strong enforcement authority that is independent, without conflict of interest, objective and fair.
[20] ERO Goal 2. Be a strong enforcement authority that is independent, without conflict of interest, objective and fair.
[21] ERO Goal 6. Promote a culture of reliability excellence.

- Provide required information to NERC on a timely basis including reporting of alleged violations and confirmed violations[22];
- Track the progress of, report status of, and approve mitigation plans[23];
- Conduct 2015 Compliance Audit Schedule based on risk to the BES and number of registered entities (Each audit covers a single registered entity that could be audited for multiple Functional Model types that they are registered for and is done in accordance with the 2015 Compliance Audit Program schedule)[24] ; and promote RAI initiatives by:
    - Utilizing the Audit Checklist and Auditor's Handbook for all on-site and off-site audits
    - Preparing a Risk Assessment and Internal Control Assessment for all on-site audits[25];
- In addition, 28 registered entities will be audited for the requirements of the version in place for CIP 002 to CIP 009. These will be separate audits. On-site CIP audits may be combined with the normally scheduled 2015 on-site audits[26];
- A spot check can be viewed as a limited unscheduled small off-site compliance audit that will be utilized to verify self-certification submittals that have been done earlier in the year or other requirements based on factors as described in the Compliance Audits section. In 2015 the number of spot checks to be done is estimated to be 350[27] ;
- Assure that NPCC Staff is trained to conduct Compliance Audits including CIP Compliance Audit training[28];
- Assure that NPCC Staff is trained to conduct Certification of entities intending to Register as BA, RC or TOP for the first time, or Certification Reviews of changes by existing BAs, RCs or TOPs that meet the criteria requiring a Certification Review[29];
- NPCC is working with the other Regions to access, train and perform certifications (and re-certification) in an effort to be consistent across the ERO[30] ;
- Continue to actively perform a risk profile of each entity prior to audit and upon completion of an audit, continue to identify risk and reliability gaps[31] ;

[22] ERO Goal 2. Be a strong enforcement authority that is independent, without conflict of interest, objective and fair.
[23] ERO Goal 2. Be a strong enforcement authority that is independent, without conflict of interest, objective and fair.; ERO Goal 5. Be accountable for mitigating reliability risks.
[24] In support of ERO Goal 3a. and 3b. Promote a culture of compliance that supports reliability excellence within industry.
[25] In support of ERO Goal 3. Promote a culture of compliance that supports reliability excellence within industry.
[26] In support of ERO Goal 3. Promote a culture of compliance that supports reliability excellence within industry.
[27] In support of ERO Goal 3. Promote a culture of compliance that supports reliability excellence within industry.
[28] In support of ERO Goal 3. Promote a culture of compliance that supports reliability excellence within industry.
[29] In support of Goal 2a. Be a strong enforcement authority that is independent, without conflict of interest, objective, and fair, and promote a culture of reliability excellence through risk-informed compliance monitoring and enforcement. a. The ERO registers and deregisters entities commensurate with risk to the BES and ensures all key reliability entities are certified to have essential capabilities.
[30] In support of Goal 2a. Be a strong enforcement authority that is independent, without conflict of interest, objective, and fair, and promote a culture of reliability excellence through risk-informed compliance monitoring and enforcement. a. The ERO registers and deregisters entities commensurate with risk to the BES and ensures all key reliability entities are certified to have essential capabilities.
[31] In support of Goal 4a. Identify the most significant risks to reliability, be accountable for mitigating reliability risks, and promote a culture of reliability excellence. a. Risks are identified and prioritized based on reliability impacts, cost and practicality of assessments, projected resources, and emerging issues.

- Develop and implement compliance reform via the Reliability Assurance Initiative (RAI) by being an integral participant in committees and workgroups involved in the RAI[32];
- Promote a culture of compliance that addresses reliability risks of NPCC registered entities by using reliability gap analysis. Assess and evaluate registered entity's Internal Controls as part of the audit and spot check process[33];
- Continue to expand the use of discretion through the utilization of compliance exception. [34] ;
- NPCC will collaborate with NERC to promote better coordination, planning, delivery and management of training efforts across the enterprise through a unified learning management system (LMS), without adversely impacting region-specific training requirements;
- Continue to implement physical security outreach and Cyber Security outreach by visiting four registered entity sites to perform an assessment of their physical security, evaluate their Cyber Security and supply recommendations for improvements[35];
- Enhance the CDAA to expand its capabilities from both the registered entity perspective and the NPCC Compliance Staff perspective[36];
- Conduct 2015 Compliance Workshops and interim information sessions for registered entities as necessary as a part of Training and Education program area[37].

Adopt and promote practices to enhance the benefits of the self-reporting of violations by both the Regional Entity and the registered entity. This would include improvement to the registered entity internal processes used for identifying and submitting self-reports (e.g. adoption of an aggregated approach for submittal of self-reports, etc.), improvement in the way Regional Entities process self-reports and the streamlining and standardizing of the amount and type of data needed to evaluate a self-report.

[32]In support of Goal 3a. Promote a culture of compliance that supports reliability excellence within industry. a. Industry has effective procedures and programs to monitor, detect, correct, report, and prevent compliance, reliability, and security issues.

[33]In support of Goal 3a and 4a Goal 3. Promote a culture of compliance that supports reliability excellence within industry. Industry has effective procedures and programs to monitor, detect, correct, report, and prevent compliance, reliability, and security issues. Goal 4. Identify the most significant risks to reliability, be accountable for mitigating reliability risks, and promote a culture of reliability excellence. a. Risks are identified and prioritized based on reliability impacts, cost and practicality of assessments, projected resources, and emerging issues.

[34]In support of Goal 2b. Goal 2. Be a strong enforcement authority that is independent, without conflict of interest, objective, and fair, and promote a culture of reliability excellence through risk-informed compliance monitoring and enforcement. 2.b. The ERO holds industry accountable for violations that create serious risk to the BES; resulting actions are timely and transparent to industry.

[35]In support of Goal 4c. Goal 4. Identify the most significant risks to reliability, be accountable for mitigating reliability risks, and promote a culture of reliability excellence. 4.c. ERO supports industry situational awareness and cybersecurity preparedness and provides independent reliability information to policy makers.

[36]In support of Goal 5c. Goal 5. Improve transparency, consistency, quality, and timeliness of results; operate as a collaborative enterprise; and improve efficiencies and cost-effectiveness. 5.c. The ERO internal risks are understood and managed; ERO processes are effective, efficient, and continuously improved.

[37]In support of Goal 5a. Goal 5. Improve transparency, consistency, quality, and timeliness of results; operate as a collaborative enterprise; and improve efficiencies and cost-effectiveness. 5.a. The ERO acts in a coordinated and collaborative manner with stakeholders.

Based on the portion of professional/technical staff time and other resources devoted to Compliance monitoring and enforcement and organizational registration and certification, NPCC estimates that it will expend 58 percent of its resources on this activity.

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- U.S. Penalty Sanctions remitted from 7/1/13 through 6/30/14 reduce U.S. LSE designee assessments for 2015.

Personnel Expenses

- NPCC anticipates no need to hire additional personnel in this program area in 2015.
- Salaries expense reflects implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Retirement expense decreased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.

Meeting and Travel Expenses

- Meeting expenses will be minimized due to a continued effort to keep costs down by holding more meetings via teleconference, at the NPCC offices or member facilities, combining or appending meetings to other mandatory training/meetings, as well as lower meeting space rental rates through negotiations. Travel expenses due to continued practice of advance bookings, adjustments to class of hotel used, increased meetings at NPCC's offices, and meetings conducted via teleconference will be held to a minimum, however, the amount of activity is expected to increase in 2015. Conference calls and internet meetings, which are budgeted as a part of G&A and then allocated to the direct programs through indirect expenses, will be conducted for business when possible.

Operating Expenses and Indirect Expenses

- Consultant and contractor costs increased due to increased workload related to the initial implementation of RAI, incorporating Risk Assessment and Internal Control assessment. Without this one time ramp up in RAI endeavors for 2015, contractor costs would have remained relatively flat. These joint ERO Enterprise initiatives are intended to benefit the registered entities, Regional Entities and NERC. With a risk and performance based assessment of each registered entity, audits will transition to a periodicity more reflective of the risk profile of the entity such that some audits will be more in-depth while others may have a reduced scope which will require less independent contractor resources.

- NPCC total overhead expenses, such as office rent and office costs, will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- Software development costs related to CMEP Data Administration Application (CDAA) and Compliance Issues Tracking System (CITS) enhancements are projected to continue into 2015.

Compliance Monitoring and Enforcement and Organization Registration and Certification Program

Funding sources and related expenses for the compliance enforcement and organization registration and certification section of the 2015 business plan are shown in the table below.

Statement of Activities and Capital Expenditures
2014 Budget & Projection, and 2015 Budget
Compliance Monitoring and Enforcement and Organization Registration and Certification

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 7,991,503	$ 7,991,503	$ -	$ 8,406,767	$ 415,263
Penalty Sanctions	87,868	87,868	-	161,378	73,510
Total ERO Funding	**$ 8,079,371**	**$ 8,079,371**	**$ -**	**$ 8,568,145**	**$ 488,774**
Membership Dues	-	-	-	-	-
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding (A)	**$ 8,079,371**	**$ 8,079,371**	**$ -**	**$ 8,568,145**	**$ 488,774**
Expenses					
Personnel Expenses					
Salaries	$ 2,287,504	$ 2,287,504	$ -	$ 2,393,832	$ 106,328
Payroll Taxes	162,571	162,571	-	162,511	(59)
Benefits	537,087	537,087	-	479,499	(57,588)
Retirement Costs	298,890	298,890	-	284,206	(14,684)
Total Personnel Expenses	**$ 3,286,052**	**$ 3,286,052**	**$ -**	**$ 3,320,048**	**$ 33,997**
Meeting Expenses					
Meetings	$ 25,000	$ 25,000	$ -	$ 32,000	$ 7,000
Travel	375,000	375,000	-	360,000	(15,000)
Conference Calls	-	-	-	-	-
Total Meeting Expenses	**$ 400,000**	**$ 400,000**	**$ -**	**$ 392,000**	**$ (8,000)**
Operating Expenses					
Consultants & Contracts	$ 1,394,433	$ 1,394,433	$ -	$ 1,728,000	$ 333,567
Office Rent	-	-	-	-	-
Office Costs	-	-	-	-	-
Professional Services	-	-	-	-	-
Computer & Equipment Leases	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Depreciation	-	-	-	-	-
Total Operating Expenses	**$ 1,394,433**	**$ 1,394,433**	**$ -**	**$ 1,728,000**	**$ 333,567**
Total Direct Expenses	**$ 5,080,485**	**$ 5,080,485**	**$ -**	**$ 5,440,048**	**$ 359,564**
Indirect Expenses	**$ 3,034,462**	**$ 3,034,462**	**$ -**	**$ 3,064,686**	**$ 30,225**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)	**$ 8,114,946**	**$ 8,114,946**	**$ -**	**$ 8,504,735**	**$ 389,788**
Change in Assets	**$ (35,575)**	**$ (35,575)**	**$ -**	**$ 63,410**	**$ 98,985**
Fixed Assets					
Depreciation	$ -	-	$ -	$ -	$ -
Computer & Software CapEx	108,000	108,000	-	122,000	14,000
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	(143,575)	(143,575)	-	(58,590)	84,985
Inc(Dec) in Fixed Assets (C)	**(35,575)**	**(35,575)**	**-**	**63,410**	**98,985**
TOTAL BUDGET (=B+C)	**$ 8,079,371**	**$ 8,079,371**	**$ -**	**$ 8,568,145**	**$ 488,774**
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	**$ (0)**	**$ (0)**	**$ -**	**$ (0)**	**$ 0**

Reliability Assessment and Performance Analysis Program

Reliability Assessment and Performance Analysis Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	5.83	5.83	0.00
Direct Expenses	$1,888,972	$1,958,577	$69,605
Indirect Expenses	$1,105,682	$1,116,695	$11,013
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	($52,315)	($21,349)	$30,967
Total Funding Requirement	$2,942,339	$3,053,923	$111,585

Program Scope and Functional Description

NPCC, through its top technical committee, the Reliability Coordinating Committee (RCC), integrates the deliverables of its Task Force's and Working Group's Reliability Assessment and Performance Analysis related activities. Consistent with the applicable NERC Reliability Standards, these efforts include:

- Reviewing the adequacy of the NPCC systems to supply load considering forecast demand, installed and planned supply and demand resources and required reserves in accordance with NPCC Reliability Directory No. 1 and other related reliability directories; and,
- Assessing the impact of planned transmission and resource additions or modifications on NPCC system reliability in accordance with NPCC Reliability Directory No. 1 and other related reliability directories.

Seasonal assessments of the overall NPCC resource adequacy assessments are performed and possible actions to mitigate any potential problems are identified. NPCC reviews operations and disturbances both internal and external to the Region in order to identify any lessons to be learned and recommends any necessary follow-up actions.

If appropriate, enhancements to Regional Standards or NPCC's more stringent, Regionally-specific reliability requirements are also recommended. NPCC promotes and conducts both inter-Area and inter-Regional studies to enhance reliability and operational effectiveness, and provides a forum for the discussion and coordination of operating issues within the NPCC Region and with other Regions.

2015 Key Assumptions

Support of identified key NERC Reliability Assessment and Performance Analysis (RAPA) projects; [38] NERC and Regional Entities will gather data or perform analysis in support of U.S. Federal and NERC initiatives, such as:

- Report Recommendation from the "*NERC Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances (GMD) on the Bulk Power System*", including:
  i. enhancing system models in support of the study of GMD impacts;
  ii. Enhancing GMD notification procedures; and,
  iii. Determining optimum locations for monitoring capability on transformers, based on studies and operational experience.
- Follow-up study from the recommendations of the "*2013 NERC Special Reliability Assessment: Increasing Dependence on Natural Gas for Electric Power – Phase II: A Vulnerability and Scenario Assessment for the North American Bulk Power System;*"
- System frequency response analysis; and,
- Assessing reliability issues resulting from compliance to final EPA environmental regulations, reliable integration of new technologies as renewable energy, smart grid, energy storage, and/or reliability assessment of increased penetration of electric vehicles.

In support of NERC's 2015 Business Plan and Budget Program Area Services and Activities, NPCC will continue to:

- Vet proposed and future metric development, collection, and analysis with industry stakeholders and identify and spotlight trends through assessments of the availability data systems and metrics (e.g., TADS, DADS, GADS, TADS, SED, etc.)
- Conduct post-seasonal assessments (Summer and Winter) and additional scenario and special reliability assessments as required. Specialized contractors may be used to complete detailed analysis to support scenario assessments. Special reliability assessments currently proposed may include: changes in resource mix due to environmental regulations, electric/gas system interdependency, delays in proposed transmission development in the reliable integration of renewable resources.

In addition, NPCC supports:

- Development of NERC's Reliability Assessment Data System (RADS), [39] for the reporting and validation of the NERC Reliability Assessment Subcommittee Seasonal and Long-Term Reliability Assessment data requirements.

[38] In support of ERO Goal 4.- Identify the most significant risks to reliability, be accountable for mitigating reliability risks, and promote a culture of reliability excellence

[39] In support of ERO Goal 5.c - The ERO internal risks are understood and managed; ERO processes are effective, efficient, and continuously improved.

- Evaluation of a common set of probabilistic reliability indices and probabilistic-based work products to supplement the NERC Long-Term Reliability Assessments;
- Coordination with event analysis, lesson learned [40] and model validation activities. [41] Specialized contractors may be used to complete detailed analysis to support model data collection and validation;
- Support of NERC PMO IT deployments; [42] and,
- Provide support and technical input for related BES risks identified by the NERC Reliability Issues Steering Committee (RISC). [43]

Definition of the Bulk Electric System (BES) Definition [44]

Implementation of the Bulk Electric System (BES) definition and Exception Process as of the July 1, 2014 BES Effective Date is not expected to significantly impact resources requirements in this program area for 2015. NPCC's 2014 survey of its registered entities did not indicate that an overwhelming number of NPCC BES Exception requests would be sought based on the filed BES Definition. Based on the Commission approved BES Definition [45] and the NPCC BES 2014 survey results, the 2015 RAPA personnel should be sufficient to process any NPCC BES Exception requests received in 2015.

NPCC will use the NERC PMO developed BESnet application and related BES reference and guidance documents to assist industry in the implementation of the BES definition approved by the Federal Energy Regulatory Commission. The BES reference and guidance documents, processes and tool are designed to provide industry with certainty and clarity about the implementation of the revised BES definition.

The procedure to request an exception from application of the BES definition is set forth in Appendix 5C to the NERC Rules of Procedure, effective July 1, 2014. The REMG formed the BES Exception Process Working Group (BEPWG) in 2012 – comprised of representations from the eight Regional Entities and NERC staff - to help create an efficient and effective Regional mechanism for processing Entity self-determined BES notifications and BES Exception requests. The activities of the BEPWG are expected to continue in 2015, in order to provide a Regional forum for consistent Regional BES Exception request review and 'lessons learned.'

[40] In support of ERO Goal 4.b - Events and system performance are consistently analyzed for sequence, cause, and remediation to identify reliability risks and trends and lessons learned.
[41] In support of ERO Goal 4.d - Reliability models and data accurately represent system behavior and are shared among stakeholders.
[42] In support of ERO Goal 5.c - The ERO internal risks are understood and managed; ERO processes are effective, efficient, and continuously improved.
[43] In support of ERO Goal 4.a - Risks are identified and prioritized based on reliability impacts, cost and practicality of assessments, projected resources, and emerging issues.
[44] In support of ERO Goal 2.a - The ERO registers and deregisters entities commensurate with risk to the BES and ensures all key reliability entities are certified to have essential capabilities.
[45] FERC Order Accepting the Revised [BES] Definition at: http://www.nerc.com/pa/RAPA/BES%20DL/2014-03-20%20BES%20-%20FERC%20Order%20Approving%20Revised%20Definition.pdf

Eastern Interconnection Reliability Assessment Group [46]

The primary function of the Eastern Interconnection Reliability Assessment Group (ERAG) is to augment reliability of the bulk-power system in the Eastern Interconnection through periodic reviews of generation and transmission expansion. These assessments are conducted by the ERAG Steering Committees. In addition, ERAG has the responsibility to develop the annual set of seasonal and future steady state and dynamic simulation base cases for use by the Regional Entities and other industry groups in the Eastern Interconnection. This is done through the ERAG Multi-Regional Modeling Working Group (MMWG). NPCC participates in the ERAG activities as one of the six Eastern Interconnection Regional Entities.

NPCC RAPA staff participates with the ERAG Management Committee and acts as the liaison between the ERAG MMWG and the NPCC SS-37 Working Group; activities include:

Management Committee Activities

- ✓ Oversee the steady state and dynamic simulation base case development;
- ✓ Make necessary changes to the modeling of governor-turbine control systems to achieve frequency response that more closely reflects actual response during system frequency deviation events. Oversee ERAG Multi-Regional Modeling Working Group (MMWG) changes to the dynamics base cases;
- ✓ Continue the review of the NERC governor survey information to assess how to revise the governor-turbine plant control models at most generators;
- ✓ Review the 2015 Summer and 2015-2016 Winter Assessments, including, the MRSS (MRO-RFC-SERC-SPP) and the R-N (RFC-NPCC) Assessments of anticipated inter-Regional, inter-Balancing Authority transfer limit conditions and sensitivities;
- ✓ Participate in discussions with NERC staff, North American Transmission Forum, NERC System Analysis and Modeling Subcommittee, FERC staff and possibly North American Generation Forum representatives regarding base case modeling improvements and future general industry modeling improvements;
- ✓ Develop ERAG Strategic Direction (i.e. anticipated new developments in MMWG process and system assessments); and,
- ✓ Confirm MMWG cases and assessments continue to have sufficient protections in place for use and transmittal of confidential data and information.

Multi-Regional Modeling Working Group Items

- ✓ Complete the steady state and dynamic simulation base cases for the 2015 series of cases;
- ✓ Complete necessary changes to the modeling of governor-turbine control systems to achieve frequency response that more closely reflects actual response during system frequency deviation events;
- ✓ Continue the review of the NERC governor survey information to assess how to revise the governor-turbine plant control models at most generators. Recommend the necessary changes in the models for specific generators;
- ✓ Incorporate dispatch information into the future and seasonal ERAG MMWG base cases so that the dispatches are more closely aligned with economic dispatch practices;

[46] In support of ERO Goal 4.d - Reliability models and data accurately represent system behavior and are shared among stakeholders.

- ✓ Determine how the Regional MMWG case development processes will change due to the use of the new web-based System Dynamics Data Base program;
- ✓ Verify procedures in the MMWG manual are followed;
- ✓ Check and confirm that the dynamic model data passes all applicable checks and acceptance criteria. Include 60 second steady state simulation of each case to detect numerical errors; and,
- ✓ Apply changes to the MMWG dynamics case so they are available for interconnection dynamics studies.

System Assessments Items

- ✓ Completion of 2015 Summer and 2015-2016 Winter Assessments, including, the MRSS and the R-N Assessments of anticipated inter-Regional, inter-Balancing Authority transfer limit conditions and sensitivities; and,
- ✓ Take additional steps to achieve consistency among the MRSS and the R-N study forums assessments and practices. Make additional recommendations to the ERAG Management Committee on how to complete this process.

NERC [47]

Through its Task Forces and Working Groups, NPCC will continue to provide the NPCC Regional perspective with active NPCC RAPA staff participation on the NERC Planning and Operating Committees and key related NERC Subcommittees, Task Forces and Working Groups:

- ✓ Reliability Assessment Data Working Group (RADWG);
- ✓ Protection System Mis-operations Task Force (PSMTF);
- ✓ Spare Equipment Database Task Force (SEDTF);
- ✓ Demand Response Availability Data System Working Group (DADSWG);
- ✓ Generating Availability Data System Working Group (GADSWG);
- ✓ Transmission Availability Data System Working Group (TADSWG);
- ✓ Model Validation Working Group (MVWG);
- ✓ Reliability Assessment Subcommittee (RAS) - Seasonal and Long-Term Reliability Assessments;
- ✓ System Analysis and Modeling Subcommittee (SAMS);
- ✓ Performance Analysis Subcommittee (PAS);
- ✓ Regional support and coordination of the NERC:
  - o Generator Availability Data System (GADS);
  - o Demand Availability Data System (DADS);
  - o Transmission Availability Data System (TADS);
  - o Spare Equipment Data Base System (SEDS);
- ✓ Incorporating any probabilistic reliability metrics required for the 2015 NERC Long-Term Reliability Assessment through the NPCC 2015 Long Range Adequacy Overview;
- ✓ Providing analytic support to ERO-RAPA group for the:
  - o Analysis of Relay and Special Protection System mis-operations;
  - o Regional coordination of data required for the calculation of metrics proposed by the NERC Reliability Metrics Working Group; and,
  - o Other activities as directed by the ERO-Executive Management Group.

[47] In support of ERO Goal 4 - Identify the most significant risks to reliability, be accountable for mitigating reliability risks, and promote a culture of reliability excellence.

As well as:

- ✓ Updating the NPCC Electric System Map; Producing the annual NPCC Load, Capacity, Energy, Fuels, and Transmission (LCEFT) Report
- ✓ Liaison with the New York Defensive Strategies Working Group in coordination and implementation of Synchro-Phasor measurement devices on the NPCC and neighboring systems and monitor related efforts of the NERC North American Synchro-Phasor Initiative;
- ✓ Processing BES Exception requests received through the BES Exception Process;
- ✓ Participating in on-going NERC analysis of the Eastern Interconnection Frequency Response;
- ✓ Developing NPCC guidelines for load modeling in system reliability studies;
- ✓ Conducting NPCC resource adequacy assessments addressing impacts of emerging reliability issues identified by NERC (e.g., environmental requirements, gas-electric system interdependency, distributed generation, delays in transmission plans, etc.);
- ✓ Coordinating any resulting NPCC inter-Area reliability analyses required to assess the proposed integration of related large-scale renewable resource proposals from Regional activities;
- ✓ Completing the 2015 NERC Seasonal (and post Seasonal) Reliability Assessments; and,
- ✓ Completing the 2015 NERC Long-Term Reliability Assessment.

2015 Goals and Key Deliverables

Task Force on Coordination of Planning

The primary mission of the NPCC Task Force on Coordination of Planning (TFCP) is to promote reliability through the coordination of NPCC Area and NERC planning processes and activities. In addition, the TFCP provides technical support regarding operating expertise to the NPCC Regional Standards Committee and the NPCC Compliance Committee as requested.

TFCP activities include, but are not limited to:

- Leading the NPCC Task Force review of the revision of NPCC criteria, guidelines, and procedures related to planning, and of those documents which provide for the uniform implementation, interpretation and monitoring of compliance with criteria, guidelines and procedures related to planning.
- Supporting the NPCC Directory Project by either drafting, reviewing or approving directories.
- Coordinating, monitoring, reviewing, and making recommendations on proposed or modified Special Protection Systems.
- Facilitating Wide-Area Planning by supporting the Joint ISO/RTO Planning Committee Activities, implementation of the Northeast Planning Protocol, and performing any NPCC interconnection reliability analyses, as required.
- Reviewing the overall reliability of the NPCC Areas and performing multi-Area probabilistic reliability assessments.
- Identifying and assisting in the development of new Regional Reliability Standards.
- Assisting the NPCC Compliance Subcommittee, to monitor and coordinate the compliance efforts of the Areas with NPCC planning documents and registered entities with NERC Reliability Standards.

- Reviewing the Standards Authorization Requests and NERC Reliability Standards as well as participating in the NERC process. Educating and informing NPCC membership and registered entities of developments.
- Ensuring coordination of data and assumptions for conducting NPCC planning studies (i.e. load forecasts, reserve requirements, DOE EIA 411 data, and new facilities)
- Monitoring the activities of other NPCC Task Forces to ensure coordination with planning activities.
- Reviewing the adequacy of the NPCC systems to supply load considering forecast demand, installed and planned supply and demand resources and required reserve margins in accordance with NPCC Directory No. 1 based on a schedule set forth in the Reliability Assessment Program.
- Coordinating the review of the compliance of future Area plans with the Basic Criteria, including an analysis of resource and transmission system additions, and the potential inter-Area effects of special protection systems, in accordance with NPCC Reliability Directory No.1 based on a schedule set forth in the Reliability Assessment Program. (Specific projects, which in the opinion of the Task Force could have an impact on the reliability of the NPCC Bulk Power System, may be reviewed outside of the set schedule).

Key TFCP Reliability Assessment and Performance Analysis Deliverables

- ✓ Coordinating activities related to reactive power and voltage control practices, which includes Under Voltage Load Shedding (UVLS) with the Task Force on Coordination of Operation and the Task Force on System Studies to ensure that developments in the NERC Planning Committee and its Subcommittees are addressed.
- ✓ Monitoring the actions of the NERC Performance Analysis Subcommittee (PAS).
- ✓ Monitoring the actions of the NERC System Analysis and Modeling Subcommittee (SAMS).
- ✓ Overseeing the A-10 BPS Implementation Plan.
- ✓ Overseeing the summer 2015 and winter 2015-2016 NPCC multi-area probabilistic reliability evaluations.
- ✓ Overseeing the 2015 NPCC Long-Range Adequacy Overview.
- ✓ Evaluating and approving Balancing Authority Area Transmission Reviews.
- ✓ Coordinating, monitoring, reviewing, and making recommendations on the retirement of existing in-service Special Protection Systems (SPS); and the implementation of proposed new or modified Special Protection Systems.
- ✓ Review the NPCC SPS criteria with respect to proposed NERC SPS Standards.
- ✓ Monitoring industry practices and making recommendations to NPCC on transmission adequacy standards related to intermittent generation such as wind or solar-voltaic.
- ✓ Reviewing and giving direction to other task forces on changes required to the Underfrequency Load Shedding (UFLS) program required to take into account increasing amounts of distribution connected generation and/or intermittent generation.
- ✓ Evaluating and recommending approval of NPCC Balancing Authority Area Resource Adequacy Assessments.
- ✓ Monitoring the developments in demand resources, energy efficiency, distributed generation and conservation methods including all intermittent renewable resources.
- ✓ Conducting resource adequacy assessment studies addressing emerging reliability issues as identified by the NERC Planning Committee (e.g., environmental requirements, etc.)
- ✓ Supporting Joint ISO/RTO Planning Committee activities.

- ✓ Facilitating Wide-Area Planning through participation in Regional and coordinating any resulting required inter-Area Reliability Assessment of the proposed integration related large-scale renewable resource proposals.
- ✓ Completion of the NERC 2015 Long-Term Reliability Assessment.
- ✓ Completion of the 2015 Review of NPCC Interconnection Assistance Reliability Benefits Study.
- ✓ Review NERC Events Analysis Lessons Learned for consideration in TFCP activities and processes.

Task Force on System Studies

The primary mission of the NPCC Task Force on System Studies (TFSS) is to provide active overall coordination of system studies of the reliability of the interconnected bulk power systems and for the review of certain NPCC documents. In addition, the TFSS provides technical support regarding operating expertise to the NPCC Regional Standards Committee and the NPCC Compliance Committee as requested.

The activities of the TFSS include, but are not limited to:

- Participating with the Task Force on Coordination of Planning, the Task Force on Coordination of Operation, and the Task Force on System Protection in reviews of the NPCC Reliability Directory No.1 and other NERC Reliability Standards and NPCC criteria, guidelines, procedures and documents which provide for the uniform implementation, interpretation and monitoring of conformance to criteria, guidelines and procedures related to system studies.
- Conducting NPCC Balancing Authority Area Reviews, in accordance with NPCC Reliability Directory No. 1, based on material presented by the Balancing Authority Areas. These reviews will assess the impact of planned transmission and resource additions or modifications on system reliability, and determine the Balancing Authority Area's conformance with the NPCC Basic Criteria.
- Reviewing and approving changes to Balancing Authority Areas' lists of bulk power system elements, in accordance with the *Classification of Bulk Power System Elements* (Document A-10). Annually review and update the NPCC BPS List.
- Reviewing and classifying new and modified Special Protection Systems, in accordance with NPCC Reliability Directory No. 7. Annually reviewing and updating the NPCC Special Protection System List.
- Conducting such load flow, transient stability, and other studies as required analyzing the overall reliability of the planned bulk power transmission systems of NPCC and the interconnections between NPCC and other Regional reliability organizations. As a part of this effort, analyze potential inter-Area effects of Special Protection Systems.
- Conducting analytical studies as appropriate to support the coordination of system planning, system operation and system protection in NPCC.
- Maintaining, through the SS-37 Working Group, a library of load flow base cases and associated dynamics data, for use in and support of Balancing Authority Area Reviews, overall transmission assessments, operational studies, inter-Regional studies, etc. Coordinate this effort with the NERC inter-Regional base case development process.
- In conjunction with other Task Forces, reviewing major system disturbances to ascertain the adequacy of the interconnected systems. Also, reviewing any associated recommendations for system modifications and considering the need for criteria changes.

- Identifying and recommending improved system study techniques. This includes, but is not limited to, the following:
  - improved techniques and models for power system simulation;
  - improved techniques for power system Reliability Assessment;
- Conducting a periodic review of the adequacy of the NPCC underfrequency load shedding program. Annually reviewing and updating the NPCC underfrequency load shedding database.
- Maintaining a listing and monitoring the status of major transmission and generation projects within NPCC.
- Maintaining liaison with other NPCC Task Forces and report to the Reliability Coordinating Committee as required.
- Monitoring the work of industry research and development organizations such as the IEEE, Canadian Electricity Association, Electric Power Research Institute, CIGRE and other technical organizations.
- Annually developing updates to the NPCC Electric System Map

Key TFSS Reliability Assessment and Performance Analysis Deliverables:

- ✓ Conducting Balancing Authority Area reviews, in accordance with the *Guidelines for NPCC Area Transmission Reviews* (Appendix B of NPCC Reliability Directory No. 1), based on material presented by the Balancing Authority Areas. These reviews assess the impact of planned transmission and resource additions or modifications on system reliability, and determine the Area's conformance with the NPCC Basic Criteria. Through the Area Transmission Reviews, re-evaluate the performance and classification of existing SPSs and Dynamic Control Systems as appropriate.
- ✓ Reviewing and classifying new and modified Special Protection Systems, in accordance with NPCC Reliability Directory No. 7 *Procedure for NPCC Review of New or Modified Bulk Power System Special Protection Systems* as required.
- ✓ Reviewing and approving changes to the Balancing Authority Areas' lists of bulk power system elements, in accordance with the *Classification of Bulk Power System Elements* (Document A-10), as required.
- ✓ Updating the NPCC Bulk Power System List.
- ✓ Through the ad hoc Load Modeling Task Force, address the recommendations from the SS-38 Load Modeling White Paper regarding the use of dynamic load models for transient stability analysis.
- ✓ Perform the Overall NPCC Transmission Assessment.
- ✓ Reviewing and updating NPCC Undervoltage Load Shedding Database.
- ✓ Participation in on-going NERC analysis of the Eastern Interconnection Frequency Response.
- ✓ Through the SS-37 Working Group, develop the annual library of power flow base cases and associated dynamic models for use by NPCC members and input into the development of the MMWG library of power flow and dynamic cases and databases for the Eastern Interconnection
  - i. Final development of NPCC power flow models for 2015
  - ii. Final development of NPCC dynamic models for 2015
  - iii. Address wind modeling issues including maintaining a database of NPCC wind models for use in the MMWG library of power flow and dynamic cases and databases for the Eastern Interconnection.
- ✓ Annually performing event replication and exercise the procedure. Reviewing existing Regional criteria and procedures for validation of data used in power flow and dynamic

simulations by benchmarking against actual system performance. If the existing criteria or procedures are found to be deficient, propose changes to provide for adequate data validation

- ✓ Updating the NPCC SS-37 Working Group Procedure Manual and other related documents including the Master Tie line Data, and Interchange Schedule, as required.
- ✓ Providing mid-term updates to the Library of NPCC/MMWG cases
- ✓ Enhancing the governor modeling on a unit by unit basis suitable for use in the system simulation.
- ✓ Annually reviewing and updating a list of NPCC underfrequency load shedding.
- ✓ Coordinate activities with those of the New York State Defensive Strategies Working Group, regarding the coordination and implementation of Synro-Phasor measurement devices.
- ✓ Incorporate NPCC guidelines for load and power system modeling approved by the RCC
- ✓ Classification of Bulk Power System Elements.
- ✓ Participate at Siemens PTI User Group meetings to provide PSSE program enhancements
- ✓ Supporting Regional system studies to integrate large-scale renewable resources.
- ✓ Provide support to NERC Event Analysis process, as needed.
- ✓ Develop updates to the NPCC Electric System Map.
- ✓ Provide support to the NERC Model Validation Working Group (MVWG) as needed.
- ✓ Review NERC Events Analysis Lessons Learned for consideration in TFSS activities and processes.

Task Force on System Protection (TFSP)

The purpose of the NPCC Task Force on System Protection (TFSP) is to promote the reliable and efficient operation of the interconnected bulk power systems in Northeastern North America through the establishment of directories, criteria, guidelines, and procedures and coordination of design, relative to the protection associated with the bulk power systems. In addition, the TFSP provides technical support regarding operating expertise to the NPCC Regional Standards Committee and the NPCC Compliance Committee as requested.

The Reliability Assessment and Performance Analysis activities of the TFSP include, but are not limited to:

- Assessing proposed protection systems and special protection systems in accordance with NPCC Reliability Directory No. 4 and No. 7.
- Reviewing and analyzing the performance of protection systems following selected major power system disturbances and events, inside as well as outside NPCC in accordance with NPCC Reliability Directory No. 4. Issue recommendations for changes to NPCC Documents, as appropriate.
- Providing technical advice on protection issues to NPCC and coordinate with other Task Forces on the application of Intelligent Electronic Devices (IEDs) that include functions related to energy management systems in addition to their protective functions, in order to safeguard the integrity of the protective functions.
- Through the SP-7 Working Group, review, on a quarterly basis all protection system (including special protection system) misoperations reported to NPCC.
- Reviewing and assessing significant protection issues of common interest or informational value.
- Reviewing and assessing regulatory and industry based documents as they relate to system protection.

- Maintaining an effective liaison with North America groups working in the protection areas (for example: NERC System Protection & Control Subcommittee.)
- Exchanging information with other power pools, Regional Reliability Councils, Regional Transmission Organizations and other industry groups on matters concerned with system protection.
- Identifying the need for special studies and new documents, recommend action to the Reliability Coordinating Committee.

Key TFSP Reliability Assessment and Performance Analysis Deliverables:

- ✓ Assessing proposed protection systems and special protection systems for compliance with NPCC Directory No. 4 and No. 7 criteria.
- ✓ Reviewing and analyzing the performance of protection systems in power system disturbances and events, brought to the attention of the Task Force, inside as well as outside NPCC in accordance with *Procedures for Task Force on System Protection Review of Disturbances* (Document C-30). Issuing recommendations for changes to NPCC Documents, as appropriate.
- ✓ Develop a new NPCC Directory for Disturbance Monitoring Equipment for related criteria, guides and procedures.
- ✓ Participate or serve as lead Task Force in the development and/or implementation of Regional Reliability Standards.
- ✓ Providing support to the NERC Event Analysis process as required.
- ✓ Participate in the ongoing development and submission of NPCC input into the development of related NERC Reliability Standards.
- ✓ Conducting any follow-up to the bulk power system protection risk assessment as directed by the Reliability Coordinating Committee.
- ✓ Through the SP-7 Working Group, monitor the review of protection system (including special protection system) mis-operations as they occurred in the NPCC Region and participation in providing the NPCC input for NERC Metric ALR4-1 on Protection Mis-operations.
- ✓ Monitor and review industry activities on the mitigation of the effects of SMD on protection systems. Report to RCC on any significant findings.
- ✓ Review mitigations and/or progress reports for BPS Risk Reduction Implementation at each meeting and annually report to the RCC on the status of this implementation.
- ✓ Participate in the development and submission of NPCC inputs/comments into the development of protection related NERC technical documents.
- ✓ Review best practices from its members and industry to pull together design considerations for the new IEC 61850 protection implementation with the output being possible additions to NPCC Directory No. 4 and Directory No. 7.
- ✓ Review NERC Events Analysis Lessons Learned for consideration in TFSP activities and processes.

Task Force on Coordination of Operation

The NPCC Task Force on Coordination of Operation (TFCO) facilitates the coordination of operations among the NPCC Reliability Coordinator areas and adjacent NERC Regions to enhance the reliability of the bulk power system. In addition, the TFCO provides technical support regarding operating expertise to the NPCC Regional Standards Committee and the NPCC Compliance Committee as requested.

The activities of the NPCC TFCO include, but are not limited to:

- Conducting seasonal reviews of the overall reliability of the generation and transmission systems in NPCC, and coordinating these efforts with parallel assessments conducted by the NPCC Task Force on Coordination of Planning and by NERC. Reviewing the operational preparedness of NPCC and recommending possible actions to mitigate any potential problems identified for each operating period.
- Reviewing operations and system disturbances and providing any necessary follow-up, including the recommendation of remedial or mitigating actions.
- Facilitating the reliable operational integration of new bulk power system facilities.
- Coordinating the development of operating NPCC requirements and procedures affecting the reliability and operability of the bulk power system in coordination with, and as directed by, NERC and NPCC.
- Promoting and sponsoring inter-Balancing Authority Area and inter-Regional studies to enhance reliability and operational effectiveness of the bulk power system.
- Providing coordination of operating issues with other NPCC Task Forces and other Regions.
- Reviewing, and acting upon, NERC actions, motions and recommendations in relation to the operation of the power system.
- Formulating the position of the TFCO on NERC Standards, and providing this position to the NPCC Regional Standards Committee as appropriate.
- Providing assistance as requested by the NPCC Regional Standards Committee in the development of Regional Standards and Directories.
- Providing assistance as requested by the NPCC Compliance Committee in monitoring and coordinating the compliance efforts of the registered entities of NPCC.

Key TFCO Reliability Assessment and Performance Analysis Deliverables:

- ✓ Review and analyze the performance of Simultaneous Activation of Reserve implementation following an event to enhance the process. Manage the implementation of action items emanating from the NERC report, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System-June 2010," and its subsequent reports:
  - ➢ Severe Impact Resilience Severe Impact Resilience Task Force
  - ➢ Geomagnetic Disturbance Task Force
  - ➢ Cyber Attack Task Force
  - ➢ Spare Equipment Database Task Force
  - ➢ Smart Grid Task Force
- ✓ Monitor the development of the NERC North American Synchro-Phasor Initiative in its effort to establish an effective control monitoring tool.
- ✓ Provide assistance to the NPCC Regional Standards Committee in the second phase of the NPCC directories process.
- ✓ Review NPCC Reliability Coordinator Area Restoration Plans.
- ✓ Complete the NPCC 2015 summer and winter Operational Reliability Assessments.
- ✓ Completion of the NERC 2015 Seasonal Reliability Assessments.
- ✓ Review NERC Events Analysis Lessons Learned for consideration in TFCO activities and processes.
- ✓ Support the implementation of the NERC Cyber Standards, as required.

NPCC Regulatory/Governmental Affairs Advisory Group

The purpose of the NPCC Regulatory/Governmental Affairs Advisory Group is to promote NPCC interaction and coordination with Federal/State/Provincial governmental and/or regulatory agencies on a coordinated Regional basis, and identify and develop policy input for NPCC and Northeast Regional governmental and/or regulatory bodies.

The NPCC Governmental/Regulatory Affairs Advisory Group provides a forum where industry and governmental and/or regulatory representatives can exchange views and strive to develop consensus policy recommendations on reliability issues specific to the NPCC Region (Northeastern United States and Eastern Canada) and share actionable information among NPCC, NERC and other related governmental and/or regulatory agencies related to Regional energy and reliability matters.

Based on the portion of professional/technical staff time and other resources devoted to Reliability Assessment and Performance Analysis, NPCC estimates that it will expend 21 percent of its resources on these activities.

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- U.S. Penalty Sanctions remitted from 7/1/13 through 6/30/14 reduce U.S. LSE designee assessments for 2015.

Personnel Expenses

- NPCC anticipates no need to hire additional personnel in this program area in 2015.
- Salaries expense reflects implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Retirement expense decreased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.

Meeting and Travel Expenses

- While the amount of activity continues to increase in 2015, due to the volume of work described above, meeting expenses will be minimized to the extent possible due to continued efforts to keep costs down by holding meetings via conference calls and internet meetings, which are budgeted as a part of G&A and then allocated to the direct programs through indirect expenses, conducting meetings at the NPCC offices or member facilities, as well as negotiating lower meeting space rental rates.

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Reliability Assessment and Performance Analysis Program

Funding sources and related expenses for the Reliability Assessment and Performance Analysis section of the 2015 business plan are shown in the table below.

Statement of Activities and Capital Expenditures
2014 Budget & Projection, and 2015 Budget
Reliability Assessment and Performance Analysis

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 2,910,322	$ 2,910,322	$ -	$ 2,995,121	$ 84,799
Penalty Sanctions	32,017	32,017	-	58,802	26,785
Total ERO Funding	**$ 2,942,339**	**$ 2,942,339**	**$ -**	**$ 3,053,923**	**$ 111,585**
Membership Dues	-	-	-	-	-
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding (A)	**$ 2,942,339**	**$ 2,942,339**	**$ -**	**$ 3,053,923**	**$ 111,585**
Expenses					
Personnel Expenses					
Salaries	$ 904,028	$ 904,028	$ -	$ 937,098	$ 33,070
Payroll Taxes	60,329	60,329	-	61,387	1,058
Benefits	226,225	226,225	-	196,252	(29,973)
Retirement Costs	190,390	190,390	-	172,840	(17,550)
Total Personnel Expenses	**$ 1,380,972**	**$ 1,380,972**	**$ -**	**$ 1,367,577**	**$ (13,395)**
Meeting Expenses					
Meetings	$ 45,000	$ 45,000	$ -	$ 41,000	$ (4,000)
Travel	175,000	175,000	-	185,000	10,000
Conference Calls	-	-	-	-	-
Total Meeting Expenses	**$ 220,000**	**$ 220,000**	**$ -**	**$ 226,000**	**$ 6,000**
Operating Expenses					
Consultants & Contracts	$ 275,000	$ 275,000	$ -	$ 365,000	$ 90,000
Office Rent	-	-	-	-	-
Office Costs	13,000	13,000	-	-	(13,000)
Professional Services	-	-	-	-	-
Computer & Equipment Leases	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Depreciation	-	-	-	-	-
Total Operating Expenses	**$ 288,000**	**$ 288,000**	**$ -**	**$ 365,000**	**$ 77,000**
Total Direct Expenses	**$ 1,888,972**	**$ 1,888,972**	**$ -**	**$ 1,958,577**	**$ 69,605**
Indirect Expenses	**$ 1,105,682**	**$ 1,105,682**	**$ -**	**$ 1,116,695**	**$ 11,013**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)	**$ 2,994,654**	**$ 2,994,654**	**$ -**	**$ 3,075,272**	**$ 80,618**
Change in Assets	**$ (52,315)**	**$ (52,315)**	**$ -**	**$ (21,349)**	**$ 30,967**
Fixed Assets					
Depreciation	$ -	-	$ -	$ -	$ -
Computer & Software CapEx	-	-	-	-	-
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	(52,315)	(52,315)	-	(21,349)	30,967
Inc(Dec) in Fixed Assets (C)	**(52,315)**	**(52,315)**	**-**	**(21,349)**	**30,967**
TOTAL BUDGET (=B+C)	2,942,339	2,942,339	-	3,053,923	111,585
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	**$ 0**	**$ 0**	**$ -**	**$ 0**	**$ 0**

Training, Education, and Operator Certification Program

Training, Education, and Operator Certification Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	0.10	0.10	0.00
Direct Expenses	$177,787	$180,222	$2,434
Indirect Expenses	$18,965	$19,154	$189
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	($897)	($366)	$531
Total Funding Requirement	$195,855	$199,010	$3,154

Program Scope and Functional Description

The NPCC Training, Education, and Operator Certification program supports NERC Rules of Procedure Section 900. The program provides education and training necessary to understand and operate the bulk electric system. The target audience of the program is bulk power system operating personnel - including system operations personnel, operations support personnel (engineering and information technology), supervisors and managers, and training personnel. This program also supports the administration of records necessary to maintain status as a NERC Continuing Education provider. NPCC staff training and development is incorporated within each respective program area.

Training Program Background and Description

NPCC establishes and coordinates programs for system operator training relating to inter-Reliability Coordinator area matters, criteria, terminology, standards and operating procedures and instructions. It develops and conducts training seminars, held twice yearly, at which potential operational problems for the coming season are discussed, the implementation of NPCC standards and procedures are discussed, significant disturbances are reviewed for lessons to be learned and table-top drills and communication and coordination exercises are conducted. The seminars promote camaraderie and better communication among system operators from the NPCC Reliability Coordinator Areas.

NPCC shares, evaluates and proposes new techniques and training aids as they become available; reviews opportunities to consolidate training among the NPCC Reliability Coordinators, which includes opportunities to share training material and training sessions and exchanges information on internal methods of system operator selection and training.

In addition, NPCC participates in the activities of the NERC Staff Training Group (STG). The main objective of the NERC STG is to coordinate the development of Regional Entity and NERC staff training and registered entity education materials to support and continually enhance reliability across North America for the benefit of all bulk electric system users, owners, and operators. The main focus of this group has been on NERC compliance auditor training.

Funding Drivers and Reliability Benefits

- Provide two high-quality continuing education seminars for system operators
    - System operators participating in the Seminars get exposure to NPCC issues and current industry operations topics, review recent NPCC or major external disturbances, discuss projected conditions for the coming summer or winter peak season and participate in hands on "table top exercises" pertaining to system operation practices. PJM operators also attend and participate in these seminars.
    - Seminar attendees also receive Continuing Education Hours (CEHs) and each Balancing Authority Area utilizes the seminar content by including it in their internal training programs to provide CEHs to all system operators
    - The seminars help to improve system operation coordination through better camaraderie among operators
- Review and revise the curriculum of the training seminars to better emphasize NERC standards, Regional Standards and business practices, NPCC wide-area operations and Regionally-specific criteria and procedures.[48]
- Enhance the system operator's awareness and knowledge of the standards, criteria and procedures they apply in real time operation.[49]
- Provide more sharing of new training approaches, exchange of information on internal methods of system operator selection, training material and training sessions.
    - Enhance efficiency and cost savings in the training programs in the NPCC Balancing Authority Areas
- Provide a forum among NPCC Reliability Coordinator / Balancing Authority (RC / BA) Areas for sharing of approaches to meet the requirements of the NERC PER standards. The sharing of approaches used by some NPCC Areas to address the PER-005-1, Requirement 3.1 on Training using simulator technology has been especially valuable to CO-2 Working Group members.
- Determine what changes would be needed for the NPCC Reliability Coordinator / Balancing Authority Areas to meet proposed expanded Systematic Approach to Training (SAT) requirement for operations support staff in PER-005-2.

2015 Key Assumptions

NPCC will conduct two workshops in 2015, for NPCC Stakeholders, for the express purpose of providing the most current and applicable information related to the development of NERC and Regional Reliability Standards and the implementation of the Compliance Monitoring and Enforcement Program (CMEP). These workshops are specifically designed, primarily through the conduct of targeted breakout class room sessions and presentations on current industry related activities, to provide for the most efficient exchange of information between the NPCC Compliance and Standards Staff and the NPCC Stakeholders. Presentations in the past have been conducted by FERC, NERC and Stakeholder representatives in addition to NPCC Staff members. To supplement these workshops, NPCC is also considering expanding the use of on-

[48] In support of ERO goal 4.b. Provide lessons learned and recommendations from events and identified risks.
[49] In support of ERO goal 4.b. Analyze significant events to identify gaps in standards, compliance effectiveness, registration, and risk controls effectiveness.

line webinars. These webinars will focus on a specific topic pertinent to developments related to compliance program implementation, standards development or technical topics.

NPCC also regularly conducts spring and fall System Operator Seminars. These seminars involve system operators from the NPCC Reliability Coordinator / Balancing Authority Areas and PJM. These will be held in early May and early November.

With the exception of meeting expenses, it is proposed that the NPCC resources to support Training and Education will remain virtually unchanged for the calendar year. In 2015, to be consistent with NERC and other Regional Entities, NPCC will charge for participation in NPCC workshops in an effort to defray some of the costs.

2015 Goals and Key Deliverables

- Prepare and conduct the spring and autumn NPCC System Operator Seminars
- Review approaches to reliability related-task definition, task instruction, and instruction tracking on an individual basis. Coordinate the effects of the PER-005-2 expanded SAT training requirements within the NPCC RC / BA Area programs.
- Expand the content of the Reliability Coordinator training programs, based on the new requirements generated by PER-005-2.
- Continue collaboration and sharing of the intended RC / BA approaches, experiences and materials to task identification and training development associated with NERC Standard PER-005-2.
- Create and expand the restricted-access NPCC repository of training resources and learning verification activities addressing fundamental power system topics, training methods and operation procedure training exercises, which may be shared as elements of operator training in compliance with NERC Standard PER-005, “System Personnel Training”.
- Participate in NERC Staff Training Group activities and provide NPCC input to the development of training policies by this group.

Based on the portion of professional/technical staff time and other resources devoted to training, education, and operator certification, NPCC estimates that it will expend 1 percent of its resources on this activity.

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- U.S. Penalty Sanctions remitted from 7/1/13 through 6/30/14 reduce U.S. LSE designee assessments for 2015.

Personnel Expenses

- NPCC anticipates no need to hire additional personnel in this program area in 2015.
- Salaries expense reflects implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Retirement expense decreased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Training, Education, and Operator Certification Program

Funding sources and related expenses for the training, education, and operator certification section of the 2015 business plan are shown in the table below.

Statement of Activities and Capital Expenditures
2014 Budget & Projection, and 2015 Budget
Training, Education, and Operator Certification

		2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding						
ERO Funding						
	ERO Assessments	$ 131,306	$ 131,306	$ -	$ 134,001	$ 2,695
	Penalty Sanctions	549	549	-	1,009	459
Total ERO Funding		**$ 131,855**	**$ 131,855**	**$ -**	**$ 135,010**	**$ 3,154**
	Membership Dues	-	-	-	-	-
	Testing Fees	-	-	-	-	-
	Services & Software	-	-	-	-	-
	Workshops	64,000	64,000	-	64,000	-
	Interest	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
Total Funding (A)		**$ 195,855**	**$ 195,855**	**$ -**	**$ 199,010**	**$ 3,154**
Expenses						
Personnel Expenses						
	Salaries	$ 17,448	$ 17,448	$ -	$ 18,460	$ 1,012
	Payroll Taxes	1,063	1,063	-	1,274	211
	Benefits	4,500	4,500	-	4,052	(448)
	Retirement Costs	4,776	4,776	-	4,436	(341)
Total Personnel Expenses		**$ 27,787**	**$ 27,787**	**$ -**	**$ 28,222**	**$ 434**
Meeting Expenses						
	Meetings	$ 135,000	$ 135,000	$ -	$ 137,000	$ 2,000
	Travel	15,000	15,000	-	15,000	-
	Conference Calls	-	-	-	-	-
Total Meeting Expenses		**$ 150,000**	**$ 150,000**	**$ -**	**$ 152,000**	**$ 2,000**
Operating Expenses						
	Consultants & Contracts	$ -	$ -	$ -	$ -	$ -
	Office Rent	-	-	-	-	-
	Office Costs	-	-	-	-	-
	Professional Services	-	-	-	-	-
	Computer & Equipment Leases	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
	Depreciation	-	-	-	-	-
Total Operating Expenses		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Total Direct Expenses	**$ 177,787**	**$ 177,787**	**$ -**	**$ 180,222**	**$ 2,434**
Indirect Expenses		**$ 18,965**	**$ 18,965**	**$ -**	**$ 19,154**	**$ 189**
Other Non-Operating Expenses		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)		**$ 196,753**	**$ 196,753**	**$ -**	**$ 199,376**	**$ 2,623**
Change in Assets		**$ (897)**	**$ (897)**	**$ -**	**$ (366)**	**$ 531**
Fixed Assets						
	Depreciation	$ -	-	$ -	$ -	$ -
	Computer & Software CapEx	-	-	-	-	-
	Furniture & Fixtures CapEx	-	-	-	-	-
	Equipment CapEx	-	-	-	-	-
	Leasehold Improvements	-	-	-	-	-
	Allocation of Fixed Assets	(897)	(897)	-	(366)	531
Inc(Dec) in Fixed Assets (C)		**(897)**	**(897)**	**-**	**(366)**	**531**
TOTAL BUDGET (=B+C)		195,855	195,855	-	199,010	3,154
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)		**$ (0)**	**$ (0)**	**$ -**	**$ (0)**	**$ 0**

Situation Awareness and Infrastructure Security Program

Situation Awareness and Infrastructure Security Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	3.00	3.00	0.00
Direct Expenses	$922,070	$937,689	$15,619
Indirect Expenses	$568,962	$574,629	$5,667
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	($26,920)	($10,986)	$15,935
Total Funding Requirement	$1,464,111	$1,501,332	$37,221

Program Scope and Functional Description

The Situation Awareness and Infrastructure Security Program is the combination of near real time awareness of conditions on the bulk power system with the programs necessary to increase the physical and cyber security of the electricity infrastructure, including the operation and maintenance of tools and other support services for the benefit of Reliability Coordinators and the system operators within the registered entities. Maintaining the real-time awareness of conditions on the interconnected bulk power systems by the NPCC Reliability Coordinator is critical to maintaining reliable operation within NPCC, including the communication of information concerning system conditions and abnormal events among the neighboring system operators responsible for the reliable operation of the bulk power systems. When a disturbance does occur, it is critical to use the event as a learning opportunity and provide a forum for the active coordination of reliability and operation among the NPCC Reliability Coordinator areas and neighboring NERC Regions to enhance the reliability of the interconnected bulk power system through the lessons to be learned which can be gleaned from such an event.

Event Analysis Program[50]

NERC and the industry pursue three avenues in the analysis of a disturbance: the identification of lessons to be learned, a formal cause code analysis and a review of applicable standards.

The Event Analysis Program recognizes that many events which occur on the bulk power system beyond the routine reporting requirements previously in place can have varying levels of significance to the electric system, providing otherwise unrealized lessons to be learned from these events and the trending of such events to identify possible reliability concerns. By integrating a "bottom-up" approach to a disturbance review within the framework of the NERC Event Analysis Program, consistency, comparability, flexibility and timeliness in the event analysis process will be promoted by NPCC, the registered entities and NERC in a collaborative initiative. Upon the identification of an event, the goal of the Event Analysis Program is to:

- identify what transpired;
- categorize the event within the NERC Event Analysis Program;

[50] In support of ERO Goal 4.b. Events and system performance are consistently analyzed for sequence, cause, and remediation to identify reliability risks and trends and lessons learned.

- establish the sequence of events;
- understand the essential root causes of the event;
- identify recommendations or corrective actions; and
- develop and disseminate to the industry, lessons to be learned so that the operational reliability of the bulk power system can be further enhanced.

In assessing any system event, it is recognized that, if the timely dissemination of lessons learned from an event or disturbance is to be realized, any potential compliance implications associated with an event must be addressed and dismissed. Throughout an event analysis effort, to make this process successful and complete, and to solidify the "bottom-up" approach, registered entities are encouraged to establish a liaison between the event analysis and compliance functions internal to the registered entity during the event analysis process. This serves to facilitate the development of a registered entity compliance self-assessment report which will perform a sufficiency review of the reliability standards deemed applicable to the event, assisting in the self-reporting of possible violations should any be discovered.

To complete this effort, the entity, the Region and NERC staff collaborate to assess the NERC Event Analysis Report and perform a formal cause code analysis, identifying a root cause and complementing any lessons learned gathered from the disturbance.

The adoption by NERC of the Event Analysis Program brings clarity and certainty about what system events are relevant to analyze and to what level of detail, targeting potential vulnerabilities to the reliability of the bulk power system for detailed and in depth analysis; only concise and succinct reviews are desired for more minor events. It also delineates the expectations of roles and responsibilities of the registered entities, NPCC and NERC in a uniform review of system disturbances by the industry, and, ultimately, the program promotes the timely development and dissemination of valuable lessons learned to the industry. The identification and tracking of emerging common elements in system events will further distinguish trends which may be of concern to reliability. By rigorously pursuing the lesser events on the system and learning from these disturbances, the larger event can be avoided or mitigated.

NPCC Staff works step-by-step with the registered entity in the total event analysis process, permitting the entity to assume the primary role in the initial analysis, the development of lessons learned which may benefit the industry and the Standards sufficiency review.

NERC Alert Process[51]

NPCC Staff works with the registered entities to appropriately respond to the NERC Alert system, a process through which notifications of potential threats to electric reliability are disseminated to the industry with the expectations placed on the entity proportional to the severity of the Alert being issued.

NPCC Staff is also working closely with the NERC Staff to incorporate greater efficiencies, industry input and precision into the NERC proposal for a more streamlined NERC Alert process which can disseminate critical information to the appropriate Subject Matter Expert within the organization who can promptly act on the alert.

[51] In support of ERO Goal 4.c. ERO supports industry situational awareness and cybersecurity preparedness and provides independent reliability information to policy makers.

Operational Status[52]

On an ongoing, but non-real time basis, NPCC monitors the operational status of the bulk power system and coordinates normal and pre-emergency communication, awareness and assistance in addition to the same during an emergency among the Reliability Coordinators within NPCC and its neighboring RCs: the New Brunswick Power Corporation, Hydro-Québec TransÉnergie, the ISO New England, Inc., the New York ISO and the Independent Electricity System Operator in Ontario. The industry is notified of significant bulk power system events that have occurred in one Reliability Coordinator Area, and which have the potential to impact reliability in other NPCC Reliability Coordinator Areas or Regions external to NPCC. These events include contingencies on the bulk power system, potential shortfalls of operating reserve, operating problems, potential security threats and potential threats or disruptions to the cyber systems.

The "NPCC Emergency Preparedness Conference Call Procedures" provide a mechanism that enables the Reliability Coordinator in NPCC, and, as circumstances may require, their counterparts in neighboring Regions, to rapidly communicate the status of current operating conditions, to facilitate the procurement of assistance during emergency conditions and to identify potential physical or cyber threats to the system.

Items of particular concern that can be discussed during the calls may include, but are not limited to, the following: anticipated weather conditions critical to the system or systems experiencing or projecting resource deficiencies; load forecast; largest first and second contingencies; potential need for emergency transfers; operating reserve requirements and expected available operating reserve capacity deficiencies; potential fuel shortages or potential fuel supply disruptions which could lead to energy shortfalls; identified or projected voltage conditions; status of short term transactions; additional capability available within four hours and additional capability available within twelve hours; generator outages; significant transmission outages; expected transfer limits and limiting elements; anticipated implementation of NERC Transmission Loading Relief (TLR); changes in the status of relay protection systems; arming of special protection systems not normally armed; and/or the application of abnormal operating procedures.

NPCC has also established a daily conference call to serve as a complement to the NPCC Emergency Preparedness Conference Call. The participants of the call are the Reliability Coordinators within NPCC and its neighboring RCs, the Midwest ISO and PJM. The conference call is implemented through a bridge, the initiation of the call quickly ringing all pre-selected telephones simultaneously. The goal of the call is to alert all Reliability Coordinators of emerging problems. If no system difficulties are anticipated for the day, no unnecessary information is to be discussed. Subjects for discussion are limited to credible events which could impact the ability of an entity to serve its load and meet its operating reserve obligations or would impose a burden to the interconnection, including the following: Projected Load; Adverse Weather; Operating Reserve; Generation; Transmission; and Sabotage. If conditions worsen in the course of the day, the NPCC Emergency Preparedness Conference Call will be implemented.

NPCC monitors the status of the bulk power system through the NERC Situational Awareness-FERC, NERC, Regions (SAFNR) initiative, a near real-time operating display for the United States portion of the Reliability Coordinators footprints of North America. Transmission voltage

[52] In support of ERO Goal 4.c. ERO supports industry situational awareness and cybersecurity preparedness and provides independent reliability information to policy makers.

levels of 230 kV and above are displayed, and the tool provides the ability to "drill down" to detailed bus information.

To ensure the capability for continued voice communications among NPCC and its Reliability Coordinators, a satellite telephone network was also established, and it is tested on a monthly basis. This back-up communications system will function in the event of a collapse of the Public Switched Telephone Network (PSTN), and cross-border voice communications can still be maintained among the Canadian Reliability Coordinators of NPCC and the Reliability Coordinators in the United States.

Critical Infrastructure Objectives

NPCC's critical infrastructure objectives are defined within the scope of the NPCC Task Force on Infrastructure Security & Technology, (TFIST) and include, but are not confined to:

- Providing a forum for NPCC review of proposed and posted documents from the NERC Critical Infrastructure Protection Committee (CIPC)
- Representing and advocating NPCC's position in the activities of NERC groups involved in the development and/or implementation of physical and cyber security

NPCC's 2015 critical infrastructure goals and objectives, as identified by the 2014-2015 Work Plan of the Task Force on Infrastructure Security and Technology include, but are not confined to:

- Oversee the implementation of version 5 of the CIP Standards
- Monitor the Homeland Security Information Network (HSIN), ES-ISAC, Critical Information Protection Information Sharing (CIPIS), NERC Alerts and Canadian Information Sharing and share information with CO-8[53]
- Coordinate Cyber Protection activities, discussions and hold workshops as may be required to maintain Cyber Security of BES Cyber Assets.[54]
- Provide continued support and participation in NERC's Critical Infrastructure Protection Committee (CIPC)[55]
- Review and submit comments on NERC proposed Reliability Standards, modified Reliability Standards, proposed Guidelines and modified Guidelines related to Infrastructure Security and Technology
- Keep current on all governmental agencies regarding applicable security recommendations and requirements, and other applicable security and reliability recommendations and keep the RCC and its committees appropriately informed, e.g. Sector Specific Plan.
- Develop and maintain levels of expertise in those areas of concern to the task force through activities such as periodic workshop presentations, seminars, and meetings, open to the general NPCC membership[56].
- Regarding the Cross Border Emergency Telecommunications recommendation
    - Continue to annually report to RCC on this testing

[53] In support of ERO Goal 5.b. Issue and track security recommendations to protect the bulk power system (related to 5.a.ii.)

[54] In support of ERO Goal 1. b. Facilitate smooth transition of new standards (e.g., CIP Version 5); and ERO Goal 3.a. Initiate compliance phase-in learning periods for new standards

[55] In support of ERO Goal 5.a. Manage risk control initiatives to be completed by ERO and coordinate other initiatives with industry (e.g., relay misoperations, situational awareness, human error, cyber attack)

[56] In support of ERO Goal 5.b. Expand the use and value of security threat and vulnerability information sharing, analytics, and analysis

    - Continue to support CO-8's monthly testing
- Assess the telecommunications industry's desire to convert Frame Relay customers to Multiprotocol Label Switching (MPLS) and potentially provide recommendations to RCC

System Operations Security Objectives

NPCC's system operations security objectives are defined within the scope of the NPCC Task Force on Coordination of Operation (TFCO) and include, but are not confined to:

- Coordinating inter-Regional pre-emergency actions in the event of a threat to the security of the Northeastern North American bulk power supply system[57]
- Assisting in the development of real time operating tools assuring cyber security concerns are addressed[58]

NPCC's 2015 operational situation awareness goals and objectives, as identified by the 2014-2015 Work Plan of the NPCC Task Force on Coordination of Operation (TFCO) include, but are not confined to:

- Continue to monitor the reliable implementation of version 5 of the Cyber Standards.[59]
- Work directly with applicable NPCC Task Forces to provide an in depth assessment of Lessons Learned unique to the NPCC members and NPCC criteria.

2015 Key Assumptions

- The monitoring of Lessons Learned will be a major focus of NERC in 2015.
- Critical infrastructure protection will fully integrate the requirements of version 5 of the Cyber Standards in 2015.

2015 Goals and Key Deliverables

- Continue to monitor the reliable implementation of version 5 of the Cyber Standards.
- Work directly with applicable NPCC Task Forces to provide an in depth assessment of Lessons Learned unique to the NPCC members and NPCC criteria.
- Establish a unique NPCC Event Analysis web site to post NPCC Lessons Learned.
- Contribute to the reduction of Category 3 events and no Category 4 or 5 events in NPCC- by disseminating to the RCC compiled information on NPCC Region specific, as well as industry wide, event related causal analysis and analysis of Lessons Learned.[60]

Based on the portion of professional/technical staff time and other resources devoted to situation awareness and infrastructure security, NPCC estimates that it will expend 10 percent of its resources on this activity.

[57] In support of ERO Goal 5.b.Issue and track security recommendations to protect the bulk power system (related to 5.a.ii.)

[58] In support of ERO Goal 5.a. Manage risk control initiatives to be completed by ERO and coordinate other initiatives with industry (e.g., relay misoperations, situational awareness, human error, cyber attack)

[59] In support of ERO Goal 5.a. Manage risk control initiatives to be completed by ERO and coordinate other initiatives with industry (e.g., relay misoperations, situational awareness, human error, cyber attack)

[60] In support of ERO Goal 4.b. Provide lessons learned and recommendations from events and identified risks

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- U.S. Penalty Sanctions remitted from 7/1/13 through 6/30/14 reduce U.S. LSE designee assessments for 2015.

Personnel Expenses

- NPCC anticipates no need to hire additional personnel in this program area in 2015.
- Salaries expense relects implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Retirement expense decreased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.
- Consultants and contracts expense increase in support of NPCC's efforts to assess and improve system frequency and generator governor response.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Situation Awareness and Infrastructure Security Program

Funding sources and related expenses for the situation awareness and infrastructure security section of the 2015 business plan are shown in the table below.

Statement of Activities and Capital Expenditures
2014 Budget & Projection, and 2015 Budget
Situation Awareness and Infrastructure Security

	2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding					
ERO Funding					
ERO Assessments	$ 1,447,636	$ 1,447,636	$ -	$ 1,471,074	$ 23,438
Penalty Sanctions	16,475	16,475	-	30,258	13,783
Total ERO Funding	**$ 1,464,111**	**$ 1,464,111**	**$ -**	**$ 1,501,332**	**$ 37,221**
Membership Dues	-	-	-	-	-
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Total Funding (A)	**$ 1,464,111**	**$ 1,464,111**	**$ -**	**$ 1,501,332**	**$ 37,221**
Expenses					
Personnel Expenses					
Salaries	$ 522,672	$ 522,672	$ -	$ 541,258	$ 18,586
Payroll Taxes	32,961	32,961	-	32,811	(150)
Benefits	88,851	88,851	-	80,801	(8,049)
Retirement Costs	117,586	117,586	-	107,819	(9,767)
Total Personnel Expenses	**$ 762,070**	**$ 762,070**	**$ -**	**$ 762,689**	**$ 619**
Meeting Expenses					
Meetings	$ 25,000	$ 25,000	$ -	$ 15,000	$ (10,000)
Travel	60,000	60,000	-	60,000	-
Conference Calls	-	-	-	-	-
Total Meeting Expenses	**$ 85,000**	**$ 85,000**	**$ -**	**$ 75,000**	**$ (10,000)**
Operating Expenses					
Consultants & Contracts	$ 75,000	$ 75,000	$ -	$ 100,000	$ 25,000
Office Rent	-	-	-	-	-
Office Costs	-	-	-	-	-
Professional Services	-	-	-	-	-
Computer & Equipment Leases	-	-	-	-	-
Miscellaneous	-	-	-	-	-
Depreciation	-	-	-	-	-
Total Operating Expenses	**$ 75,000**	**$ 75,000**	**$ -**	**$ 100,000**	**$ 25,000**
Total Direct Expenses	**$ 922,070**	**$ 922,070**	**$ -**	**$ 937,689**	**$ 15,619**
Indirect Expenses	**$ 568,962**	**$ 568,962**	**$ -**	**$ 574,629**	**$ 5,667**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)	**$ 1,491,031**	**$ 1,491,031**	**$ -**	**$ 1,512,318**	**$ 21,286**
Change in Assets	**$ (26,920)**	**$ (26,920)**	**$ -**	**$ (10,986)**	**$ 15,935**
Fixed Assets					
Depreciation	$ -	-	$ -	$ -	$ -
Computer & Software CapEx	-	-	-	-	-
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	(26,920)	(26,920)	-	(10,986)	15,935
Inc(Dec) in Fixed Assets (C)	**(26,920)**	**(26,920)**	**-**	**(10,986)**	**15,935**
TOTAL BUDGET (=B+C)	1,464,111	1,464,111	-	1,501,332	37,221
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)	**$ (0)**	**$ (0)**	**$ -**	**$ (0)**	**$ (0)**

Administrative Services

Administrative Services Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	9.00	9.00	0.00
Total Direct Expenses	$5,689,616	$5,746,287	$56,671
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Less: Other Funding Sources	$0	$0	$0
Total Allocation to Regional Entity Division Programs as Indirect Expenses	($5,283,757)	($5,336,385)	($52,629)
Total Allocation to Criteria Services Division Programs as Indirect Expenses	($405,859)	($409,902)	($4,043)
Funding Requirement for Working Capital and Operating Reserves	($300,126)	($355,161)	($55,035)

Program Scope and Functional Description

Administrative services support the previously identified five program areas of: reliability standards; compliance monitoring and enforcement and organization registration and certification; training, education, and operator certification; reliability assessment and performance analysis; and situation awareness and infrastructure security. Administrative services consist of: technical committees and members' forums; general and administrative; legal and regulatory; information technology; human resources; and finance and accounting.

Methodology for Allocation of Administrative Services Expenses to Programs

NPCC total overhead expenses, such as office rent and office costs, will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Funding Sources and Requirements — Explanation of Increase (Decrease)

Personnel Expenses

- NPCC anticipates no need to hire additional personnel in this program area in 2015.
- Salaries expense reflect implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Retirement expense decreased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.

Administrative Services

Funding sources and related expenses for the Administrative Services section of the 2015 business plan are shown in the table below.

Statement of Activities and Capital Expenditures 2014 Budget & Projection, and 2015 Budget ADMINISTRATIVE SERVICES						
		2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding						
ERO Funding						
	ERO Assessments	$ (300,126)	$ (300,126)	$ -	$ (355,161)	$ (55,035)
	Penalty Sanctions	-	-	-	-	-
Total ERO Funding		**$ (300,126)**	**$ (300,126)**	**$ -**	**$ (355,161)**	**$ (55,035)**
	Membership Dues	-	-	-	-	-
	Testing Fees	-	-	-	-	-
	Services & Software	-	-	-	-	-
	Workshops	-	-	-	-	-
	Interest	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
Total Funding (A)		**$ (300,126)**	**$ (300,126)**	**$ -**	**$ (355,161)**	**$ (55,035)**
Expenses						
Personnel Expenses						
	Salaries	$ 1,676,735	$ 1,676,735	$ -	$ 1,769,318	$ 92,583
	Payroll Taxes	96,083	96,083	-	97,804	1,722
	Benefits	442,256	442,256	-	402,307	(39,949)
	Retirement Costs	425,270	425,270	-	435,638	10,368
Total Personnel Expenses		**$ 2,640,344**	**$ 2,640,344**	**$ -**	**$ 2,705,068**	**$ 64,724**
Meeting Expenses						
	Meetings	$ 110,000	$ 110,000	$ -	$ 120,000	$ 10,000
	Travel	155,000	155,000	-	155,000	-
	Conference Calls	77,000	77,000	-	45,000	(32,000)
Total Meeting Expenses		**$ 342,000**	**$ 342,000**	**$ -**	**$ 320,000**	**$ (22,000)**
Operating Expenses						
	Consultants & Contracts	$ 150,000	$ 150,000	$ -	$ 124,000	$ (26,000)
	Office Rent	737,272	737,272	-	751,500	14,228
	Office Costs	523,500	523,500	-	578,700	55,200
	Professional Services	966,500	966,500	-	1,025,000	58,500
	Computer & Equipment Leases	-	-	-	-	-
	Miscellaneous	80,000	80,000	-	40,000	(40,000)
	Depreciation	250,000	250,000	-	202,019	(47,981)
Total Operating Expenses		**$ 2,707,272**	**$ 2,707,272**	**$ -**	**$ 2,721,219**	**$ 13,947**
	Total Direct Expenses	**$ 5,689,616**	**$ 5,689,616**	**$ -**	**$ 5,746,287**	**$ 56,671**
Indirect Expenses		**$ (5,689,616)**	**$ (5,689,616)**	**$ -**	**$ (5,746,287)**	**$ (56,671)**
Other Non-Operating Expenses		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)		**$ -**	**$ -**	**$ -**	**$ (0)**	**$ (0)**
Change in Assets		**$ (300,126)**	**$ (300,126)**	**$ -**	**$ (355,161)**	**$ (55,035)**
Fixed Assets						
	Depreciation	(250,000)	(250,000)	$ -	(202,019)	$ 47,981
	Computer & Software CapEx	-	-	-	100,000	100,000
	Furniture & Fixtures CapEx	-	-	-	-	-
	Equipment CapEx	-	-	-	-	-
	Leasehold Improvements	-	-	-	-	-
	Allocation of Fixed Assets	250,000	250,000	-	102,019	(147,981)
Inc(Dec) in Fixed Assets (C)		**-**	**-**	**-**	**-**	**-**
TOTAL BUDGET (=B+C)		-	-	-	(0)	(0)
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)		**$ (300,126)**	**$ (300,126)**	**$ -**	**$ (355,161)**	**$ (55,035)**

Technical Committees and Member Forums

Technical Committees and Members Forum Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	0.50	0.50	0.00
Total Direct Expenses	$75,711	$73,779	($1,932)
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Working Capital Requirement	$0	$0	$0

Program Scope and Functional Description

The success of the NPCC programs depends on the active and direct volunteerism and participation of its members. The stakeholders are the source of expertise in the industry. To promote the reliable and efficient operation of the interconnected bulk power systems in Northeastern North America, NPCC invites high level policy makers from Federal, Provincial and State regulatory and/or governmental authorities and senior executives within NPCC and NERC to identify and discuss emerging issues related to the reliability of the NPCC Region.

2015 Key Assumptions

- NPCC's standing committee and subgroup structure for effective stakeholder involvement will continue in 2015
- NPCC will continue to utilize methods to encourage active involvement in its Regional programs that require less stakeholder travel and face-to-face meetings, as the economy improves in 2015
- NPCC will continue to invest in technology and innovation to allow efficient collaboration on technical issues related to reliability

2015 Goals and Key Deliverables

The 2015 NPCC General Meeting provides an opportunity for NPCC Members to meet high level policy makers from Federal, Provincial and State regulatory and/or governmental authorities and senior NERC and NPCC executives to discuss topics related to the reliable planning and operation of the power system, including consideration of emerging reliability, critical infrastructure and environmental issues.

2015 Public Information Committee Goals and Objectives

The objective of the NPCC Public Information Committee is to highlight and summarize NPCC activities and accomplishments in the past year, disseminate and coordinate the appropriate release of information to the media, respond to related requests for information, and coordinate with related NPCC Area, NERC media and public information activities. Activities anticipated for include, but are not limited to:

- Conducting the Media Event – release of the Summer 2015 NPCC Reliability Assessment

- Participation in NERC Regional communication initiatives:
    - Regional communications teleconferences as required
    - Coordination of Emergency or Blackout communications plans
    - Coordination with other NERC activities as required (i.e., situation awareness, event analysis, reliability assessments, etc.)

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- Not applicable

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

General and Administrative

General and Administrative Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	2.50	2.50	0.00
Total Direct Expenses	$3,293,356	$3,209,290	($84,066)
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Working Capital Requirement	($300,126)	($355,161)	($55,035)

Program Scope and Functional Description

The NPCC general and administrative function provides executive management of the corporation, management of NPCC office, and other administrative support programs.

NPCC total overhead expenses, such as office rent and office costs, will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Funding Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- Not applicable

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Legal and Regulatory

Legal and Regulatory Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	1.00	1.00	0.00
Total Direct Expenses	$621,004	$628,183	$7,179
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Working Capital Requirement	$0	$0	$0

Program Scope and Functional Description

NPCC's professional legal services provide counsel to the President and CEO, Board of Directors, Vice President and COO, Treasurer and staff on a wide range of legal and regulatory matters including legislation, corporate law, code of conduct, confidentiality, governance, employment law, tax matters, contract law and other areas affecting NPCC. Regulatory counsel provides legal advice to advance significant corporate policy and strategic planning initiatives and also provides legal support to other program areas on matters arising in connection with the performance of NPCC's delegated functions. Regulatory counsel drafts agreements and pleadings and provides interpretations of relevant statutes, regulations, court opinions, and regulatory decisions of FERC, state agencies and provincial authorities. Outside counsel, as necessary, reviews items filed with the governmental agencies for legal sufficiency, maintains relationships with U.S. and Canadian jurisdictions and provides contract review.

Funding Sources (Other than ERO Assessments)

- Not applicable

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Information Technology

Information Technology Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	3.00	3.00	0.00
Total Direct Expenses	$1,037,624	$1,111,674	$74,050
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Working Capital Requirement	$0	$0	$0

Program Scope and Functional Description

NPCC's Information Technology services ensure information assets and the environment in which they operate are secure and in conformance to NPCC IT Policies and Procedures. NPCC maintains an offsite backup server for continuity of essential operations in the event that its primary location is unavailable.

2015 Key Assumptions

- Continue to develop and maintain the compliance portal through collaboration with other Regions and NERC (CUG).
- Achieve greater consistency with the other Regions and NERC by participating in the NERC IT Steering Group (ITSG) and deriving the efficiencies and cost savings which may result from the projects of this group.[61]
    - The ERO EMG identifies and prioritizes ERO-wide applications to be developed under a PMO housed at NERC. The NERC IT budget does not supplant the Regional Entities' need for IT expenditures for specific regional projects, but to the extent that agreed-upon ERO Enterprise applications provide greater efficiencies, there should not be any unnecessary, redundant expenditures at the regional level.
- Support the Event Analysis program through continued participation in the tools used for the tracking and analysis of system events.[62]
- Support the Bulk Electric System Exception Process "BEP" to enable and facilitate tracking and processing of exceptions submitted.[63] Maintenance of the BESNET support services such as updates, patching, coordinating issues with NERC.
- Support Cyber Security Reviews done by compliance to provide advisory role during those reviews.

[61] ERO Goal 7.b. Develop test and deploy ERO enterprise applications, platform and database

[62] ERO Goal 6.b. Evaluate event disturbances using phasor measurements and other methods to assess sufficiency of data and models;
ERO Goal 4.b. Provide lessons learned and recommendations from events and identified risks;
ERO Goal 4.b. Merge event driven databases and cause codes into one (e.g., event analysis, TADS, GADS, relay mis-operations)

[63] ERO Goal 2.a. Develop and implement BES exception process.

2015 Goals and Key Deliverables

Responsibilities encompass a variety of complex technical, administrative, and supervisory work in the development, installation, and maintenance of information technology systems. IT goals include, but are not limited to:

- Create an information security program and environment aimed at reducing breach of security risks
- Determine long-term software and systems needs and hardware acquisitions
- Develop and implement information security standards and procedures
- Ensure all information systems are functional and secure, and that all applications running on those systems meet business requirements for performance, availability, and security
- Plan and implement organization-wide information systems, services, and network facilities, including local area networks, wide-area networks, and peripheral systems
- Provide outreach and education to NPCC members in IT best practices
- Continually improve Disaster Recovery policies and practices to ensure continuity of service

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- Not applicable

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Human Resources

Human Resources Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	1.00	1.00	0.00
Total Direct Expenses	$178,931	$183,817	$4,886
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Working Capital Requirement	$0	$0	$0

Program Scope and Functional Description

NPCC has assembled an exceptional team of highly qualified employees to carry out the activities of NPCC. The human resources function, in adherence with applicable federal and state laws, designs, plans, and implements human resources policies and procedures, including staffing, compensation, benefits, employee relations, and training and development.

An enhanced employee time tracking system was implemented in 2013 based on FERC audit recommendations. Employee time tracking and reporting is also handled by the human resources program area.

Funding Sources (Other than ERO Assessments)

- Not applicable

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Accounting and Finance

Accounting and Finance Program Resources (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	1.00	1.00	0.00
Total Direct Expenses	$482,991	$494,544	$11,554
Other Non-Operating Expenses	$0	$0	$0
Inc(Dec) in Fixed Assets	$0	$0	$0
Working Capital Requirement	$0	$0	$0

Program Scope and Functional Description

The accounting and finance function directs the overall financial plans and accounting practices of the organization; oversees treasury, accounting, budget, tax, and audit activities; and oversees financial and accounting system controls and standards. NPCC uses a CPA firm to prepare its unaudited statements of activities and financial statements for quarterly reviews. Independent audits have identified this system as a best practice.

2015 Goals and Key Deliverables

The objectives are to provide or obtain the financial and accounting services for NPCC and coordinate with NERC requirements:

- Utilize the NERC System of Accounts for consistency
- Utilize an accrual method of accounting for consistency with NERC in methodology
- Cash Management
- Budget Development using the NERC budget template formats
- Forecasts and Projections
- Alignment of NPCC Committees, Task Forces and Working Groups with the programs
- Payroll and expense administration
- Preparation of unaudited Quarterly Financial Statements
- IRS Reporting
- Annual Independent Audit initiated by the Regional Entity

Funding Sources and Requirements — Explanation of Increase (Decrease)

Funding Sources (Other than ERO Assessments)

- Not applicable

Operating Expenses and Indirect Expenses

- NPCC total overhead expenses, such as office rent and office costs will be charged to the Administrative Services Programs and then reallocated proportionately based on FTE to the programs through Indirect Expenses.

Other Non-Operating Expenses

- None

Fixed Asset Additions

- None

Regional Entity Assessment Analysis

In the area of assessments there are distinct funding mechanisms as outlined in the following table. For the Regional Entity division, the North American Electric Reliability Corporation (NERC) will assess load serving entities (LSEs) or their designees (within NPCC the designees are the Balancing Authority Areas (BAAs) for New York, New England, New Brunswick, Nova Scotia, Ontario and Québec) based upon 2013 proportional Net Energy for Load (NEL) and other specific program area funding arrangements and make quarterly remittances to the Regional Entity on or about the 15th day of January, April, July and October. For funding associated with the criteria services division, the Independent System Operators/Balancing Authority Areas (ISO/BAAs) will be assessed by NPCC for their proportional share of the divisional budget based upon 2012 NEL within the Region. Non ISO/BAA Full Members will be assessed no membership fee.

NPCC Cost Allocation Methodology

The accompanying table provides information regarding cost allocation for both the Regional Entity division and the criteria services division of NPCC, including the details associated with the funding of the Compliance Program within the RE division. For purposes of determining assessments to support NPCC's resource requirements, costs are allocated among the BAAs within NPCC as the designees for the load-serving-entities in New York, New England, Ontario, Québec, New Brunswick and Nova Scotia (Column A-1).

In order to reflect and respect the international membership and nature of NPCC, the compliance responsibilities and authorities within the U.S., and the specific compliance responsibilities within each of the Canadian provinces within NPCC, the attendant costs of portions of the compliance program differ among the areas within the Regional Entity. Within the U.S. portion of NPCC all costs attributable to delegated (statutory) functions performed by NPCC, including all compliance functions, are assessed based on a NEL allocation. Within the Canadian portion of NPCC those costs attributable to compliance functions performed by NPCC on behalf of provincial governmental and/or regulatory authorities are allocated consistent with the unique Memoranda of Understanding or Agreements that have been entered into for those provinces. To address these different compliance regimes, NPCC developed a composite cost allocation methodology that allocates compliance costs on a fair and equitable basis within the Regional Entity.

As an initial step of that methodology, the NEL for each of the BAAs and their relative percentage to the NPCC total NEL is calculated for the most recent year for which data is available, the second previous year (Columns B-1 and C-1, respectively). In order to establish the RE division funding requirements for each balancing authority area on a NEL basis for all programs except for compliance (Column F-1), the proposed expenses and fixed assets of all other programs are calculated (Column D-1) and the adjustment for the RE division cash reserve requirement is identified (Column E-1). Any penalty monies received from NPCC registered entities within the U.S. prior to June 30th of the year preceding the business plan and budget year are then allocated among the NPCC program areas based on their FTE ratio and between the U.S. BAAs based on their relative NELs (Columns B-1a., C-1a. and G-1, respectively). Consistent with each of the Canadian provincial MOUs and agreements, all penalty monies resulting from compliance actions within Canada, if any, would remain within the applicable province. The total budgeted fees for NPCC workshop participation are indicated as a credit

(Column H-1), with the resultant addition being the RE division assessment, without the compliance program costs, calculated on a NEL basis (Column I-1).

In accordance with the *NPCC Amended and Restated Bylaws* the CS division proposed expenses and fixed assets of all programs are calculated (Column J-1) and the adjustment for the CS division cash reserve requirement is identified (Column K-1), with the resultant addition being the CS division funding requirement and assessment, calculated on a NEL basis (Column L-1).

For costs associated with the RE division compliance program, NPCC's allocation methodology apportions X% of the costs for the program, attributed to CORC Fundamentals (CF), between the BAAs in the United States and Canada on a NEL basis (Column B-2).

Audits and Investigations (AI) related costs, representing X% of the costs of the compliance program, are allocated between U.S. and Canadian BAAs in NPCC, and among the Canadian provinces, using an audit-based methodology (Columns C-2a., C-2c., and D-2b., respectively). The audit-based methodology incorporates relative costs based on categories of compliance audits which are reflective of their size and complexity, as well as the differing compliance program implementation models that are utilized in NPCC due to the international nature of the Regional Entity. The portion allocated to the U.S. BAAs in NPCC is calculated using the audit-based methodology, and this amount is then re-allocated between the New York and New England BAAs based on their relative NEL (Columns C-2b. and D-2a.).

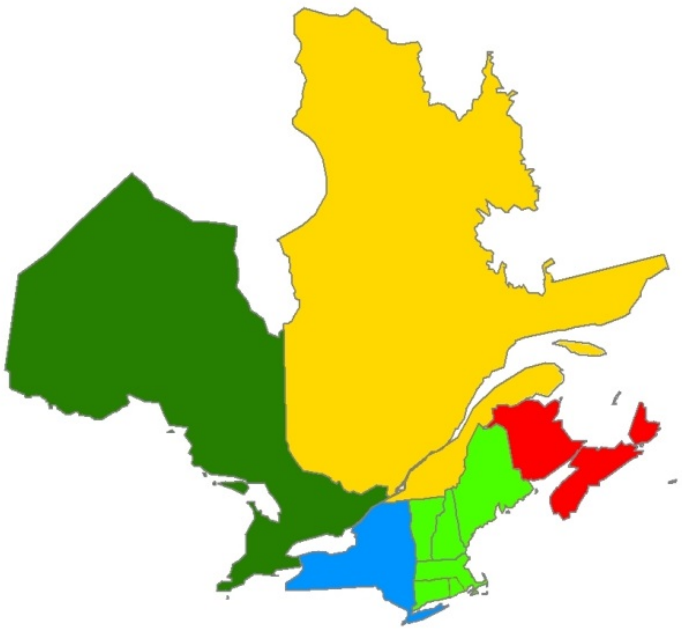
The remaining X% of the costs of the compliance program represent Mitigation and Enforcement (ME) related costs and are allocated between U.S. and Canadian BAAs in NPCC, and among the Canadian provinces, using an enforcement activity based methodology, (Columns E-2a., E-2c., and F-2b., respectively). Based on historical data, NPCC reviewed each BAAs percentage of violations, mitigation plans and settlement agreements to determine each BAAs total average percentage of enforcement activities. The portion allocated to the U.S. BAAs in NPCC is calculated using the enforcement activity based methodology, and this amount is then re-allocated between the New York and New England BAAs based on their relative NEL (Columns E-2b. and F-2a.).

Any penalty monies received from NPCC registered entities within the U.S. by June 30th of the year preceding the business plan and budget year are then allocated among the NPCC program areas based on their FTE ratio and between the U.S. BAAs based on their relative NELs, and then added to the total compliance program expenses and fixed assets to yield a total compliance program assessment (Columns C-1a., H-2, G-2 and I-2, respectively).

Finally, the total RE division funding requirements and assessments by BAA are tabulated and the total funding requirements and assessments for NPCC, both the RE and CS divisions, are combined (Column M).

Table to be Inserted

Section B – Supplemental Financial Information
2015 Business Plan and Budget



Section B — Supplemental Financial Information

Reserve Balance

Table B-1 – Reserve Balance

Working Capital and Operating Reserve Analysis 2014-2015
REGIONAL ENTITY DIVISION

	Total Reserve	Operating Reserve	Working Capital
Beginning Total Reserve, December 31, 2013	**5,245,194**	4,013,698	1,231,496
Plus: 2014 ERO Funding (from LSEs or designees)	13,611,880	13,611,880	0
Plus: 2014 Other funding sources	217,000	217,000	0
Less: 2014 Projected expenses & capital expenditures	(14,129,006)	(14,129,006)	0
Projected Total Reserve, December 31, 2014	**4,945,068**	**3,713,572**	**1,231,496**
Desired Total Reserve, December 31, 2015 [1]	**4,589,907**	3,358,411 [2]	1,231,496 [3]
31.06% of Total Regional Entity Budget of $14,778,539			
Less: Projected Working Capital and Operating Reserve, December 31, 2014	(4,945,068)	(3,713,572)	(1,231,496)
Increase(decrease) in assessments to achieve desired Total Reserve	**(355,161)**	(355,161)	0

2015 Expenses and Capital Expenditures	14,778,539
Less: Penalty Sanctions [4]	(281,000)
Less: Other Funding Sources	(64,000)
Adjustment to achieve desired Total Reserve balance	(355,161)
2015 Assessment	**14,078,378**

[1] Total Reserve within a range of 16.67% - 33.33% of Budget.
[2] Operating Reserve within a range from 8.33% to 25.00% of Budget. $3,358,411 represents 22.72% of the 2015 budget of $14,778,539
[3] Working Capital equal to 8.33% of Budget. $1,231,496 represents 8.33% of the 2015 budget of $14,778,539
[4] Represents collections prior to June 30, 2014.

Explanation of Changes in Reserve Policy from Prior Year

On October 29, 2013 NPCC's Board of Directors approved management's proposed Working Capital and Operating Reserve Policy. The policy calls for a range between 8.33% (30 days) and 25.00% (90 days) rather than the specific required level of Operating Reserves of 8.33%. This range will allow for more stability in Assessments. The Working Capital required balance remains unchanged at 8.33% (30 days).

Breakdown by Statement of Activity Sections

The following detailed schedules are in support of the Regional Entity division Statement of Activities on page 13 of the 2015 Business Plan and Budget. All significant variances have been disclosed by program area in the preceding pages.

Penalty Sanctions

U.S. penalty monies received prior to June 30, 2014 are to be used to offset assessments in the 2015 Budget, as documented in the NERC Policy – Accounting, Financial Statement, and Budgetary Treatment of Penalties Imposed and Received for Violations of Reliability Standard. Penalty monies received from July 1, 2014 through June 30, 2015 will be used to offset U.S. load serving entity designee assessments in the 2016 Budget.

All penalties received prior to June 30, 2014 are detailed below, including date received and the penalty amount.

Allocation Method: U.S. penalty sanctions received have been allocated to the following Regional Entity division programs to reduce assessments: Reliability Standards; Compliance Monitoring & Enforcement and Organization Registration & Certification; Reliability Assessments and Performance Analysis; Training, Education and Operator Certification; and Situation Awareness and Infrastructure Security. U.S. penalty sanctions are allocated based upon the number of FTEs in the Program divided by the aggregate total FTEs in the Programs receiving the allocation.

Table B-2 – Penalty Sanctions

Penalty Sanctions Received Prior to June 30, 2014	Date Received	Amount Received
Penalty Payment 1	7/5/2013	$ 50,000.00
Penalty Payment 2	7/5/2013	$ 10,000.00
Penalty Payment 3	7/5/2013	$ 30,000.00
Penalty Payment 4	7/5/2013	$ 25,000.00
Penalty Payment 5	9/4/2013	$ 7,000.00
Penalty Payment 6	10/16/2013	$ 25,000.00
Penalty Payment 7	11/1/2013	$ 5,000.00
Penalty Payment 8	1/8/2014	$ 25,000.00
Penalty Payment 9	3/6/2014	$ 14,000.00
Penalty Payment 10	4/30/2014	$ 90,000.00
Total Penalties Received		**$ 281,000.00**

Table B-3 – Supplemental Funding

Outside Funding Breakdown By Program (excluding ERO Assessments & Penalty Sanctions)	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget
Reliability Standards				
Total	$ -	$ -	$ -	$ -
Compliance Monitoring, Enforcement & Org. Registration				
	$ -	$ -	$ -	$ -
	-	-	-	-
Total	$ -	$ -	$ -	$ -
Reliability Assessment and Performance Analysis				
	$ -	$ -	$ -	$ -
	-	-	-	-
Total	$ -	$ -	$ -	$ -
Training and Education				
Workshops	$ 64,000	$ 64,000	$ 64,000	$ -
Total	$ 64,000	$ 64,000	$ 64,000	$ -
Situation Awareness and Infrastructure Security				
	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ -	$ -
Technical Committees and Member Forums				
	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ -	$ -
Administrative Services Programs				
	$ -	$ -	$ -	$ -
Total	$ -	$ -	$ -	$ -
Total Outside Funding	$ 64,000	$ 64,000	$ 64,000	$ -

Explanation of Significant Variances –2015 Budget versus 2014 Budget

- NPCC assumed no interest income because of continuing low market interest rates.

Table B-4 – Personnel Expenses

Personnel Expenses	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Salaries					
Salary	$ 5,886,227	$ 5,886,227	$ 6,175,425	$ 289,198	4.9%
Employment Agency Fees	$ 15,000	$ 15,000	$ 10,000	$ (5,000)	-33.3%
Temporary Office Services	$ 10,000	$ 10,000	$ 10,000	$ -	0.0%
Total Salaries	$ 5,911,227	$ 5,911,227	$ 6,195,425	$ 284,198	4.8%
Total Payroll Taxes	$ 384,311	$ 384,311	$ 387,209	$ 2,898	0.8%
Benefits					
Education Reimbursement	$ -	$ -	$ 10,000	$ 10,000	-
Training and Seminars	$ 36,123	$ 36,123	$ 36,123	$ -	0.0%
Medical Insurance	$ 915,306	$ 915,306	$ 720,337	$ (194,969)	-21.3%
Life-LTD-STD Insurance	$ 63,552	$ 63,552	$ 64,366	$ 815	1.3%
Worker's Compensation	$ 14,700	$ 14,700	$ 14,700	$ -	0.0%
Vacation	$ 400,580	$ 400,580	$ 410,868	$ 10,288	2.6%
Relocation	$ -	$ -	$ -	$ -	-
Total Benefits	$ 1,430,261	$ 1,430,261	$ 1,256,395	$ (173,866)	-12.2%
Retirement					
Pension Contribution	$ 590,892	$ 590,892	$ 353,723	$ (237,169)	-40.1%
Employee Savings Plan	$ 478,469	$ 478,469	$ 644,290	$ 165,821	34.7%
Savings Admin	$ 32,000	$ 32,000	$ 32,000	$ -	0.0%
Deferred Compensation	$ 23,000	$ 23,000	$ 60,000	$ 37,000	160.9%
Total Retirement	$ 1,124,361	$ 1,124,361	$ 1,090,013	$ (34,348)	-3.1%
Total Personnel Costs	**$ 8,850,160**	**$ 8,850,160**	**$ 8,929,041**	**$ 78,881**	**0.9%**
FTEs	36.86	36.86	36.86	-	0.0%
Cost per FTE					
Salaries	$ 160,370	$ 160,370	$ 168,080	$ 7,710	4.8%
Payroll Taxes	$ 10,426	$ 10,426	$ 10,505	$ 79	0.8%
Benefits	$ 38,803	$ 38,803	$ 34,086	$ (4,717)	-12.2%
Retirement	$ 30,504	$ 30,504	$ 29,572	$ (932)	-3.1%
Total Cost per FTE	**$ 240,102**	**$ 240,102**	**$ 242,242**	**$ 2,140**	**0.9%**

Explanation of Significant Variances –2015 Budget versus 2014 Budget

- The increase in Salaries reflects an overall general wage increase of 3%, at risk (variable incentives) compensation at less than 100% of program levels, and implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.
- Benefits expense decreased due to more staff opting out of company sponsored health insurance for superior coverage through prior employer or spouse.
- Pension contribution decreased while employee savings plan increased due to transition of employees formerly accruing benefits under the defined benefit plan to receiving defined contribution benefits in 2015.
- The decrease in Employment Agency Fee is due to no planned staff additions in 2015. Agencies would be used only to fill positions vacated during the year.
- A 2% vacancy factor is assumed based on historical vacancy trends.

Table B-5 – Consultants and Contracts

Consultants	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Consultants					
Reliability Standards	$ -	$ -	$ -	$ -	-
Compliance Enforcement and Organization Registration and Certification	$ 10,000	$ 10,000	$ 15,000	$ 5,000	50.0%
Reliability Assessment and Performance Analysis	$ -	$ -	$ -	$ -	-
Training and Education	$ -	$ -	$ -	$ -	-
Situation Awareness and Infrastructure Security	$ -	$ -	$ -	$ -	-
Member Forums	$ -	$ -	$ -	$ -	-
General and Administrative	$ 50,000	$ 50,000	$ 35,000	$ (15,000)	-30.0%
Legal and Regulatory	$ -	$ -	$ -	$ -	-
Information Technology	$ -	$ -	$ -	$ -	-
Human Resources	$ -	$ -	$ -	$ -	-
Accounting and Finance	$ -	$ -	$ -	$ -	-
Consultants Total	**$ 60,000**	**$ 60,000**	**$ 50,000**	**$ (10,000)**	**-16.7%**

Contracts	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Reliability Standards	$ 30,000	$ 30,000	$ 25,000	$ (5,000)	-16.7%
Compliance Enforcement and Organization Registration and Certification	$ 1,384,433	$ 1,384,433	$ 1,713,000	$ 328,567	23.7%
Reliability Assessment and Performance Analysis	$ 275,000	$ 275,000	$ 365,000	$ 90,000	32.7%
Training and Education	$ -	$ -	$ -	$ -	-
Situation Awareness and Infrastructure Security	$ 75,000	$ 75,000	$ 100,000	$ 25,000	33.3%
Member Forums	$ -	$ -	$ -	$ -	-
General and Administrative	$ 90,000	$ 90,000	$ 82,000	$ (8,000)	-8.9%
Legal and Regulatory	$ -	$ -	$ -	$ -	-
Information Technology	$ -	$ -	$ -	$ -	-
Human Resources	$ -	$ -	$ -	$ -	-
Accounting and Finance	$ 10,000	$ 10,000	$ 7,000	$ (3,000)	-30.0%
Contracts Total	**$ 1,864,433**	**$ 1,864,433**	**$ 2,292,000**	**$ 427,567**	**22.9%**
Total Consultants and Contracts	**$ 1,924,433**	**$ 1,924,433**	**$ 2,342,000**	**$ 417,567**	**21.7%**

Explanation of Significant Variances –2015 Budget versus 2014 Budget

- Compliance Enforcement and Organization Registration and Certification consultant and contractor costs increased due to increased workload related to the initial implementation of the RAI, incorporating Risk Assessment and Internal Control assessment. Without this one time ramp up in RAI endeavors for 2015, contractor costs would have remained relatively flat. These joint ERO Enterprise initiatives are intended to benefit the registered entities, Regional Entities and NERC. With a risk and performance based assessment of each registered entity, audits will transition to a periodicity more reflective of the risk profile of the entity such that some audits will be more in-depth while others may have a reduced scope which will require less independent contractor resources.

- Reliability Assessment and Performance Analysis contracts expense increase is related to implementation of the revised BES definition.

Table B-6 – Office Rent

Office Rent	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Office Rent	$ 654,772	$ 654,772	$ 645,000	$ (9,772)	-1.5%
Utilities	$ 35,000	$ 35,000	$ 40,000	$ 5,000	14.3%
Maintenance	$ 15,000	$ 15,000	$ 22,000	$ 7,000	46.7%
Security	$ 2,500	$ 2,500	$ 2,500	$ -	0.0%
Real Estate Taxes	$ 30,000	$ 30,000	$ 42,000	$ 12,000	40.0%
Total Office Rent	**$ 737,273**	**$ 737,273**	**$ 751,501**	**$ 14,228**	**1.9%**

Table B-7 – Office Costs

Office Costs	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Telephone	$ 110,000	$ 110,000	$ 110,000	$ -	0.0%
Internet Expense	$ 80,000	$ 80,000	$ 80,000	$ -	0.0%
Office Supplies	$ 35,000	$ 35,000	$ 36,000	$ 1,000	2.9%
Computer Supplies and Maintenance	$ 213,000	$ 213,000	$ 260,000	$ 47,000	22.1%
Subscriptions & Publications	$ 13,000	$ 13,000	$ 13,500	$ 500	3.8%
Dues	$ 4,000	$ 4,000	$ 4,000	$ -	0.0%
Postage	$ 1,500	$ 1,500	$ 1,200	$ (300)	-20.0%
Express Shipping	$ 10,000	$ 10,000	$ 10,000	$ -	0.0%
Copying	$ 25,000	$ 25,000	$ 25,000	$ -	0.0%
Reports	$ -	$ -	$ 5,000	$ 5,000	-
Stationary and Office Forms	$ 5,000	$ 5,000	$ 3,000	$ (2,000)	-40.0%
Equipment Repair/Service Contracts	$ 10,000	$ 10,000	$ 8,000	$ (2,000)	-20.0%
Bank Charges	$ 30,000	$ 30,000	$ 23,000	$ (7,000)	-23.3%
Sales and Use Tax	$ -	$ -	$ -	$ -	-
Merchant Credit Card Fees	$ -	$ -	$ -	$ -	-
Presentation and Publicity	$ -	$ -	$ -	$ -	-
Total Office Costs	**$ 536,500**	**$ 536,499**	**$ 578,700**	**$ 42,200**	**7.9%**

Explanation of Significant Variances –2015 Budget versus 2014 Budget

- Computer Supplies and Maintenance expense is based on contracts currently in place and historical actual expense.

Table B-8 - Professional Services

Professional Services	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
BOT Fee	$ 280,000	$ 280,000	$ 325,000	$ 45,000	16.1%
BOT Search Fee	$ -	$ -	$ -	$ -	-
Legal - Reorganization	$ -	$ -	$ -	$ -	-
Accounting & Auditing Fees	$ 300,000	$ 300,000	$ 310,000	$ 10,000	3.3%
Legal Fees - Other	$ 350,000	$ 350,000	$ 350,000	$ -	0.0%
Insurance - Commercial	$ 36,500	$ 36,500	$ 40,000	$ 3,500	9.6%
Total Services	**$ 966,500**	**$ 966,501**	**$ 1,025,000**	**$ 58,500**	**6.1%**

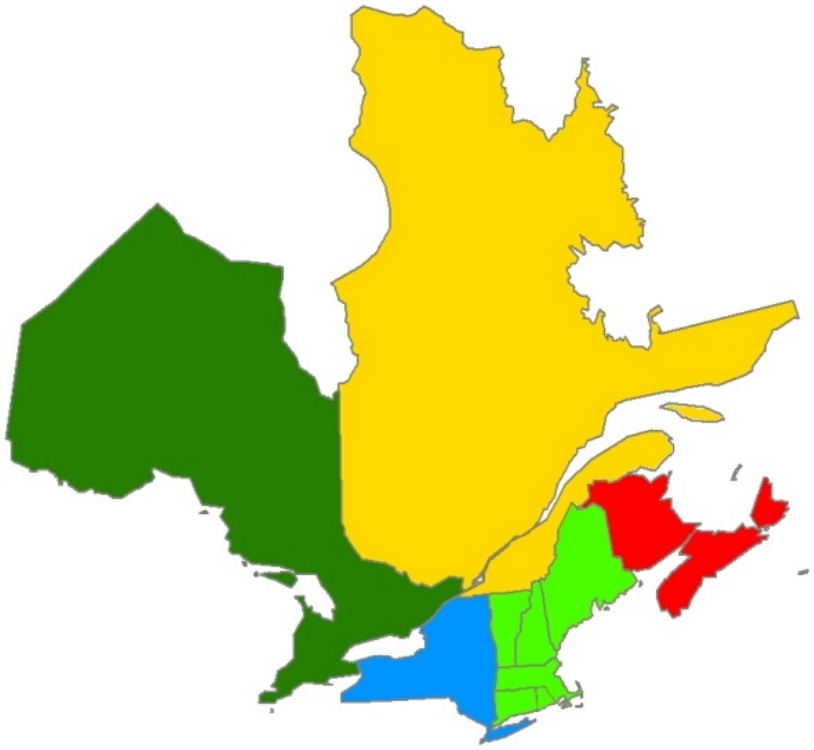
Table B-9 – Other Non-Operating Expenses

Other Non-Operating Expenses	Budget 2014	Projection 2014	Budget 2015	Variance 2015 Budget v 2014 Budget	Variance %
Interest Expense	$ -	$ -	$ -	$ -	-
Office Relocation	$ -	$ -	$ -	$ -	-
Total Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**-**

Table B-10 – 2016 and 2017 Projections

Table to be Inserted

Section C – Criteria Services Division Activities
2015 Business Plan and Budget



Section C —2014 Criteria Services Division Business Plan and Budget

Criteria Services Division (in whole dollars)	2014 Budget	2015 Budget	Increase (Decrease)
Total FTEs	2.14	2.14	0.00
Total Direct Expenses	$683,240	$729,550	$46,310
Total Indirect Expenses	$405,859	$409,902	$4,043
Other Non-Operating Expenses	$0	$0	$0
Working Capital and Operating Reserves Requirement	($75,391)	($94,220)	($18,829)
Inc(Dec) in Fixed Assets	($24,000)	($10,011)	$13,989
Funding Requirement	$989,708	$1,035,221	$45,513

NPCC Regionally-Specific Criteria Services Background

NPCC Criteria Services division activities are based on the development, maintenance and promulgation of Regionally-specific more stringent criteria as well as criteria establishing resource adequacy requirements within the Region. These criteria contain requirements which are more stringent and more specific than the existing NERC Reliability Standards requirements. These criteria require continual evaluation to ensure they are "not inconsistent with" any NERC reliability standards.

Membership and Governance

Full members are subject to compliance with Regionally-specific criteria, in addition to continent-wide Reliability Standards, and receive criteria-related services from the Criteria Services division.

Full Members, aside from those who perform the Balancing Authority function, are not assessed an annual membership fee. Those that perform Balancing Authority functions are assessed and remit a proportional net energy for load share of expenses for criteria services. NPCC would also directly assign criteria service division costs to a Balancing Authority Area or entity, where significant costs are incurred for that Balancing Authority Area. The funding for NPCC's Criteria Services division is approved by the NPCC Board of Directors.

Criteria Services Division Functional Scope

Through its Criteria Services division, NPCC promotes the reliable and efficient operation of the international, interconnected bulk power systems in Northeastern North America through the establishment of Regionally-specific criteria, and monitoring and enforcement of compliance with such criteria.

NPCC provides Full Members with Regional reliability assurance services, and acts as the vehicle through which States and Provinces can fulfill their political mandates, with respect to resource adequacy, as well as overseeing the Northeastern North American electric infrastructure.

Major 2015 Assumptions and Cost Impacts

The Criteria Services division services are expected to remain stable throughout 2015 when compared to the Regional Entity division.

- The Criteria Compliance Enforcement Program (CCEP) review and evaluation process has matured and been enhanced after its inception in 2012. Criteria Compliance submittals to the CC are done as necessary.
- Past non-compliances, if any, followed the due process stated in the CCEP-1 process document and proper resolution/enforcement action taken.

2015 Primary Goals and Objectives

- Review, maintain, and revise the NPCC Regional Reliability Directories to facilitate compliance assessments and ensure the Criteria portions of the Directories are "not inconsistent" with, nor duplicative with, the approved and effective NERC Standards.
- The criteria services division and CCEP Working Group (reporting to the Compliance Committee) will work with the various Task Forces to develop Criteria Compliance Reporting Forms for additional NPCC Directories to ensure that the more stringent or Regionally-specific criteria is being met.
- The criteria services division and CCEP working group will work with TFCO, TFCP, TFSS, and TFSP to review criteria and measures within each specific NPCC Directory to identify and develop them into specific reporting forms for approval.
- Review impact of Bulk Electric System definition on Directory and Criteria content and compliance reporting.
- Review impact of Sector or NPCC organizational changes on the Directory and Criteria review, enforcement and arbitration processes
- Assist Legal with preparation of revised Directories for Regulatory filings with the individual Provinces in accordance with their respective Memorandum of Understandings (MOUs) as well as the State of New York Public Service Commission
- Facilitate any requested interpretations for NPCC Criteria with the necessary subject matter experts and identify potential opportunities for clarifications of the Criteria.

NPCC Reliability Directory Maintenance and Development

The NPCC Regional Reliability Directories were developed to demonstrate that the NPCC more stringent criteria are not inconsistent with the NERC Reliability Standards as mandated by the NERC Rules of Procedure. The Directory project was also undertaken to remove any redundancies with the NERC Reliability Standards and to clearly delineate the more stringent NPCC criteria requirements. In 2013 the directories were further reviewed and revision of the directories is underway to transition the criteria language into a "requirement type" format. This further revision facilitates the NPCC Region's CCEP and ensures the continued delineation of the more stringent and more specific Regional criteria from the latest approved and effective set of NERC ERO standards.

In 2015, work will proceed with maintenance and revision of the Directories to address any future redundancies with NERC or NPCC Reliability Standards as well as the continued need for additional more stringent or specific NPCC Regional criteria requirements as new NERC Reliability Standards are developed and existing standards are revised. NPCC will continue to rely on contractors for subject matter expertise on an as-needed basis throughout 2015. The amount of Regional documents being converted into Directories and the maintenance of the Directories require subject matter expert input. In addition, changes will be necessary to bring the Phase II Directory project to completion. This project will require significant resources to translate the existing criteria language into "requirements" that are clear, concise and measurable. Also a standards template will be applied to the existing Directories to make them more consistent with the look of the standards. As NERC standards improve, the need for NPCC Directories and amount of criteria contained therein will gradually decrease over time however in the interim, significant review is necessary to ensure the criteria remain "not inconsistent with" the NERC standards as outlined in the NERC Rules of Procedure.

The following Directories will either be under revision or reviewed for further development based on a schedule set forth in the NPCC Reliability Assessment Program:

Operations and Planning Directories

Directory #1, *Basic Criteria for Design and Operation of Interconnected Power Systems*
This directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with all the existing NERC TPL, BAL, IRO, INT, MOD, TOP, PRC and VAR standards. The NPCC Task Force on Coordination of Planning will lead a multi-disciplinary working group, consisting of operations and planning subject matter experts to review and revise this directory to reflect the FERC ruling on TPL and other TOP changes.

Directory #2, *Emergency Operations*
This directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with all the existing NERC EOP and TOP standards. The NPCC Task Force on Coordination of Operation will lead this review and revision.

Directory # 3, *Maintenance Requirements for BPS Protection*
This Directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with certain applicable NERC PRC standards. The NPCC Task Force on System Protection will lead this review and revision.

Directory # 4, *BPS Protection*
This Directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with certain applicable NERC PRC standards. The NPCC Task Force on System Protection will lead this review and revision.

Directory # 5, *Operating Reserve Requirements*
This directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with all the existing applicable NERC BAL, INT, and IRO standards. The NPCC Task Force on Coordination of Operation will lead this review and revision.

Directory # 7, *Special Protection Systems*
This Directory documents NPCC's Regionally-specific, more stringent criteria for application and approval of SPS. The NPCC Task Force on System Protection will lead this review and revision.

Directory # 8 System Restoration
This Directory documents NPCC's Regionally-specific, more stringent criteria with which each applicable entity must plan for and perform power system restoration following a major or a total blackout, and demonstrates coordination and consistency with applicable NERC EOP standards. The NPCC Task Force on Coordination of Operation will lead this review and revision.

Directory # 9, *Verification of Generator Gross and Net Reactive Power Capability*
This Directory documents NPCC's Regionally-specific, more stringent criteria for verifying the Gross Reactive Power
Capability and Net Reactive Power Capability of generators or generating facilities. The NPCC Task Force on Coordination of Operation will lead this review and revision.

Directory # 11, *Disturbance Monitoring*, This directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with certain existing NERC PRC standards. The NPCC Task Force on System Protection will lead this review and revision until such time as the NPCC PRC-002-01 Disturbance Monitoring Regional Standard is adopted by FERC and the applicable governmental authorities.

Directory # 12, *UFLS Program*, This directory documents NPCC's Regionally-specific, more stringent criteria, and demonstrates coordination and consistency with certain existing NERC and NPCC developing PRC standard(s). The NPCC Task Force on System Studies will lead this review and revision until such time as the NPCC PRC-006-01 UFLS Regional Standard is approved by the NPCC membership, NERC BOT, the FERC and all the applicable governmental authorities in the Provinces of Canada within NPCC's footprint.

NPCC Criteria Compliance Background

The NPCC criteria services division promotes the reliable operation of the bulk power system through implementation of a comprehensive compliance program. The compliance program that includes monitoring, assessing and enforcing compliance with more stringent, Regionally specific NPCC Criteria requirements, is known as the NPCC Criteria Compliance and Enforcement Program (CCEP) described in process document CCEP-1. This program was developed by the criteria services division and the CCEP Working Group under the purview of the NPCC Compliance Committee. The products of this program support the various Task Forces in their assessments of the NPCC Directories in meeting their goals for the Reliability Coordinating Committee as stated in Section A of this Business Plan.

The more stringent, Regionally-specific NPCC Criteria requirements reflect the unique operational and planning aspects of the bulk power system within the NPCC Region and are included in the NPCC "A" documents and their successors, the NPCC Directories.

NPCC issues non-monetary sanctions to enforce compliance with NPCC Criteria.

- The CCEP program is described in document CCEP-1, *NPCC Criteria Compliance and Enforcement Program (CCEP) Process Document*
- The implementation plan is described in document CCEP-2, *Implementation Plan for 2011 NPCC Criteria Compliance and Enforcement Program*
- On April 5, 2011, the above became effective upon Full Member approval of CCEP-1, and CCEP-2 and retired the following
    - NPCC Criteria A-8, Reliability Compliance and Enforcement Program (RCEP)
    - NPCC Guide B-22, Guidelines for Implementation of the NPCC Inc. Compliance Program
    - NPCC Procedure C-32, Review Process for NPCC Reliability Compliance Enforcement Program
    - Each of the above have been annotated as "retired effective 4/5/11 upon Full Member approval of CCEP-1… and CCEP-2…" on the NPCC public website

The CCEP-1 document

- recognizes the applicability of NPCC's Regionally-specific, more stringent reliability criteria to the Full Members of NPCC, consistent with the *Amended and Restated ByLaws*, and respects the provisions of the several Canadian Memoranda of Understanding in the execution of the processes described
- provides a comprehensive CCEP Process Diagram showing the process of evaluating and approving Criteria Certification submittals, and additional processes and responsibilities in the event that non-compliances, disputes and sanctions arise
- describes the roles and responsibilities of Reporting Members, CC, RCC and Enforcement Panel in the compliance review and enforcement process
- describes Levels of Non-Compliance, associated non-monetary Sanctions, Lateness Policy and the Arbitration/Dispute Resolution process
- addresses Mitigation Plans for any violations under the enforcement process; and
- lists the mandatory Certification Forms to be submitted for review by the Task Forces to ensure compliance with NPCC Directories are being met

The CCEP currently requires annual submittal of Certification Forms by the Reliability Coordinators and Balancing Authorities to confirm compliance with various NPCC Directories. Currently the required Certification forms are for Directory #1- *Area Transmission Review*, Directory #8 - *Key Facility List*, Directory #9 – *Generator Real Power Verification*, Directory #10 - *Verification of Generator Gross and Net Reactive Power Capability*, and Directory #12 - *UFLS Program Requirements*. In 2014 NPCC anticipates expansion of the CCEP to include compliance assessment activities to all active Directories.

The CCEP identifies those specific NPCC Directories that are subject to monitoring, assessment and enforcement. These Directories also are subject to NPCC Criteria Compliance Audits.

The NPCC Compliance Committee (CC) has final approval of compliance assessments related to CCEP. The CCEP describes the roles and responsibilities of committees and panels used to resolve contested compliance and/or sanction or penalty determinations related to NPCC Directories.

Explanation of Significant Variances – 2015 Budget versus 2014 Budget

Personnel Expenses

- Salaries expense reflects implementation of recommendations of NPCC's Management Development and Compensation Committee, which were based on an independent compensation study.

2014 Budget and Projection and 2015 Budget Comparisons

Statement of Activities 2014 Budget & Projection, and 2015 Budget CRITERIA SERVICES DIVISION						
		2014 Budget	2014 Projection	Variance 2014 Projection v 2014 Budget Over(Under)	2015 Budget	Variance 2015 Budget v 2014 Budget Over(Under)
Funding						
ERO Funding						
	ERO Assessments	$ -	$ -	$ -	$ -	$ -
	Penalty Sanctions	-	-	-	-	-
Total ERO Funding		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
	Membership Dues	989,708	989,708	-	760,033	(229,675)
	Testing Fees	-	-	-	-	-
	Services & Software	-	-	-	-	-
	Workshops	-	-	-	-	-
	Interest	-	-	-	-	-
	Miscellaneous	-	-	-	-	-
Total Funding (A)		**$ 989,708**	**$ 989,708**	**$ -**	**$ 760,033**	**$ (229,675)**
Expenses						
Personnel Expenses						
	Salaries	$ 312,166	$ 312,166	$ -	$ 369,319	$ 57,153
	Payroll Taxes	21,536	21,536	-	22,681	1,145
	Benefits	64,153	64,153	-	76,900	12,747
	Retirement Costs	129,818	129,818	-	145,639	15,821
Total Personnel Expenses		**$ 527,674**	**$ 527,674**	**$ -**	**$ 614,539**	**$ 86,866**
Meeting Expenses						
	Meetings	$ 10,000	$ 10,000	$ -	$ 10,000	$ -
	Travel	63,000	63,000	-	63,000	-
	Conference Calls	-	-	-	-	-
Total Meeting Expenses		**$ 73,000**	**$ 73,000**	**$ -**	**$ 73,000**	**$ -**
Operating Expenses						
	Consultants & Contracts	$ 55,000	$ 55,000	$ -	$ 30,000	$ (25,000)
	Office Rent	-	-	-	-	-
	Office Costs	-	-	-	-	-
	Professional Services	-	-	-	-	-
	Computer & Equipment Leases	-	-	-	-	-
	Miscellaneous	3,567	3,567	-	2,000	(1,567)
	Depreciation	24,000	24,000	-	10,011	(13,989)
Total Operating Expenses		**$ 82,567**	**$ 82,567**	**$ -**	**$ 42,011**	**$ (40,556)**
	Total Direct Expenses	**$ 683,240**	**$ 683,240**	**$ -**	**$ 729,550**	**$ 46,310**
Indirect Expenses		**$ 405,859**	**$ -**	**$ -**	**$ 409,902**	**$ 4,043**
Other Non-Operating Expenses		**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (B)		**$ 1,089,100**	**$ 1,089,100**	**$ -**	**$ 1,139,452**	**$ 50,353**
Change in Assets		**$ (99,391)**	**$ (99,391)**	**$ -**	**$ (379,419)**	**$ (280,027)**
Fixed Assets						
	Depreciation	$ (24,000)	(24,000)	$ -	$ (10,011)	$ 13,989
	Computer & Software CapEx	-	-	-	-	-
	Furniture & Fixtures CapEx	-	-	-	-	-
	Equipment CapEx	-	-	-	-	-
	Leasehold Improvements	-	-	-	-	-
	Allocation of Fixed Assets	-	-	-	-	-
Inc(Dec) in Fixed Assets (C)		**(24,000)**	**(24,000)**	**-**	**(10,011)**	**13,989**
TOTAL BUDGET (=B+C)		1,065,100	1,065,100	-	1,129,441	64,342
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)		**$ (75,391)**	**$ (75,391)**	**$ -**	**$ (369,408)**	**$ (294,016)**

Personnel Analysis

Total FTE's by Program Area	Budget 2014	Projection 2014	Direct FTEs 2015 Budget	Shared FTEs[1] 2015 Budget	Total FTEs 2015 Budget	Change from 2014 Budget
CRITERIA SERVICES DIVISION						
Operational Programs						
Reliability Standards	1.07	1.07	1.00	0.07	1.07	0.00
Compliance Enforcement and Organization Registration and Certification	0.00	0.00	0.00	0.00	0.00	0.00
Training and Education	0.00	0.00	0.00	0.00	0.00	0.00
Reliability Assessment and Performance Analysis	1.07	1.07	1.00	0.07	1.07	0.00
Situation Awareness and Infrastructure Security	0.00	0.00	0.00	0.00	0.00	0.00
Total FTEs Operational Programs	**2.14**	**2.14**	**2.00**	**0.14**	**2.14**	**0.00**
Administrative Programs						
Member Forums	0.00	0.00	0.00	0.00	0.00	0.00
General and Administrative	0.00	0.00	0.00	0.00	0.00	0.00
Information Technology	0.00	0.00	0.00	0.00	0.00	0.00
Legal and Regulatory	0.00	0.00	0.00	0.00	0.00	0.00
Human Resources	0.00	0.00	0.00	0.00	0.00	0.00
Accounting and Finance	0.00	0.00	0.00	0.00	0.00	0.00
Total FTEs Administrative Programs	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Total FTEs	**2.14**	**2.14**	**2.00**	**0.14**	**2.14**	**0.00**

[1]A shared FTE is defined as an employee who performs both Regional Entity and Criteria Services division functions.

Reserve Analysis 2014-2015

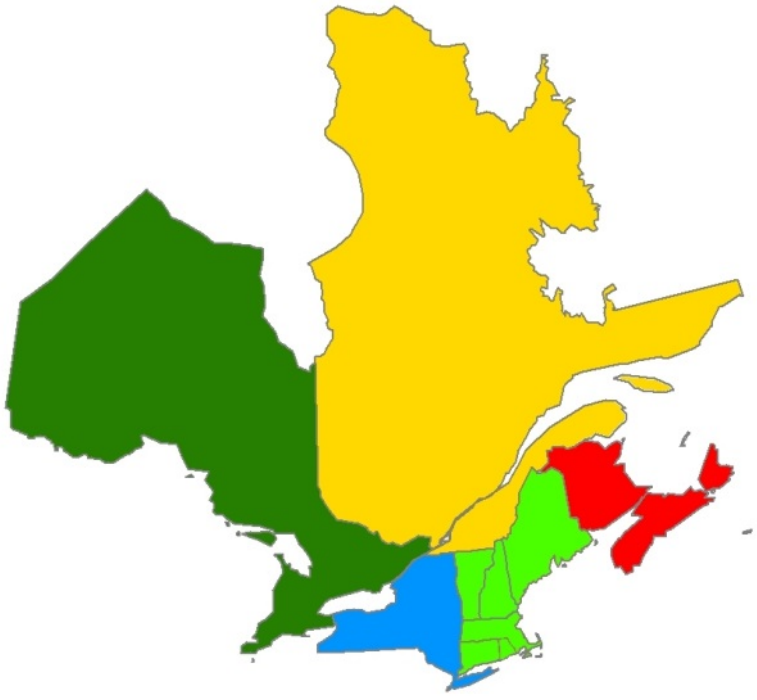
Working Capital and Operating Reserve Analysis 2014-2015			
CRITERIA SERVICES DIVISION			
	Total Reserve	**Operating Reserve**	**Working Capital**
Beginning Working Capital and Operating Reserves, December 31, 2013	816,612	727,857	88,755
2014 Non-Statutory Funding (from members)	989,708	989,708	0
2014 Other funding sources	0	0	0
Less: 2014 Projected expenses & fixed asset additions	(1,065,100)	(1,065,100)	0
Projected Working Capital, December 31, 2014	**741,220**	**652,465**	**88,755**
Desired Working Capital and Operating Reserve, December 31, 2015	**647,000**	552,884	94,116
Less: Projected Working Capital Reserve Balance December 31, 2014	(741,220)	(652,465)	(88,755)
Increase(decrease) in assessments to achieve desired Total Reserve	(94,220)	(99,581)	5,361
2015 Funding requirement for expenses and fixed asset additions	1,129,441		
Adjustment to achieve desired Working Capital and Operating Reserve balance	(94,220)		
2015 Funding and reserve requirement	1,035,221		

Explanation of Changes in Reserve Policy from Prior Year

On October 29, 2013 NPCC's Board of Directors approved management's proposed Working Capital and Operating Reserve Policy. The policy calls for a range between 8.33% (30 days) and 25.00% (90 days) rather than the specific required level of Operating Reserves of 8.33%. This range will allow for more stability in Assessments. The Working Capital required balance remains unchanged at 8.33% (30 days).

Section D – Additional Consolidated Financial Statements

2015 Business Plan and Budget



Section D

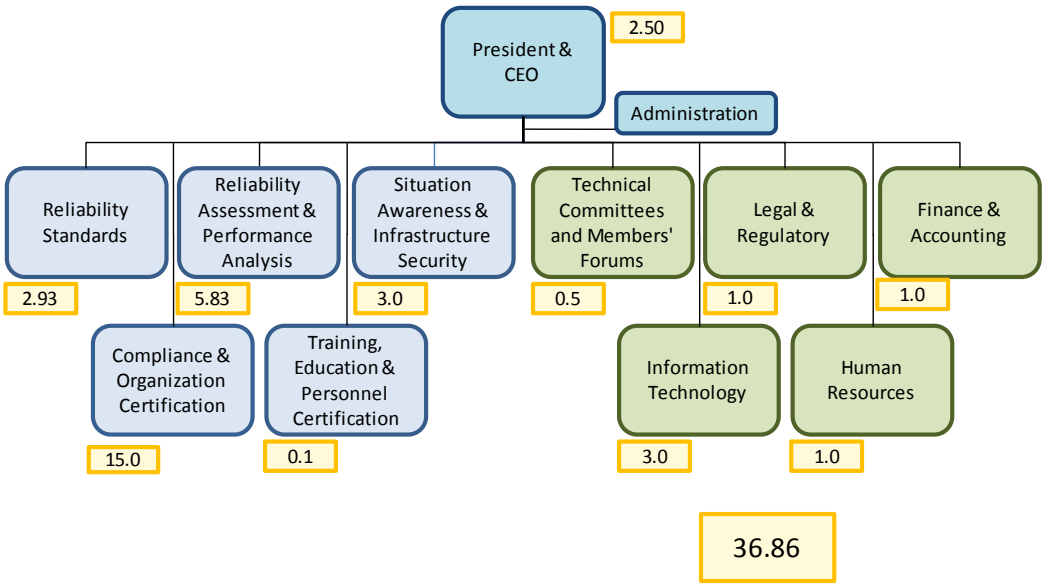
Statement of Financial Position

Table to be Inserted

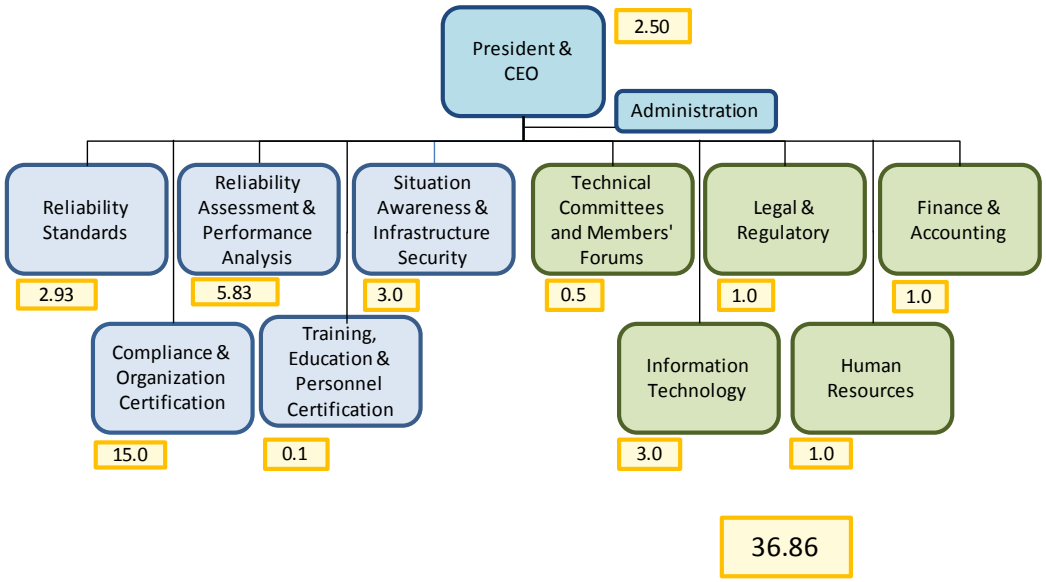
Table to be Inserted

Table to be Inserted

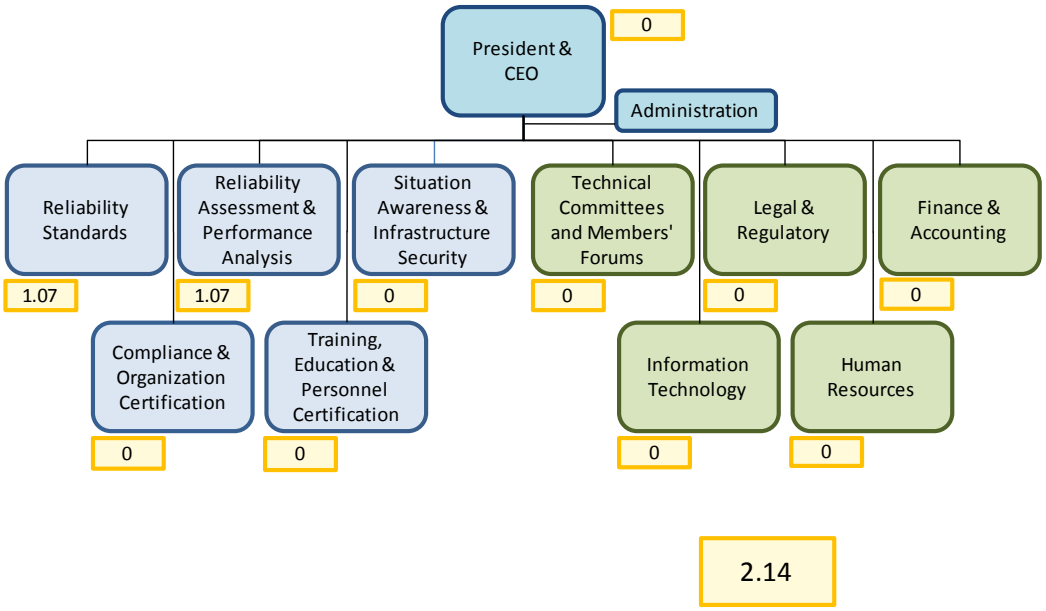
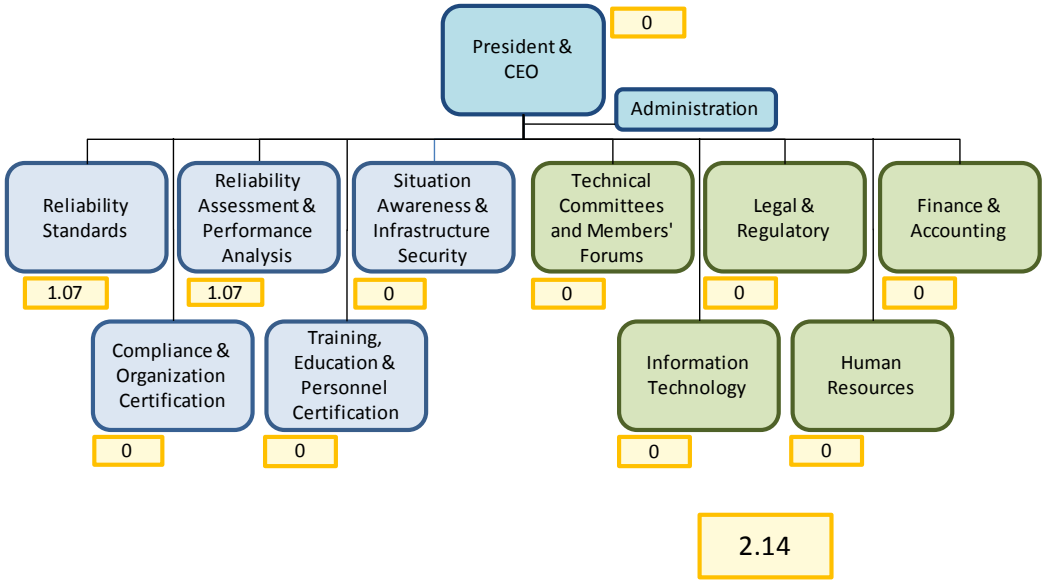
2014 Budget Staff Allocations - RE Division



2015 Budget Staff Allocations - RE Division



2014 Budget Staff Allocations - CS Division



2015 Budget Staff Allocations - CS Division